



Microsoft

# WINDOWS SERVER 2003 PKI and CERTIFICATE SECURITY

*Brian Komar with  
the Microsoft PKI Team*

**PUBLISHED BY**

Microsoft Press  
A Division of Microsoft Corporation  
One Microsoft Way  
Redmond, Washington 98052-6399

Copyright © 2004 by Brian Komar

All rights reserved. No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

Library of Congress Cataloging-in-Publication Data pending.

ISBN 0-7356-2021-0

Printed and bound in the United States of America.

1 2 3 4 5 6 7 8 9 QWT 9 8 7 6 5 4

Distributed in Canada by H.B. Fenn and Company Ltd.

A CIP catalogue record for this book is available from the British Library.

Microsoft Press books are available through booksellers and distributors worldwide. For further information about international editions, contact your local Microsoft Corporation office or contact Microsoft Press International directly at fax (425) 936-7329. Visit our Web site at [www.microsoft.com/learning/](http://www.microsoft.com/learning/). Send comments to [rkinput@microsoft.com](mailto:rkinput@microsoft.com).

Active Directory, ActiveX, Microsoft, Outlook, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

This book expresses the author's views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the authors, Microsoft Corporation, nor its resellers or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

**Acquisitions Editor:** Martin DelRe

**Project Editor:** Denise Bankaitis

**Technical Editor:** Ronald Beckelaar

**Indexer:** Julie Kawabata

*To my parents, Ron and Bernice*



# Contents

Acknowledgments . . . . .	xvii
Introduction . . . . .	xix

## Part I Foundations of PKI

<b>1</b>	<b>Basics of Cryptography</b>	<b>3</b>
	Encryption Types . . . . .	3
	Algorithms and Keys . . . . .	4
	Data Encryption. . . . .	5
	Symmetric Encryption . . . . .	5
	Asymmetric Encryption. . . . .	7
	Combining Symmetric and Asymmetric Encryption . . . . .	10
	Digital Signing of Data . . . . .	12
	The Hash Process . . . . .	12
	Hash Algorithms . . . . .	12
	Combining Asymmetric Signing and Hash Algorithms . . . . .	13
	Case Study: Microsoft Applications and Their Encryption Algorithms . . . . .	14
	Opening the EFS White Paper. . . . .	14
	Case Study Questions . . . . .	15
	Additional Information . . . . .	15
<b>2</b>	<b>Primer to PKI</b>	<b>17</b>
	Certificates. . . . .	17
	X.509 Version 1 . . . . .	18
	X.509 Version 2 . . . . .	20
	X.509 Version 3 . . . . .	21
	Certification Authorities . . . . .	27
	Root CA . . . . .	28
	Intermediate CA . . . . .	29
	Policy CA . . . . .	29
	Issuing CA . . . . .	31
	Certificate Revocation Lists . . . . .	31
	Types of CRLs . . . . .	31
	Revocation Reasons . . . . .	32

**What do you think of this book?**  
We want to hear from you!

Microsoft is interested in hearing your feedback about this publication so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit: [www.microsoft.com/learning/booksurvey/](http://www.microsoft.com/learning/booksurvey/)

Case Study: Inspecting an X.509 Certificate . . . . . 33  
    Opening the Certificate File . . . . . 33  
    Case Study Questions . . . . . 33  
Additional Information . . . . . 34

**3 Policies and PKI 35**

Security Policy. . . . . 36  
    Defining Effective Security Policies . . . . . 37  
    Resources for Developing Security Policies . . . . . 37  
    Defining PKI-Related Security Policies . . . . . 38  
Certificate Policy . . . . . 39  
    Contents of a Certificate Policy. . . . . 40  
    Certificate Policy Example . . . . . 40  
Certificate Practice Statement (CPS). . . . . 42  
    CPS: Introduction . . . . . 43  
    CPS: General Provisions . . . . . 44  
    CPS: Identification and Authentication . . . . . 44  
    CPS: Operational Requirements . . . . . 45  
    CPS: Physical, Procedural, and Personnel Security Controls . . . . . 46  
    CPS: Technical Security Controls . . . . . 46  
    CPS: Certificate and Certificate Revocation List (CRL) Profiles . . . . . 47  
    CPS: Specification Administration. . . . . 47  
Case Study: Planning Policy Documents . . . . . 47  
    Design Requirements . . . . . 47  
    Case Study Questions . . . . . 48  
Additional Information . . . . . 48

**Part II Establishing a PKI**

**4 Preparing an Active Directory Environment 51**

Preparing a Windows 2000 Active Directory Environment . . . . . 51  
    Microsoft Exchange Modifications. . . . . 52  
    Extending the Schema. . . . . 58  
    Modifying Membership in Cert Publishers . . . . . 60  
Preparing a Windows Server 2003 Active Directory Environment . . . . . 63  
Preparing Non-Active Directory Environments . . . . . 64  
Case Study: Preparing Active Directory . . . . . 64  
    Network Details . . . . . 65  
    Case Study Questions . . . . . 65  
Additional Information . . . . . 66

<b>5</b>	<b>Designing a Certification Authority Hierarchy</b>	<b>67</b>
	Determining the Number of Tiers in a CA Hierarchy . . . . .	67
	A Single-Tier CA Hierarchy . . . . .	67
	A Two-Tier CA Hierarchy . . . . .	68
	A Three-Tier CA Hierarchy . . . . .	69
	A Four-Tier CA Hierarchy . . . . .	70
	Organizing Issuing CAs . . . . .	71
	Choosing an Architecture . . . . .	73
	Gathering Required Information . . . . .	74
	Identifying PKI-Enabled Applications . . . . .	74
	Determining Security Requirements . . . . .	76
	Determining Technical Requirements . . . . .	78
	Determining Business Requirements . . . . .	85
	Determining External Requirements . . . . .	85
	Case Study: Identifying Requirements . . . . .	87
	Case Study Questions . . . . .	88
	Additional Information . . . . .	89
<b>6</b>	<b>Implementing a CA Hierarchy</b>	<b>91</b>
	Preparing Configuration Scripts for Installation . . . . .	93
	CAPolicy.inf File . . . . .	93
	Pre-Installation Scripts . . . . .	102
	Post-Installation Scripts . . . . .	106
	Implementing an Enterprise Root CA . . . . .	113
	Creating a CAPolicy.inf File . . . . .	114
	Installing Internet Information Services . . . . .	115
	Installing Certificate Services . . . . .	116
	Post-Installation Configuration . . . . .	117
	Enabling Auditing . . . . .	118
	Implementing a Standalone Root CA . . . . .	119
	Creating a CAPolicy.inf File . . . . .	120
	Installing Certificate Services . . . . .	121
	Post-Installation Configuration . . . . .	122
	Object Access Auditing . . . . .	123
	Implementing an Offline Policy CA . . . . .	124
	Pre-Installation Configuration . . . . .	124
	Creating a CAPolicy.inf File . . . . .	125
	Installing Certificate Services . . . . .	125
	Post-Installation Configuration . . . . .	130
	Object Access Auditing . . . . .	131

	Implementing an Online Issuing CA . . . . .	131
	Pre-Installation Configuration . . . . .	131
	Creating a CAPolicy.inf File . . . . .	133
	Installing IIS . . . . .	134
	Installing Certificate Services . . . . .	134
	Post-Installation Configuration . . . . .	138
	Object Access Auditing . . . . .	139
	Verifying Installation . . . . .	140
	Case Study: Deploying a PKI . . . . .	141
	Case Study Questions . . . . .	142
	Additional Information . . . . .	144
<b>7</b>	<b>Securing a CA Hierarchy</b>	<b>145</b>
	Designing CA Configuration Security Measures . . . . .	145
	Designing Physical Security Measures . . . . .	148
	Securing the CA's Private Key . . . . .	150
	Private Key Stored in the Local Machine Store . . . . .	150
	Private Keys Stored on Smart Cards . . . . .	151
	Private Keys Stored on Hardware Security Modules . . . . .	152
	Hardware Security Modules . . . . .	152
	Categories of HSMs . . . . .	153
	HSM Vendors . . . . .	154
	HSM Deployment Methods . . . . .	158
	Case Study: Planning HSM Deployment . . . . .	162
	Scenario . . . . .	163
	Case Study Questions . . . . .	164
	Additional Information . . . . .	165
<b>8</b>	<b>Designing Certificate Templates</b>	<b>167</b>
	Certificate Template Versions . . . . .	167
	Version 1 Certificate Templates . . . . .	167
	Version 2 Certificate Templates . . . . .	170
	Enrolling Certificates Based on Certificate Templates . . . . .	171
	Modifying Certificate Templates . . . . .	171
	Modifying Version 1 Certificate Template Permissions . . . . .	171
	Modifying Version 2 Certificate Templates . . . . .	172
	Best Practices for Certificate Template Design . . . . .	182
	Case Study: Certificate Template Design . . . . .	183
	Requirements . . . . .	183
	Case Study Questions . . . . .	183
	Additional Information . . . . .	185



<b>9</b>	<b>Certificate Validation</b>	<b>187</b>
	Certificate Validation Process . . . . .	187
	Certificate Validity Checks . . . . .	188
	Certificate Revocation . . . . .	189
	Types of CRLs . . . . .	189
	CRL Retrieval Process . . . . .	190
	Revocation Reasons . . . . .	190
	Revoking a Certificate . . . . .	191
	Building Certificate Chains . . . . .	192
	Exact Match . . . . .	193
	Key Match . . . . .	194
	Name Match . . . . .	195
	Designing PKI Object Publication . . . . .	196
	Choosing Publication Protocols . . . . .	196
	Choosing Publication Points . . . . .	197
	Choosing Publication Intervals . . . . .	199
	Troubleshooting Publication Points . . . . .	201
	Certutil . . . . .	202
	PKI Health Tool . . . . .	202
	Case Study: Choosing Publication Points . . . . .	204
	Design Requirements . . . . .	204
	Case Study Questions . . . . .	205
	Additional Information . . . . .	205
<b>10</b>	<b>Role Separation</b>	<b>207</b>
	Common Criteria Roles . . . . .	207
	Common Criteria Levels . . . . .	207
	The Windows Server 2003 Implementation of Common Criteria . . . . .	210
	Assigning Common Criteria Roles . . . . .	215
	Implementing Certificate Manager Restrictions . . . . .	217
	Enforcing Common Criteria Role Separation . . . . .	218
	Other PKI Management Roles . . . . .	220
	Local Administrator . . . . .	220
	Enterprise Admins . . . . .	221
	Certificate Template Manager . . . . .	222
	Enrollment Agent . . . . .	226
	Key Recovery Agent . . . . .	227
	Case Study: Planning PKI Management Roles . . . . .	228
	Scenario . . . . .	228
	Case Study Questions . . . . .	229
	Additional Information . . . . .	230

<b>11</b>	<b>Planning and Implementing Disaster Recovery</b>	<b>233</b>
	Developing Required Documentation . . . . .	234
	Choosing a Backup Method . . . . .	235
	System State Backups . . . . .	236
	Manual Backups . . . . .	236
	Performing System State Backups . . . . .	237
	Performing Manual Backups . . . . .	238
	Using the Certification Authority Console . . . . .	238
	Using Certutil . . . . .	239
	Other Backup Methods . . . . .	241
	Restoration Procedures . . . . .	242
	Reinstalling Certificate Services . . . . .	242
	Restoring System State Backups . . . . .	244
	Restoring Manual Backups . . . . .	245
	Evaluating Backup Methods . . . . .	245
	Hardware Failure . . . . .	246
	Certificate Services Failure . . . . .	246
	Server Replacement . . . . .	247
	Case Study: Replacing Server Hardware . . . . .	248
	Scenario . . . . .	249
	Case Study Questions . . . . .	249
	Additional Information . . . . .	250
<b>12</b>	<b>Deploying Certificates</b>	<b>251</b>
	Certificate Enrollment Methods . . . . .	253
	Choosing an Enrollment Method . . . . .	255
	Choosing Among Manual Enrollment Methods . . . . .	255
	Choosing Among Automatic Enrollment Methods . . . . .	255
	Publishing Certificate Templates for Enrollment . . . . .	256
	Performing Manual Enrollment . . . . .	257
	Using the Certificate Request Wizard . . . . .	265
	Performing Automatic Enrollment . . . . .	267
	Automatic Certificate Request Settings . . . . .	267
	Autoenrollment Settings . . . . .	268
	Performing Scripted Enrollment . . . . .	270
	Certreq.exe . . . . .	270
	Custom Scripting . . . . .	273
	Case Study: Selecting a Deployment Method . . . . .	274
	Scenario . . . . .	275
	Case Study Questions . . . . .	275
	Additional Information . . . . .	276

<b>13</b>	<b>Creating Trust Between Organizations</b>	<b>279</b>
	Methods of Creating Trust . . . . .	279
	Certificate Trust Lists . . . . .	280
	Common Root CAs . . . . .	282
	Cross Certification . . . . .	284
	Bridge CAs . . . . .	285
	Qualified Subordination Conditions . . . . .	288
	Name Constraints . . . . .	289
	Basic Constraints . . . . .	292
	Application Policies . . . . .	294
	Certificate Policies . . . . .	296
	Guidelines for Qualified Subordination Conditions . . . . .	299
	Implementing Qualified Subordination . . . . .	299
	Implementing the Policy.inf File . . . . .	301
	Acquiring a Partner's CA Certificate . . . . .	302
	Generating the Cross Certification Authority Certificate . . . . .	302
	Publishing to Active Directory . . . . .	304
	Verifying Qualified Subordination . . . . .	304
	Case Study: Trusting Certificates from Another Forest . . . . .	305
	Case Study Questions . . . . .	306
	Additional Information . . . . .	307
<b>Part III</b>	<b>Deploying Application-Specific Solutions</b>	
<b>14</b>	<b>Archiving Encryption Keys</b>	<b>311</b>
	Roles in Key Archival . . . . .	312
	The Key Archival Process . . . . .	312
	The Key Recovery Process . . . . .	314
	Requirements for Key Archival . . . . .	315
	Defining Key Recovery Agents . . . . .	316
	Enabling a CA for Key Archival . . . . .	320
	Enabling Key Archival in a Certificate Template . . . . .	322
	Performing Key Recovery . . . . .	322
	Certutil . . . . .	322
	Key Recovery Tool . . . . .	323
	Importing the Recovered Private Key . . . . .	325
	Best Practices . . . . .	326
	Case Study: Lucerne Publishing . . . . .	327
	Scenario . . . . .	328
	Case Study Questions . . . . .	328
	Additional Information . . . . .	329

<b>15</b>	<b>Smart Card Deployment</b>	<b>331</b>
	Using Smart Cards in an Active Directory Environment . . . . .	331
	Smart Cards and Kerberos. . . . .	332
	Requirements for Smart Card Certificates. . . . .	333
	Planning Smart Card Deployment . . . . .	334
	Increasing the Assurance of Smart Card Certificates . . . . .	335
	Identifying the Required Certificate Templates . . . . .	335
	Determining Certificate Distribution Methods . . . . .	336
	Designing Certificate Templates for Smart Cards . . . . .	338
	Deploying a Smart Card Management System . . . . .	342
	Procedures . . . . .	342
	Enabling ActiveX Controls. . . . .	342
	Requesting Smart Card Certificates on Behalf of Other Users. . . . .	345
	Enabling Autoenrollment . . . . .	346
	Implementing Additional Security for Smart Cards . . . . .	347
	Requiring Smart Cards for Interactive Logon . . . . .	347
	Requiring Smart Cards for Remote Access . . . . .	348
	Defining Smart Card Removal Behavior . . . . .	348
	Using Smart Cards for Administrative Tasks . . . . .	348
	Best Practices . . . . .	349
	Case Study: City Power and Light . . . . .	350
	Case Study Questions . . . . .	352
	Additional Information . . . . .	353
<b>16</b>	<b>Encrypting File System</b>	<b>355</b>
	EFS Processes . . . . .	356
	How Windows Chooses an EFS Encryption Certificate . . . . .	356
	Local EFS Encryption. . . . .	357
	Remote EFS Encryption Using SMB. . . . .	358
	Remote EFS Encryption Using WebDAV . . . . .	359
	EFS Decryption . . . . .	359
	EFS Data Recovery . . . . .	360
	One Application, Two Recovery Methods . . . . .	361
	Data Recovery . . . . .	362
	Key Recovery . . . . .	366
	Deploying EFS. . . . .	366
	Enabling and Disabling EFS . . . . .	366
	Certificate Templates for EFS Encryption. . . . .	367
	Certificate Enrollment . . . . .	370
	Best Practices . . . . .	371

	Case Study: Lucerne Publishing . . . . .	372
	Scenario . . . . .	373
	Design Requirements . . . . .	373
	Proposed Solution . . . . .	373
	Case Study Questions . . . . .	375
	Additional Information . . . . .	375
<b>17</b>	<b>Implementing SSL Encryption for Web Servers</b>	<b>377</b>
	How SSL Works . . . . .	377
	Certificate Requirements for SSL . . . . .	380
	Choosing a Web Server Certificate Provider . . . . .	380
	Placement of Web Server Certificates . . . . .	381
	Single Web Server . . . . .	381
	Clustered Web Servers . . . . .	382
	Web Server Protected by ISA with Server Publishing . . . . .	383
	Web Server Protected by ISA with Web Publishing . . . . .	383
	Choosing a Certificate Template . . . . .	385
	Issuing Web Server Certificates . . . . .	386
	Issuing Web Server Certificates to Forest Members . . . . .	386
	Issuing Web Server Certificates to Non-Forest Members . . . . .	389
	Issuing Web Server Certificates to Third-Party Web Servers and Web Acceleration Devices . . . . .	393
	Certificate-Based Authentication . . . . .	394
	Defining Certificate Mappings . . . . .	395
	Choosing Where to Perform Certificate Mappings . . . . .	396
	Performing Certificate-Based Authentication . . . . .	397
	Configure IIS to Use Active Directory Mappings . . . . .	397
	Configure IIS to Use IIS Certificate Mappings . . . . .	402
	Best Practices . . . . .	404
	Case Study: The Phone Company . . . . .	406
	Scenario . . . . .	406
	Case Study Questions . . . . .	408
	Additional Information . . . . .	408
<b>18</b>	<b>Secure E-Mail</b>	<b>411</b>
	Securing E-Mail . . . . .	411
	Secure Multipurpose Internet Mail Extensions (S/MIME) . . . . .	412
	SSL for Internet Protocols . . . . .	415
	Choosing Certification Authorities . . . . .	419
	Choosing Commercial CAs . . . . .	419
	Choosing Private CAs . . . . .	420

- Choosing Certificate Templates . . . . . 421
  - A Combined Signing and Encryption Template . . . . . 421
  - Dual Certificates for E-Mail. . . . . 422
- Choosing Deployment Methods . . . . . 425
- Enabling Secure E-Mail . . . . . 426
  - Enabling Outlook . . . . . 427
  - Enabling OWA . . . . . 428
  - Enabling Outlook Express. . . . . 429
  - Sending Secure E-Mail. . . . . 430
- Migrating from Previous Exchange Server Versions . . . . . 431
  - Upgrade to Exchange 2000 . . . . . 431
  - Enable Key Archival at the Windows Server 2003 Enterprise CA . . . . . 432
  - Install an Encryption Certificate at the Enterprise CA . . . . . 432
  - Enable Foreign Certificate Import at the Enterprise CA . . . . . 432
  - Export the Exchange KMS Database. . . . . 433
  - Import the Exchange KMS Database into Enterprise CA Database . . . . . 435
- Best Practices . . . . . 435
- Case Study: Adventure Works . . . . . 436
  - Scenario. . . . . 437
  - Case Study Questions . . . . . 438
- Additional Information . . . . . 439

**19 Virtual Private Networking 441**

- Certificate Deployment for VPN. . . . . 441
  - Point-to-Point Tunneling Protocol (PPTP). . . . . 441
  - Layer Two Tunneling Protocol (L2TP) with IP Security. . . . . 444
- Certificate Template Design . . . . . 446
  - User Authentication. . . . . 446
  - Server Authentication . . . . . 447
  - IPSec Endpoint Authentication . . . . . 448
- Deploying a VPN Solution. . . . . 449
  - IAS Server Configuration . . . . . 450
  - VPN Server Configuration. . . . . 454
  - Create a VPN Connection Object. . . . . 456
- Best Practices . . . . . 459
- Case Study: Lucerne Publishing . . . . . 460
  - Scenario. . . . . 461
  - Case Study Questions . . . . . 462
- Additional Information . . . . . 463

<b>20</b>	<b>Wireless Networking</b>	<b>467</b>
	Threats Introduced by Wireless Networking . . . . .	467
	Protecting for Wireless Communications . . . . .	468
	MAC Filtering . . . . .	468
	Wired Equivalent Privacy . . . . .	469
	Wi-Fi Protected Access . . . . .	470
	802.1x Authentication Types . . . . .	470
	EAP/TLS Authentication . . . . .	471
	PEAP Authentication . . . . .	471
	How 802.1x Authentication Works . . . . .	471
	Planning Certificates for 802.1x Authentication . . . . .	473
	Computer Certificates for RADIUS Servers . . . . .	473
	User Certificates for Clients . . . . .	474
	Computer Certificates for Clients . . . . .	474
	Deploying Certificates to Users and Computers . . . . .	475
	RADIUS Server . . . . .	475
	Client Computers . . . . .	476
	Users . . . . .	476
	Implementing 802.1x Authentication . . . . .	477
	Configuring the RADIUS Server . . . . .	477
	Configuring the Wireless Access Point . . . . .	483
	Connecting to the Wireless Network . . . . .	483
	Best Practices . . . . .	486
	Case Study: Margie's Travel . . . . .	486
	Scenario . . . . .	487
	Case Study Questions . . . . .	488
	Additional Information . . . . .	489
<b>21</b>	<b>Code Signing</b>	<b>491</b>
	How Code Signing Works . . . . .	491
	Certification of Code Signing Certificates . . . . .	493
	Commercial Certification . . . . .	494
	Corporate Certification . . . . .	495
	Planning Deployment of Code Signing Certificates . . . . .	496
	Certificate Template Design . . . . .	496
	Planning Enrollment Methods . . . . .	497
	Performing Code Signing . . . . .	497
	Gathering the Required Tools . . . . .	497
	Using Signcode.exe . . . . .	498
	Visual Basic for Applications Projects . . . . .	500

Verifying the Signature . . . . . 502  
    Internet Explorer . . . . . 502  
    The Check Trust Program (Chktrust.exe) . . . . . 503  
Best Practices . . . . . 504  
Case Study: Lucerne Publishing . . . . . 505  
    Scenario . . . . . 505  
    Case Study Questions . . . . . 506  
Additional Information . . . . . 506

**Appendix: Case Study Answers 509**

Chapter 1: Basics of Cryptography . . . . . 509  
Chapter 2: Primer to PKI . . . . . 510  
Chapter 3: Policies and PKI . . . . . 511  
Chapter 4: Preparing an Active Directory Environment . . . . . 512  
Chapter 5: Designing a Certification Authority Hierarchy . . . . . 513  
Chapter 6: Implementing a CA Hierarchy . . . . . 515  
Chapter 7: Securing a CA Hierarchy . . . . . 518  
Chapter 8: Designing Certificate Templates . . . . . 519  
Chapter 9: Certificate Validation . . . . . 521  
Chapter 10: Role Separation . . . . . 521  
Chapter 11: Planning and Implementing Disaster Recovery . . . . . 524  
Chapter 12: Issuing Certificates . . . . . 525  
Chapter 13: Creating Trust Between Organizations . . . . . 527  
Chapter 14: Archiving Encryption Keys . . . . . 528  
Chapter 15: Smart Card Deployment . . . . . 529  
Chapter 16: Encrypting File System . . . . . 531  
Chapter 17: Implementing SSL Encryption for Web Servers . . . . . 532  
Chapter 18: Secure E-Mail . . . . . 533  
Chapter 19: Virtual Private Networking . . . . . 535  
Chapter 20: Wireless Networking . . . . . 537  
Chapter 21: Code Signing . . . . . 539

Index . . . . . 541

**What do you think of this book?**  
We want to hear from you!

Microsoft is interested in hearing your feedback about this publication so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit: [www.microsoft.com/learning/booksurvey/](http://www.microsoft.com/learning/booksurvey/)



# Acknowledgments

When you work on a book project, several people are involved in the writing process one way or another, and I am going to try my best to thank everyone who helped me through the research, envisioning, and writing of this book. If I did miss anyone, it is only because there were so many people who played a part in making this book a reality!

The first group of people that I want to thank is the PKI product and testing team, current members and past members, from Microsoft: David Cross, Vic Heller, Laudon Williams, Trevor Freeman, Phil Hallin, Darren Canavor, Sergio Dutra, Krish Shenoy, Larry Talbot, Mike Danseglio, and Vishal Agarwal. All of you helped me get my head around several of the specifics of the Microsoft PKI. I especially want to thank David Cross and Trevor Freeman who assisted me with the three white papers that I wrote for Microsoft during the beta phase of Microsoft Windows Server 2003. The informal discussions we shared on content and best practices greatly assisted me in thinking “outside the box” when looking at PKI solutions. I would not be where I am today without the guidance and mentoring you provided, and continue to provide, to me!

The second group of people that I have to thank is Microsoft Consulting Services and my clients over the last two years. Lori Woehler, Christi Droz, and John Howie have all assisted me in developing a great PKI offering for our clients. I would like to thank some of Microsoft’s great PKI consultants, Carsten Kinder, Ayman AlRashed, and Ian Hellen, for the continual exchange of ideas and recommendations for solving our clients’ PKI deployment requirements. Finally, from this group, I also have to thank my engagement managers and especially my clients, for believing in the methodologies that my company uses for PKI deployments.

A book is only as good as the project team that helps the author translate thoughts to words on a page. I want to specifically thank the following individuals:

- Martin DelRe for bringing the book proposal to Microsoft Press.
- Denise Bankaitis for keeping the project flowing (especially with my attempting to write parts of this book on every continent, or so it seemed).
- David Cross and Ronald Beekelaar for your outstanding technical review of the content. Although the reviews took me hours to incorporate, the book is much stronger because of your efforts and knowledge.
- Brenda Pittsley, Sandi Resnick, and Erika Kauppi for your copy edits and reviews of the finalized content. Your attention to detail is so very much appreciated.

- Dan Latimer and Joel Panchot for the long hours you spent on the book's layout and art. Your commitment to quality has made a noticeable difference in the book's appearance.
- Kristen McCarthy for helping me with the initial drafts of each chapter and for attempting to cure me of my horrible habit of using passive voice. Kristen, you make me shine as an author because of your efforts to clean up my words.

Finally, I have to thank a group of developers from my customers and Microsoft that provided me with a certificate enrollment script that simply amazes me. Ryan Hurst, Doug McDorman, Gary Cole, Ken Jackson, and Carlos Lopez all contributed to the enrollment script used in several examples of this book, and without their knowledge, dedication, and superior coding skills, the book would have been missing a crucial component for assisting in the deployment of certificates to users and computers.

# Introduction

Welcome to *Microsoft Windows Server 2003 PKI and Certificate Security*. This book provides detailed information about designing and implementing public key infrastructure (PKI) solutions with the Windows Server 2003 certification authority (CA). This book is based on the white papers and guidelines produced by the Microsoft PKI product team and on my experience working with Microsoft Consulting Services at customer sites over the past two years.

## About This Book

Although you are welcome to read the book from cover to cover, it is divided into three self-contained parts. Each part contains chapters that build on the lessons and practices described within that part. Each chapter ends with a case study that enforces the critical concepts discussed in the chapter, allowing you to validate how well you understand the concepts of the chapter.



**Note** The answers for the case study questions are available in the Appendix, “Case Study Answers” in both the print copy of the book and the eBook, which can be found on the Microsoft Windows Server 2003 PKI and Certificate Security Companion CD.

The three parts of this book are:

- **Part 1, “Foundations of PKI.”** Part 1 provides an overview of cryptography and PKI concepts and culminates with one of the most important chapters in the book, “Policies and PKI.” Part 1 ensures that you understand the relationship between a PKI and your organization’s security policies. Without strong policies and procedures, a PKI is simply a collection of application servers, rather than a mechanism for securing your network and its applications.
- **Part 2, “Establishing a PKI.”** Part 2 provides a framework for designing and implementing a PKI within your organization, including detailed information on preparing your Active Directory environment and designing and implementing your organization’s certification authority (CA) hierarchy. Part 2 includes information on designing and implementing a CA hierarchy, designing certificate templates, planning deployment of certificates to users and computers, and disaster recovery recommendations. When you complete Part 2 you will have a CA hierarchy that is ready to deploy certificates for any PKI-enabled application used by your organization.

- **Part 3, “Deploying Application-Specific Solutions.”** Part 3 provides detailed information on deploying certificates for specific PKI-enabled applications. Each chapter in this section offers details on the types of certificates required for the specific application, recommendations on how to deploy the certificates to the required users and computers, and provides best practices for deploying each PKI-enabled application.

## Microsoft Windows Server 2003 PKI and Certificate Security Companion CD

The companion CD with this book contains a variety of tools, scripts, and white papers to help you deploy a Windows Server 2003 PKI and issue certificates to computers running Windows 2000, Windows XP, and Windows Server 2003. Many of these tools are from the *Microsoft Windows Server 2003 Resource Kit* (Microsoft Press, 2004). The included tools can be implemented on computers running either the Windows XP or Windows Server 2003 operating systems. Specifically, the tools are on the CD in the *Resource Kit Tools* folder, and the scripts and batch files are in the *Resources* folder in a sub-folder based on the chapter in which the script or batch file is referenced. Some of the Case Studies in the book require additional files. These additional files are found on the CD in the *Case Studies* folder in a sub-folder based on the chapter requiring the additional files. The companion CD further includes a fully searchable electronic version (eBook) of the book. To view the electronic version of the book, you'll need Adobe Acrobat or Adobe Reader. To obtain more information about these products or to download Adobe Reader, visit [www.adobe.com](http://www.adobe.com).

## Resource Kit Support Policy

Microsoft does not support the tools and scripts supplied on the *Microsoft Windows Server 2003 PKI and Certificate Security* companion CD. Microsoft does not guarantee the performance of the tools or scripting examples, or any bug fixes for these tools and scripts. However, Microsoft Press provides a way for customers who purchase this book to report any problems with the software and receive feedback on such issues—just send e-mail to [mspinput@microsoft.com](mailto:mspinput@microsoft.com). This e-mail address is only for issues related to *Microsoft Windows Server 2003 PKI and Certificate Security*. Microsoft Press also provides corrections for books and companion CDs through the World Wide Web at: [www.microsoft.com/learning/support/](http://www.microsoft.com/learning/support/). To connect directly to the Microsoft Knowledge Base and enter a query regarding a question or issue you might have, go to: [www.microsoft.com/learning/support/search.asp](http://www.microsoft.com/learning/support/search.asp). For issues related to the Windows operating system, please refer to the support information included with your product.

**Part I**

# **Foundations of PKI**



# Chapter 1

# Basics of Cryptography

This chapter will introduce the fundamentals of cryptography and provide a basic understanding of the type of encryption and signing that takes place in public key infrastructure (PKI)–enabled applications. This overview is not an in-depth look at cryptographic functions.



**More Info** For more information on cryptography, check out *Cryptography and Network Security: Principles and Practice*, Third Edition, by William Stallings, or *Practical Cryptography*, by Niels Ferguson and Bruce Schneier, which are referenced in the “Additional Information” section at the end of this chapter.

## Encryption Types

Cryptography supports symmetric encryption and asymmetric encryption for cryptographic functions.

- **Symmetric encryption.** The same key is used for encryption and decryption. The key must be exchanged so that both the data sender and the recipient can access the plaintext data.
- **Asymmetric encryption.** Two mathematically related keys, a key pair consisting of a public key and a private key, are used in the encryption and decryption processes.
  - If the public key is used for encryption, the associated private key is used for decryption.
  - If the private key is used for encryption, the associated public key is used for decryption.



**Note** Only one person can hold the private key, but the public key can be distributed freely. The public key, as an attribute of a digital certificate, is often published in a network-accessible directory (such as Active Directory) to allow easier access.

## Algorithms and Keys

When data is encrypted with cryptography, two inputs are required for encryption: an algorithm and a key.

- **Algorithm.** An algorithm defines how data is transformed when original plaintext data is converted into ciphertext. Both the data sender and the recipient must know the algorithm used for data transformation so that the same algorithm is used to decrypt the ciphertext back into the original plaintext data.
- **Key.** A key is used as an input to the algorithm, along with the plaintext data, so that the algorithm can convert plaintext data into ciphertext or decrypt ciphertext back into plaintext data.

All applications determine how these inputs are distributed between the sender and recipient. Although it is not a security issue if an attacker identifies the algorithm used to encrypt the data, interception of the key is considered a security risk.

To enable encryption, a PKI-enabled application must do the following:

- **Identify the algorithms that are supported by the application.** In some cases, the application must allow for algorithm negotiation so that the sender and recipient can negotiate the strongest form of encryption.
- **Generate a key for use with the algorithm.** In the best circumstances, the key is a one-time key—that is, it is only used for a single encryption and decryption process. When a key is reused many times, it becomes easier for attackers to determine the key, through a process called *differential cryptanalysis*. Differential cryptanalysis allows an attacker to determine the encryption key by supplying the encryption algorithm and several samples of ciphertext produced with the encryption key.
- **Determine a key distribution method.** The key must be securely transmitted from the sender to the recipient—that is, it must be protected against interception during this transmission and might have to be transmitted out-of-band (not on the network) or in an encrypted state.



# Data Encryption

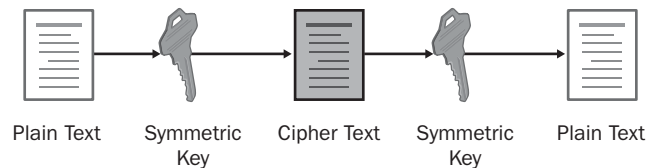
Encryption protects data against inspection by unauthorized people. This section will describe how symmetric encryption and asymmetric encryption processes work and how some applications combine symmetric and asymmetric processes.

## Symmetric Encryption

As mentioned, symmetric encryption uses the same key for both encryption and decryption. The algorithms associated with symmetric encryption are able to encrypt large amounts of data in little time thanks to the use of a single key and the fact that symmetric encryption algorithms are much simpler when compared to asymmetric encryption algorithms. (See Figure 1.1.)



**Note** Symmetric encryption is often referred to as *bulk encryption* because of its speed encrypting large amounts of plaintext data.



**Figure 1-1** The symmetric encryption process

When data is encrypted with a symmetric algorithm, the data sender generates a random symmetric key. The length of the key, typically in bits, is determined by the algorithm and the application using the symmetric algorithm.

Once the symmetric key is generated, the key is used to encrypt the plaintext data into an encrypted state, referred to as **ciphertext**. The ciphertext is then sent or made available to the data recipient.



**Note** The symmetric key must be securely transmitted to the recipient before the recipient can decrypt the ciphertext. The transmission of the symmetric key is the biggest security risk when using symmetric encryption algorithms. If the symmetric key is intercepted, attackers can decrypt all data.

When a recipient receives the encrypted ciphertext and the symmetric key, he or she can use the symmetric key to decrypt the data back into its original plaintext format.

## Symmetric Algorithms

Many of the most commonly used encryption algorithms are symmetric because of their ability to encrypt large amounts of data in little time. Symmetric algorithms used by PKI-enabled applications include:



**Note** This is not an exhaustive list of symmetric encryption protocols.

- **Data Encryption Standard (DES).** An encryption algorithm that encrypts data with a 56-bit, randomly generated symmetric key.
- **Data Encryption Standard XORed (DESX).** DESX is a stronger variation of the DES encryption algorithm. Rather than encrypting the plaintext directly, the plaintext is processed through an Exclusive Or (XOR) function with 64 bits of additional key material before the resulting data is encrypted with the DES algorithm. The output of the DES algorithm is also transformed with an XOR function with another 64 bits of key material. This helps protect the data against key search attacks based on the relatively short length of the DES 56-bit key.
- **Rivest's Cipher version 2 (RC2) (40 bit).** A variable key-size block cipher with an initial block size of 64 bits that uses an additional string of 40 bits called a *salt*. The salt is appended to the encryption key, and this lengthened key is used to encrypt the message.
- **RC2 (128 bit).** A variation on the RC2 (40-bit) cipher, where the salt length is increased to 88 bits.
- **RC4.** A variable key-size stream cipher with byte-oriented operations. The algorithm is based on the use of a random permutation and is commonly used for the encryption of traffic to and from secure Web sites using the SSL protocol.
- **Triple DES (3DES).** A variation on the DES encryption algorithm in which DES encryption is applied three times to the plaintext. The plaintext is encrypted with key A, decrypted with key B, and encrypted again with key C. A common form of 3DES uses only two keys: the plaintext is encrypted with key A, decrypted with key B, and encrypted again with key A.
- **Advanced Encryption Standard (AES).** Developed as a successor to DES, rather than using a 56-bit key, AES is able to use 128-bit, 192-bit, and 256-bit keys.



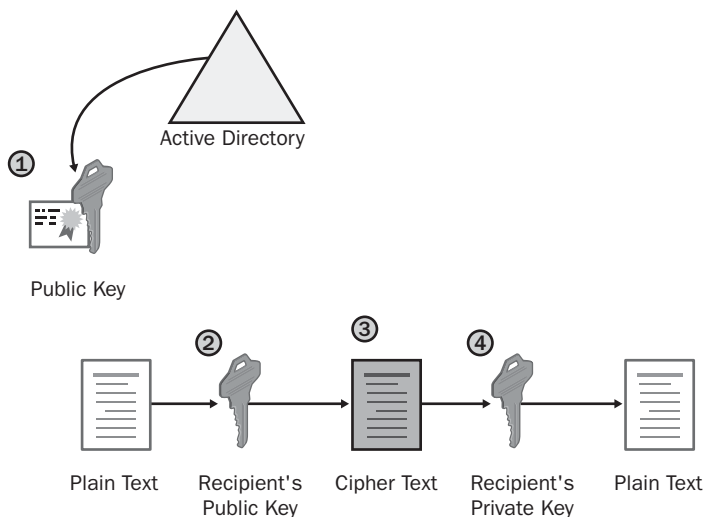
**Note** AES was developed in response to a call for proposals by the National Institute of Standards and Technology (NIST) for encryption of unclassified data. Several algorithms were proposed, and the algorithm ultimately selected was the Rijndael algorithm. More information on AES is provided in the “Additional Information” section at the end of this chapter.

## Asymmetric Encryption

Asymmetric encryption increases the security of the encryption process by utilizing two separate but mathematically related keys known as a public key and a private key. The encryption process is more secure because the private key is possessed only by the user or computer that generates the key pair. The public key can be distributed to any person who wishes to send encrypted data to the private key holder.

Asymmetric encryption’s use of two keys and the complexity of the asymmetric encryption algorithm makes the encryption process much slower. Studies have shown that symmetric encryption is at least 100 times faster than asymmetric encryption when using software-based cryptography and can be as much as 10,000 times faster when using hardware-based cryptography.

When data is encrypted with asymmetric encryption, the key pair used is owned by the data recipient. The use of this key pair ensures that only the recipient has access to the necessary private key to decrypt the data, limiting data encryption to the recipient. (See Figure 1-2.)



**Figure 1-2** The asymmetric encryption process

1. The data sender obtains the recipient's public key. This can be sent to the data originator by the recipient or retrieved from a directory, such as Active Directory.
2. The plaintext data is passed through an asymmetric encryption algorithm, using the recipient's public key as the encryption key. The encryption algorithm creates the encrypted ciphertext.
3. The ciphertext is sent or made available to the recipient. There is no need to send the key, as the recipient already has the private key required to decrypt the ciphertext.
4. The recipient decrypts the ciphertext with his or her private key, and the resulting plaintext is the original plaintext created by the data originator.



**Important** It is very rare for an application to only use an asymmetric encryption algorithm. Typically, the data is encrypted with a symmetric algorithm, and then only the symmetric encryption key is encrypted with the asymmetric encryption algorithm. This combination is discussed later in this chapter in the section titled “Combining Symmetric and Asymmetric Encryption.”

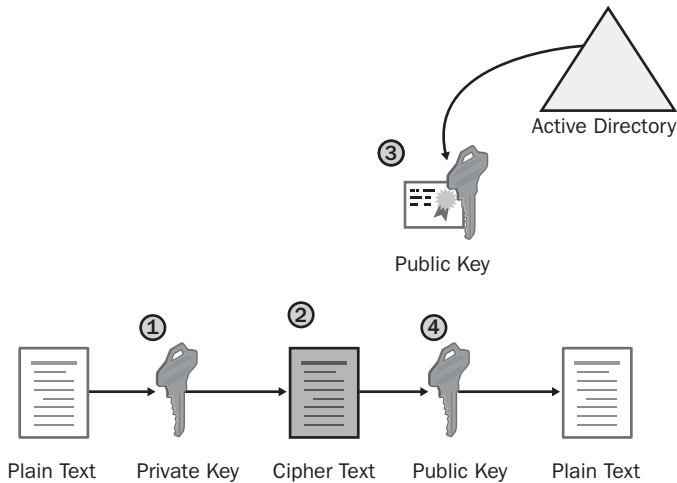
### Asymmetric Signing Process

Asymmetric algorithms can be used to protect data from modification and prove the data creator's identity. In this scenario, the public and private key roles are reversed, requiring use of the originator's key pair.



**Note** Proof of the originator's identity is accomplished because only the originator has access to the private key of the key pair. Of course, this is subject to the method used to protect the originator's private key. A hardware-protected private key, such as a private key stored on a smart card, provides more assurance than a private key stored in the user's local certificate store.

Figure 1-3 shows how asymmetric signing proves the sender's identity and prevents the data from being modified.



**Figure 1-3** The asymmetric signing process

1. The plaintext data is passed through an asymmetric encryption algorithm, using the originator's private key as the encryption key. The result of the encryption algorithm is the encrypted ciphertext.
2. The ciphertext is sent or made available to the recipient.
3. The data recipient obtains the originator's public key. The public key can be sent with the ciphertext, or the recipient can obtain the public key from a trusted source, such as a directory.
4. The recipient decrypts the ciphertext with the originator's public key. The resulting plaintext is the original plaintext created by the data originator.

Decryption by the public key of the originator's key pair proves that the data was created by the originator. It also proves that the data was not modified in transit, as any modification results in a decryption process failure.

## Asymmetric Algorithms

The following asymmetric algorithms are used in PKI-enabled applications when encrypting or digitally signing data.

- **Diffie-Hellman key agreement.** This algorithm is not based on encryption and decryption but instead relies on mathematical functions that enable two parties to generate a shared secret key for exchanging information online confidentially. When the Diffie-Hellman key agreement is used between two hosts, the two hosts agree on a public value ( $v$ ) and a large prime number ( $p$ ). Each

host chooses his or her own secret value and, using their three inputs (the public value, the prime number, and their secret value), they arrive at a public value that can be exchanged. These two public values are used to calculate a shared secret key used by both hosts to encrypt data sent between them.

- **Rivest Shamir Adleman (RSA).** This algorithm can be used for encrypting and signing data. The encryption and signing processes are performed through a series of modular multiplications. The security of the RSA algorithm can be increased by using longer key lengths, such as 1,024 bits or higher—the longer the key length, however, the slower the encryption or signing process.



**Note** Both Diffie-Hellman and RSA can be used for key exchange, allowing secure transmission or negotiation of a symmetric key between the data originator and recipient.

- **Digital Signature Algorithm (DSA).** This algorithm can be used only for signing data; it cannot be used for encryption. The DSA signing process is performed through a series of calculations based on a selected prime number. Although intended to have a maximum key size of 1,024 bits, longer key sizes are now supported.

RSA and DSA are only comparable in the creation and validation of digital signatures.

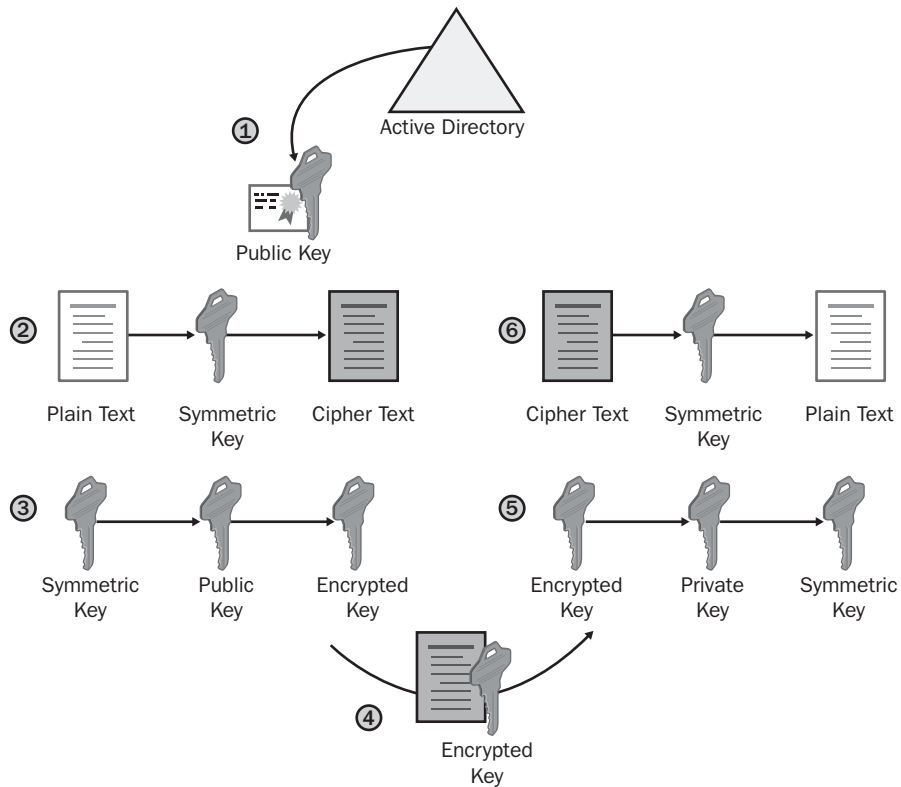
- When DSA is used, the process of creating the digital signature is faster than the validation process.
- When RSA is used, the opposite is true. It takes longer to generate the digital signature than it does to validate it.

When a developer of an application must decide whether to use RSA or DSA for digital signing, the decision often comes down to which operation is performed more frequently. For example, if you are signing a device driver for use by Microsoft Windows, it is better to use RSA because it is more common for the signature to be validated than created. On the other hand, if you are creating several documents that might be referenced by others, you get better performance using DSA to sign the documents.

## Combining Symmetric and Asymmetric Encryption

In most applications, symmetric and asymmetric encryption are combined to take advantage of each method's strengths. (See Figure 1-4.) When symmetric and asymmetric encryption are combined, the following takes place:

- Symmetric encryption is used to convert the plaintext to ciphertext. This takes advantage of the symmetric encryption speed.
- Asymmetric encryption is used to exchange the symmetric key used for encryption. This takes advantage of the security of asymmetric encryption, ensuring that only the intended recipient can decrypt the symmetric key.



**Figure 1-4** Combining symmetric and asymmetric encryption

1. The sender retrieves the recipient's public key. The sender retrieves the public key from a trusted source, such as Active Directory.
2. The sender generates a symmetric key and uses this key to encrypt the original data.
3. The symmetric key is encrypted with the recipient's public key to prevent the symmetric key from being intercepted during transmission.
4. The encrypted symmetric key and encrypted data are provided to the intended recipient.

5. The recipient uses his or her private key to decrypt the encrypted symmetric key.
6. The encrypted data is decrypted with the symmetric key, which results in the recipient obtaining the original data.

## Digital Signing of Data

The goal of cryptography is three-fold: to keep data secret, to protect data against modification, and to prove the source of the data. While encryption can keep data secret and protect data against modification, only digital signing proves the source of the data, in addition to protecting the data from modification. Digital signing protects data in the following ways:

- The digital signing process uses a hash algorithm to identify whether the original data has been modified in any way.
- A digital signature applied to the resulting message digest identifies who signed the message digest. This signing prevents users from denying they signed the message digest, as only they have access to the private key used to sign the message digest. The inability for signers to deny that a signature is theirs is known as *non-repudiation*.

## The Hash Process

A hash algorithm takes a plaintext document as input and produces a mathematical result for the two inputs. This mathematical result is referred to as a hash value, message digest, or digest. If a single character is changed in the plaintext document, the resulting message digest will no longer match the original message digest.



**Note** It is technically possible for two data inputs to produce the same digest with the hash algorithm. Although possible, it is mathematically improbable.

## Hash Algorithms

The following hash algorithms are commonly used in PKI-enabled applications to produce a hash value:

- **Message Digest 5 (MD5).** This algorithm takes a message of any length and produces a 128-bit message digest.
- **Secure Hash Algorithm 1 (SHA1).** This algorithm takes data that is less than 264 bits in length and produces a 160-bit message digest.

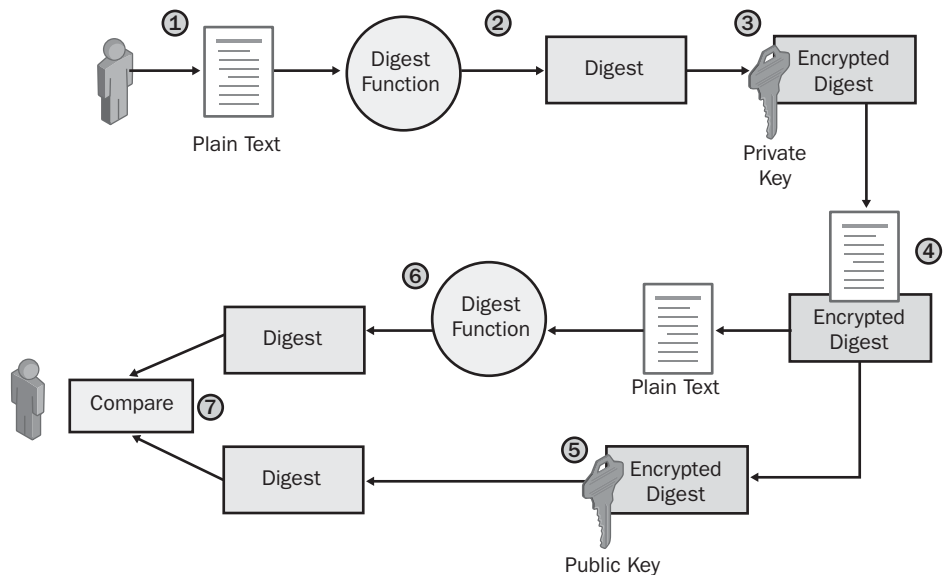


Although the SHA1 algorithm is slightly slower than MD5, it is considered harder to find two data inputs that result in the same has value when you use the SHA1 algorithm.

## Combining Asymmetric Signing and Hash Algorithms

Most applications that perform digital signing use a combination of asymmetric signing and hash algorithms. While the hash algorithm provides a mechanism to determine whether the original message has been modified in any way, the addition of a digital signature protects the resulting digest from modification and proves that the digest was created by the originator of the data.

Figure 1-5 shows the interaction of hash algorithms and asymmetric signing in the digital signing process:



**Figure 1-5** Digital signing with asymmetric signing and hash algorithms

1. The originator creates a plaintext data file.
2. The originator's software runs a hash algorithm against the plaintext message to create a message digest.
3. The digest is encrypted using the originator's private key.
4. The plaintext message and the encrypted digest are sent or made available to the recipient.



**Note** When using digital signing, no encryption is applied to the plaintext data. The plaintext can be modified, but modification invalidates the encrypted digest sent with the message.

5. The recipient decrypts the encrypted digest by using the sender's public key. The public key can be retrieved from a directory where the public key is stored (such as Active Directory) or included with the signed data.
6. The recipient runs the same hash algorithm used by the sender to create his or her own digest of the message. This digest is created against the plaintext message received from the originator.
7. The two digests are compared. If the digests differ, the message or digest has been modified during transmission.

## Case Study: Microsoft Applications and Their Encryption Algorithms

In this case study, you will research the encryption and hash algorithms supported by Encrypting File System (EFS). The research involves reviewing white papers available on the Internet (or the compact disc that accompanies this book if you do not have Internet connectivity).

### Opening the EFS White Paper

Use the following procedure to open the “Encrypting File System in Windows XP and Windows Server 2003” white paper:

1. Insert the accompanying compact disc in your CD-ROM drive.
2. Open Windows Explorer.
3. Open the folder CD:\Case Studies\Chapter1\.
4. In the CD:\Case Studies\Chapter1 folder, double-click Encrypting File System in Windows XP and Windows Server 2003.htm.



**Note** Alternatively, you can locate the “Encrypting File System in Windows XP and Windows Server 2003” white paper at [www.microsoft.com/technet/prodtechnol/winxppro/deploy/cryptfs.msp](http://www.microsoft.com/technet/prodtechnol/winxppro/deploy/cryptfs.msp).

5. From the Edit menu, click Find (on This Page).
6. In the Find dialog box, in the Find What box, type **Default Encryption Algorithm** and click Find Next.
7. In the Find dialog box, click Cancel.

## Case Study Questions

1. Based on the encryption algorithms discussed in the “Default Encryption Algorithms” section of the white paper, does EFS use symmetric or asymmetric encryption?
2. What encryption algorithm is used to encrypt EFS data on a Windows 2000 workstation?
3. What encryption algorithms can be used to encrypt EFS data on Windows XP?
4. How does the application of Windows XP, Service Pack 1, affect EFS encryption?
5. What Group Policy setting enables the use of 3DES and AES encryption algorithms?
6. What asymmetric encryption algorithm is used to protect the File Encryption Key (FEK) in EFS?
7. A developer in your organization has a laptop that dual boots between Windows 2000, Professional, and Windows XP, Professional. Both operating systems have the latest service packs and security updates. The user’s Outlook data file is encrypted, and the same EFS key pair is used in both operating systems to provide access to the Outlook data file.

This morning, your developer was unable to access the Outlook data file when working in Windows 2000, but you are still able to create new encrypted files. Fearing that the Outlook data file was corrupt, he booted into Windows XP and was able to access the data file. What is the probable cause of this problem?

## Additional Information

- Microsoft Official Curriculum, Course 2821: “Designing and Managing a Windows Public Key Infrastructure” ([www.microsoft.com/traincert/syllabi/2821afinal.asp](http://www.microsoft.com/traincert/syllabi/2821afinal.asp))
- *Cryptography and Network Security: Principles and Practice*, Third Edition, by William Stallings (<http://vig.prenhall.com/catalog/academic/product/0,4096,0130914290,00.html>)

- *Practical Cryptography*, by Niels Ferguson and Bruce Schneier ([www.wiley.com/WileyCDA/WileyTitle/productCd-047122894X.html](http://www.wiley.com/WileyCDA/WileyTitle/productCd-047122894X.html))
- “Cryptography and PKI Basics” ([www.microsoft.com/technet/prodtechnol/windows2000serv/deploy/confeat/cryptpki.mspix](http://www.microsoft.com/technet/prodtechnol/windows2000serv/deploy/confeat/cryptpki.mspix))
- “Cryptography and Microsoft Public Key Infrastructure” ([www.microsoft.com/technet/security/topics/crypto/cryptpki.mspix](http://www.microsoft.com/technet/security/topics/crypto/cryptpki.mspix))
- “Differential Cryptanalysis” ([http://en.wikipedia.org/wiki/Differential\\_cryptanalysis](http://en.wikipedia.org/wiki/Differential_cryptanalysis))
- “Specification for the Advanced Encryption Standard (AES)” (<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>)
- *Microsoft Windows Server 2000 Resource Kit*, Chapter 14: “Cryptography for Network and Information Security” ([www.microsoft.com/resources/documentation/windows/2000/server/reskit/en-us/distsys/part2/dsgcb14.mspix](http://www.microsoft.com/resources/documentation/windows/2000/server/reskit/en-us/distsys/part2/dsgcb14.mspix))
- “Encrypting File System in Windows XP and Windows Server 2003” ([www.microsoft.com/technet/prodtechnol/winxp/secure/encryptfs.mspix](http://www.microsoft.com/technet/prodtechnol/winxp/secure/encryptfs.mspix))

## Chapter 2

# Primer to PKI

Before learning how to design and implement public key infrastructure (PKI)-enabled applications with the Windows Server 2003 PKI, you'll need to know some of the basics about PKI. This chapter looks at the following building blocks of a PKI:

- **Certificate.** A digital representation of the user, computer, service, or network device on the network referred to as the subject of the certificate.
- **Certification Authority.** A computer on the network that issues certificates to users, computers, services, or network devices.
- **Certificate Revocation List.** A listing of certificates that are revoked by the CA. The revocation date and reason are recorded in the certificate revocation list.

## Certificates

Certificates provide the foundation of a public key infrastructure (PKI). These are electronic credentials, issued by a certification authority (CA), that are associated with a public and private key pair.

A certificate is a digitally signed collection of information roughly 2 to 4 KB in size. A certificate typically includes the following:

- Information about the user, computer, or network device that holds the private key corresponding to the issued certificate. The user, computer, or network device is referred to as the *subject* of the certificate.
- Information about the issuing CA.
- The public key of the certificate's associated public and private key pair.
- The names of the encryption and/or digital signing algorithms supported by the certificate.
- A list of X.509 version 3 extensions included in the issued certificate.
- Information for determining the revocation status and validity of the certificate.

The CA must ensure the identity of the requestor before issuing a certificate. Identity validation can be based on the user's security credentials or require an

in-person interview to validate requestor identity. Once identity is confirmed, the CA issues the certificate and digitally signs the certificate with its private key to prevent content modification.



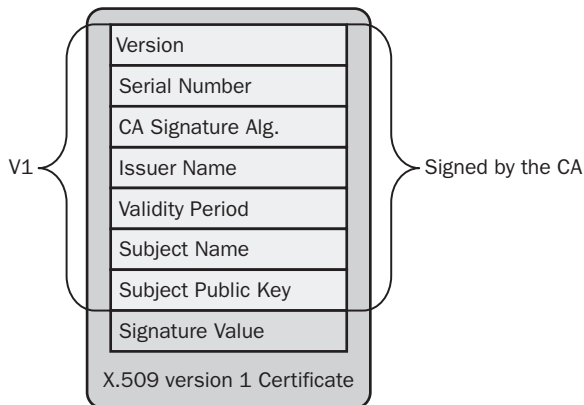
**Note** It is nearly impossible for another user, computer, network device, or service to impersonate the subject of a certificate because impersonation requires access to the certificate holder's private key. Impersonation is not possible if an attacker has access to the certificate only.

Three versions of digital certificates can be used in a PKI:

- X.509 version 1 certificates
- X.509 version 2 certificates
- X.509 version 3 certificates

## X.509 Version 1

The X.509 version 1 certificate was defined in 1988. Its advanced age means you rarely see version 1 certificates in networking. The exceptions are some of the older root certificates and older Exchange Key Management Service (KMS) deployments. The X.509 version 1 format defines the certificate fields, as shown in Figure 2-1.



**Figure 2-1** The X.509 version 1 certificate fields

An X.509 version 1 certificate contains the following fields:

- **Version.** Contains a value indicating that the certificate is an X.509 version 1 certificate.
- **Serial Number.** Provides a numeric identifier that is unique for each CA-issued certificate.
- **CA Signature Algorithm.** The name of the algorithm the CA uses to sign the contents of a digital certificate. Figure 2-1 shows the fields included when creating the digital signature.
- **Issuer Name.** The distinguished name of the certificate's issuing CA. Typically, the distinguished name is represented in an X.500 or distinguished name format specified in the X.509 specification and Request for Comment (RFC) 3280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile."
- **Validity Period.** The range of time for which the certificate is considered valid. In some offerings, the validity period is split into two fields: Valid From and Valid To.
- **Subject Name.** The name of the computer, user, network device, or service represented by the certificate. Typically, the subject name is represented in an X.500 or distinguished name format specified in the X.509 specification, but it can include other name formats, such as an RFC 822, "Standard for the Format of ARPA Internet Text Messages," e-mail name format.
- **Subject Public Key.** The public key of the certificate holder. The public key is provided to the CA in a certificate request and is included in the issued certificate. This field also contains the public key algorithm identifier, which indicates which public key algorithm is used to generate the key pair associated with the certificate.
- **Signature Value.** Contains the signature value that results from the CA signature algorithm used to sign the digital certificate.

In a version 1 certificate, the Issuer Name and Subject Name fields allow certificates to be organized into a *chain* of certificates that starts at the certificate issued to a user, computer, network device, or service and terminates with a root CA certificate.

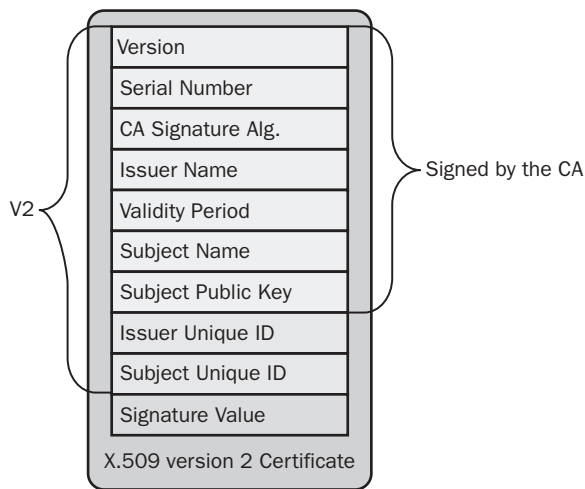


**Note** Certificate chaining is fully discussed in Chapter 9, “Certificate Validation.”

## X.509 Version 2

Although the X.509 version 1 certificate format provides basic information about the certificate holder, the format offers little information about the certificate issuer. By including only the issuer, issuer name, CA signature algorithm, and signature value, the version 1 format does not provide any provisions for CA renewal.

When a CA’s certificate is renewed, two certificates possess the same Issuer Name field value. Likewise, it is possible for another organization to create a CA with the same issuer name. To address this, the X.509 version 2 certificate format was introduced in 1993. The version 2 format introduced two new fields to the certificate. (See Figure 2-2.)



**Figure 2-2** The X.509 version 2 certificate fields

The X.509 version 2 certificate format introduced the following fields:

- Issuer Unique ID.** An optional field that contains a unique identifier, typically a hexadecimal string, for the issuing CA as defined by the issuing CA. When a CA renews its certificate, a new Issuer Unique ID is generated for that certificate version.



- **Subject Unique ID.** An optional field that contains a unique identifier, typically a hexadecimal string, for the certificate's subject as defined by the issuing CA. If the subject is also a CA, this unique identifier is placed in the Issuer Unique ID.



**Note** In addition to introducing the Issuer Unique ID and Subject Unique ID fields, the X.509 version 2 certificate's Version field changed to a value of 2 to indicate the version number.

The Issuer Unique ID and Subject Unique ID fields improved the certificate chaining process. The process now finds the CA certificate by matching the issuer name in the issued certificate to the subject name in the CA certificate and performs a second check by matching the Issuer Unique ID in the issued certificate with the Subject Unique ID of the CA certificate.

This additional level of matching allows a distinction between CA certificates when the CA renews a certificate. This method also allows for a distinction between CAs with the same subject name. (The likelihood of CA certificates with the same name increases when simple names are used—for example, CN=Root CA rather than CN=Fabrikam Industries Inc. Corporate Root CA,O=Fabrikam,C=NL.)

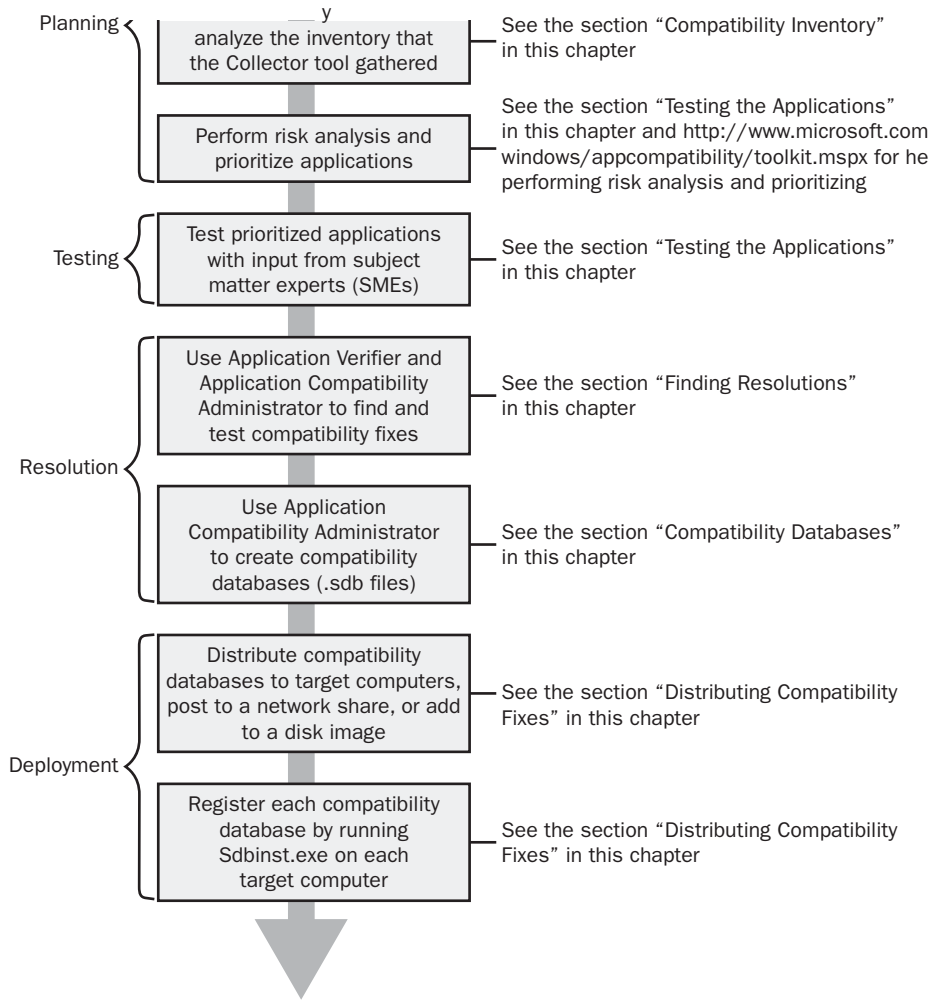
Although the addition of the Issuer Unique ID and Subject Unique ID aids in chain building, it's still possible for collisions to occur when two certificates share the same Subject Name and Subject Unique ID fields.



**Note** Although the X.509 version 2 format improved on the version 1 format, the standard was not widely supported. In fact, RFC 3280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," recommends the omission of these X.590 version 2 fields.

## X.509 Version 3

Released in 1996, the X.509 version 3 format introduced *extensions* to address the problems associated with matching the Issuer Unique ID with the Subject Unique ID, as well as other certificate-validation issues. An X.509 version 3 certificate can contain one or more certificate extensions. (See Figure 2-3.)



**Figure 2-3** The X.509 version 3 certificate fields

Each extension in an X.509 version 3 certificate is composed of three parts:

- **Extension Identifier.** An object identifier (OID) that indicates the format and definitions of the extension.
- **Criticality Flag.** An indicator that identifies whether the information in an extension is important. If an application cannot recognize the critical extension, the certificate cannot be accepted or used. If the criticality flag is not set, an application can use the certificate even when the application does not recognize the extension.

- **Extension Value.** The value assigned to the extension. The value varies depending on the specific extension.

In an X.509 version 3 certificate, the following certificate extensions can exist:

- **Authority Key Identifier.** This extension can contain one of two values. The value can be either
  - The subject of the CA and serial number of the CA certificate that issued the current certificate.
  - A hash of the public key of the CA certificate that issued the current certificate.
- **Subject Key Identifier.** This extension contains a hash of the current certificate's public key.



**Note** The use of the Authority Key Identifier and Subject Key Identifier in certificate chaining and validation is described in Chapter 9, “Certificate Validation.”

- **Key Usage.** A CA, user, computer, network device, or service can have more than one certificate. The Key Usage extension defines the security services for which a certificate can be used. The options can be used in any combination and can include the following:
  - **Digital Signature.** The public key can be used to verify signatures. This key is also used for client authentication and data-origin validation.
  - **Non-Repudiation.** The public key can be used to validate the signer's identity, preventing a signer from denying that he/she signed a package.
  - **Key Encipherment.** The public key can be used for key transport for processes, such as symmetric key exchange. This Key Usage value is used when an RSA key is used for key management.
  - **Data Encipherment.** The public key can be used to directly encrypt data, rather than exchanging a symmetric key for data encryption.
  - **Key Agreement.** The public key can be used for key transport for processes such as symmetric key exchange. This value is used when a Diffie-Hellman key is used for key management.

- **Key Cert Sign.** The public key can be used to verify a certificate's signature.
- **CRL Sign.** The public key can be used to verify a CRL's signature.
- **Encipher Only.** This value is used in conjunction with the Key Agreement Key Usage extension. The resulting symmetric key can only be used for data encryption.
- **Decipher Only.** This value is used in conjunction with the Key Agreement Key Usage extension. The resulting symmetric key can be used only for data decryption.
- **Private Key Usage Period.** This extension allows a different validity period to be defined for the private key of a key pair. The Private Key Usage Period can be set to a period shorter than the certificate's validity period. This gives the private key the ability to sign documents for a shorter period (say, one year), while the public key can be used to validate the signature for the certificate's entire five-year validity period.
- **Certificate Policies.** This extension describes the policies and procedures used to validate a certificate's subject before the certificate is issued. Certificate policies are represented by OIDs. Optionally, a certificate policy can include a policy qualifier, which is typically a URL that describes, in text, the policies and procedures.
- **Policy Mappings.** This extension allows for policy-information translation between two organizations. For example, imagine that one organization defines a certificate policy named Management Signing, which is included in certificates used for signing for large purchase orders. Another organization can have a certificate policy named Large Orders, which also is used to sign large purchase orders. Policy mapping allows the two certificate policies to be deemed equivalent.



**Note** Policy mapping typically requires that the participating organizations' legal departments inspect each certificate policy. The policies can be deemed equivalent only after the legal departments are satisfied.

- **Subject Alternative Name.** This extension provides a list of alternate names for the certificate's subject. While the subject can include the subject name in an X.500 distinguished name format, the Subject Alternative Name allows for other representations, such as a User Principal Name (UPN), e-mail address, IP address, or DNS name.

- **Issuer Alternative Name.** This extension provides a list of alternate names for the issuing CA. Though it is not typically implemented, the Issuer Alternative Name extension can contain the e-mail name associated with a CA.



**Note** The Subject Alternative Name and Issuer Alternative Name extensions can be either critical or noncritical. RFC 3280 defines that if the Subject field is not empty, these extensions can be marked noncritical. If the Subject field is empty, these extensions must be marked critical to allow applications to inspect the name formats.

- **Subject Dir Attribute.** This extension can include any attributes from an organization's X.500 or Lightweight Directory Access Protocol (LDAP) directory. For example, the country attribute from a directory can be included in the Subject Dir Attribute extension. This extension can contain multiple attributes from the organization's directory. For each attribute, the OID and its corresponding value must be included.
- **Basic Constraints.** This extension allows a certificate to designate whether the certificate is issued to a CA or to a user, computer, network device, or service. Also, the Basic Constraints extension includes a path length constraint, which limits how many subordinate CAs can exist below a specific CA's issued certificate.
- **Name Constraints.** This extension allows an organization to designate which name spaces are allowed or disallowed in a CA-issued certificate. A separate name constraint must be defined for each name-space format used in certificates. For example, separate constraints are required for LDAP names versus e-mail names.
- **Policy Constraints.** This extension can be included in CA certificates. The extension can prohibit policy mapping between CAs or require that each certificate in a certificate chain includes an explicit certificate policy OID.
- **Enhanced Key Usage.** This extension indicates how a certificate's public key can be used. The Enhanced Key Usage extension provides additional information beyond the general purposes defined in the Key Usage extension. For example, OIDs exist for Client Authentication (1.3.6.1.5.5.7.3.2), Server Authentication (1.3.6.1.5.5.7.3.1), and Secure E-mail (1.3.6.1.5.5.7.3.4). When a certificate is presented to an application, an application can require the presence of an Enhanced Key Usage OID specific to that application.



**Note** Enhanced Key Usage OIDs are also used when defining qualified subordination constraints. These constraints are discussed in Chapter 13, “Creating Trust Between Organizations.”

- **CRL Distribution Point** This extension contains one or more URLs where the issuing CA’s base CRL is published. If revocation checking is enabled, an application will use the URL to retrieve an updated version of the CRL. URLs can use Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), or LDAP.
- **Authority Info Access.** This extension contains one or more URLs where the issuing CA’s certificate is published. An application uses the URL when building a certificate chain to retrieve the CA certificate if it does not exist in the application’s certificate cache.
- **Inhibit Any Policy.** This extension is included in a CA certificate to inhibit the use of the All Issuance Policies OID (2.5.29.32.0) in subordinate CA certificates. This extension prevents the All Issuance Policies OID from being considered a match to a specific certificate policy OID in a subordinate CA certificate. The value of this extension defines the number of certificates that can appear below the CA certificate before the All Issuance Policies OID is not recognized.
- **Freshest CRL.** This extension contains one or more URLs where the issuing CA’s delta CRL is published. The delta CRL contains only the certificates revoked since the last base CRL was published. If revocation checking is enabled, an application will use the URL to retrieve an updated version of the delta CRL. URLs can use the HTTP, LDAP, or FTP protocols.



**Note** The use of base CRLs and delta CRLs is discussed in Chapter 9, “Certificate Validation.”

- **Subject Information Access.** This extension contains information on how to access additional details about the certificate’s subject. If the certificate is a CA certificate, the information can include particulars about the certificate validation services or the CA policy. If the certificate is issued to a user, computer, network device, or service, the extension can contain information about the services offered by the certificate subject and how to access those services.



**Note** In addition to introducing the extensions listed here, the X.509 version 3 certificate's Version field changed to a value of 3 to indicate the version number.

## Certification Authorities

A CA is an essential component of the Microsoft PKI solution. In a Windows Server 2003 network, a CA is a Windows Server 2003 computer with Certificate Services installed. It performs the following tasks:

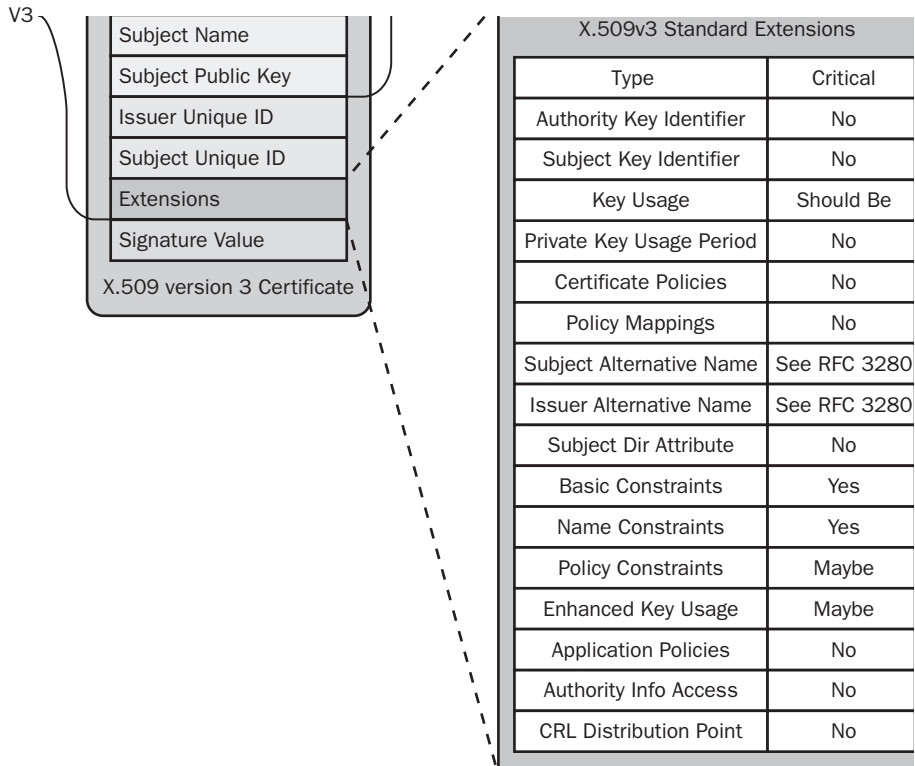
- **Verifies the identity of a certificate requestor.** The CA must validate the requestor's identity before it can issue a certificate. Validation can range from ensuring that the requestor has the necessary permissions to ask for a specific type of certificate to having a certificate manager perform a face-to-face interview with the certificate requestor.
- **Issues certificates to requestors.** After the requestor's identity is validated, the CA issues the requested type of certificate to the user, computer, network device, or service. The type of certificate requested determines the content of the issued certificate. For example, a Web server certificate request results in a certificate that can only be used by the Web server to set up Secure Sockets Layer (SSL) connections.
- **Manages certificate revocation.** The CA publishes a CRL at regularly scheduled intervals. The CRL contains a list of serial numbers of certificates that are revoked and the reason codes for each revocation.

In an enterprise PKI, more than one CA is typically implemented. The CAs are organized into a CA hierarchy consisting of a single root CA and several other subordinate CAs, as shown in Figure 2-4.

In Figure 2-4, the CAs are organized in a *root CA hierarchy*, which increases security and scalability of a CA hierarchy by allowing nonissuing CAs to be removed from the network. If the root CA and second-tier CAs in a root CA hierarchy are removed from the network, the offline CAs are protected from network-sourced attacks.



**Note** Do not assume that a root CA hierarchy always implements offline CAs. It is possible to deploy a root CA hierarchy without offline CAs, but it is not recommended because of security issues.



**Figure 2-4** CA hierarchy roles

A root CA hierarchy allows the delegation of administration to different business units or divisions within an organization. Common-criteria role separation allows the designation of CA management roles at each CA in the hierarchy, giving different administration groups the ability to manage one CA in the CA hierarchy but not others.



**Note** The root CA hierarchy is supported by all leading commercial CA vendors, including RSA, Thawte, and VeriSign. The root CA hierarchy is also supported by most applications and network devices, allowing for interoperability with a variety of applications and network devices.

## Root CA

A root CA is the topmost CA in a CA hierarchy. In a PKI, the root CA acts as the trust point for certificates issued by CAs in the hierarchy. This means that if a certificate can be traced up through the CA hierarchy to a root CA that is trusted by a user, computer, network device, or service, the certificate is considered trusted.



A root CA is special in that its certificate is self-issued. This means that the certificate's Issuer Name and Subject Name fields contain the same distinguished name. The only way to validate whether a root certificate is valid is to include the root CA certificate in a trusted root store. The trusted root store contains the actual root CA certificate to designate that the certificate is trusted.



**Note** If a self-signed certificate is not included in the trusted root store, it is considered a nontrusted root CA. If revocation checking is enabled in an application, a certificate that is chained to a nontrusted root CA is considered nontrusted.

The root CA can issue certificates to other CAs or to users, computers, network devices, or services on the network. When the root CA issues a certificate to another network entity, the root CA certificate signs the certificate with its private key to prevent content modification and to indicate that the root CA issued the certificate.



**Note** Typically, the root CA only issues certificates to other CAs, not to users, computers, network devices, or services on the network.

## Intermediate CA

An ***intermediate CA*** is a CA that is subordinate to another CA and issues certificates to other CAs in the CA hierarchy. The intermediate CA can exist at any level in the CA hierarchy, except at the root CA level.



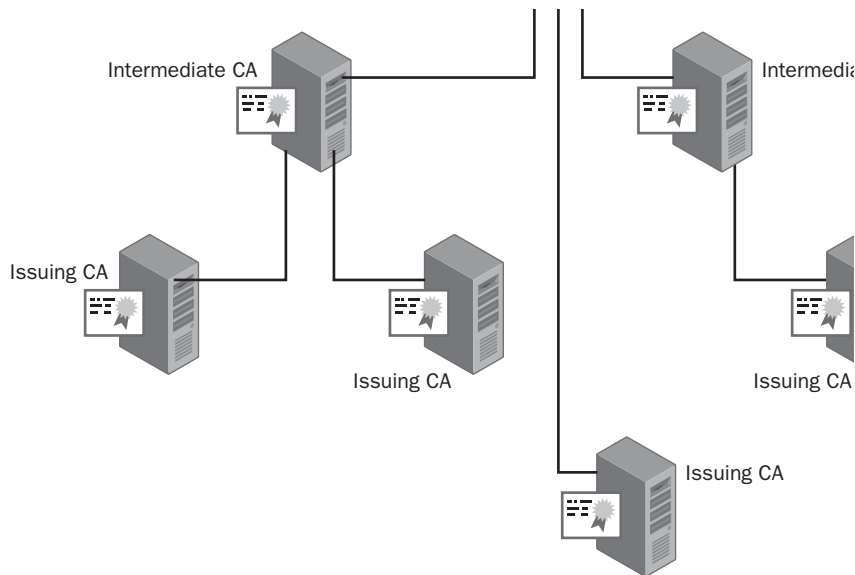
**Note** The CA that issues a certificate to another CA is often referred to as a *parent CA*. For example, a root CA that issues a certificate to an intermediate CA is referenced as the parent CA to the intermediate CA. The intermediate CA is also referred to as a *subordinate CA*, as it is directly subordinate to the parent CA in the hierarchy.

## Policy CA

A special category of intermediate CA is a *policy CA*. A policy CA describes the policies and procedures an organization implements to validate certificate-holder identity and secure the CAs in the CA hierarchy. A policy CA only issues certificates to

other CAs in the hierarchy. It is assumed that all CAs that are subordinate to a policy CA—whether directly subordinate or two or more levels below the policy CA—enforce the policies and procedures defined at the policy CA.

If an organization must implement multiple policies and procedures when issuing certificates, multiple policy CAs must exist in the CA hierarchy. (See Figure 2-5.)



**Figure 2-5** Policy CA example

In this example, two policy CAs exist in the CA hierarchy. The Internal Policy CA defines the policies and procedures used to validate the identity of certificates issued to employees. The two issuing CAs (Americas CA and Europe CA), which are directly subordinate to the Internal Policy CA, must enforce the policies and procedures defined by the Internal Policy CA.

The External Policy CA defines the policies and procedures used to validate identity and secure the process of issuing certificates to nonemployees. The Customers CA, as a subordinate CA to the External Policy CA, must enforce the policies and procedures defined by the External Policy CA.



**Note** More than one policy or procedure can be defined at a policy CA, but it is also valid to implement one policy CA for each policy or procedure applied by the organization.

## Issuing CA

An issuing CA issues certificates to users, computers, network devices, or services on the network. An issuing CA is typically located on the third tier of a CA hierarchy, but it can exist on the second level, as shown in Figure 2-4.

As mentioned, an issuing CA must enforce any policies and procedures defined by a policy CA that exists between the issuing CA and the root CA in the CA hierarchy.

## Certificate Revocation Lists

In some cases, a CA must revoke a certificate before the certificate's validity period expires. When a certificate is revoked, the CA includes the serial number of the certificate and the reason for the revocation in the CRL.

### Types of CRLs

Windows Server 2003 supports the issuance of two types of CRLs: base CRLs and delta CRLs.



**Note** Windows Server 2003 does not support the issuance of indirect (or partitioned) CRLs.

A *base CRL* contains the serial numbers of all certificates revoked on a CA, as well as the reason for each revocation specific to a given private key used by the CA. The base CRL contains all certificates signed by a CA's specific private key. If a CA's certificate is renewed with a new key pair, a new CRL is generated that includes only revoked certificates signed with the CA's new private key.

A *delta CRL* contains only the serial numbers and revocation reasons for certificates revoked since the last base CRL was published. A delta CRL is implemented to provide more timely revocation information from a CA and to decrease the amount of data downloaded when retrieving a CRL. When a new base CRL is published, the revoked certificates in the delta CRL are rolled into the base CRL. The next delta CRL will only contain certificates revoked since the new base CRL was published.

The delta CRL is much smaller than a base CRL because only the most recent revocations are included. The base CRL, which contains all revoked certificates, can be downloaded less frequently.



**Note** If you implement delta CRLs, you must still download the base CRL. It is the combination of the base CRL and the delta CRL that provides the complete information on all revoked certificates.

## Revocation Reasons

When a certificate is revoked, the CRL entry can contain further information about the revocation. The reason codes can include:

- **Key Compromise.** The private key associated with the certificate has been stolen or otherwise acquired by an unauthorized person, such as when a computer is stolen or a smart card is lost.
- **CA Compromise.** The private key of a CA has been compromised. This can occur when the computer running Certificate Services or the physical device that stores the CA's private key is stolen. If a CA's certificate is revoked, every certificate issued by the CA is also considered revoked because the CA that issued the certificates is no longer considered trustworthy.
- **Affiliation Changed.** The subject of the certificate, typically a user, is no longer affiliated with an organization.
- **Superseded.** The revoked certificate has been replaced by a new certificate. This can occur because of changes in the extensions in a certificate or the certificate's subject name changes.
- **Cessation of Operation.** The certificate's subject has been decommissioned. This can take place when a Web server is replaced by a new Web server with a new name. Likewise, this can occur when a merger takes place and the previous DNS name is decommissioned, requiring replacement of all Web server certificates.
- **Certificate Hold.** A revocation where a certificate is determined to be temporarily revoked. This can occur when an employee takes a leave of absence. The Certificate Hold reason is the only revocation reason that allows a certificate to be unrevoked.



**Note** Although Certificate Hold allows a certificate to be unrevoked, use of the Certificate Hold reason code is not recommended, as it can be difficult to determine if a certificate was valid at a specific time.

- **Remove from CRL.** This reason is used when a certificate is unrevoked after being revoked with the Certificate Hold reason. This revocation reason is only used in delta CRLs to indicate that a certificate revoked in the base CRL is unrevoked in the delta CRL.
- **Unspecified.** If a certificate is revoked without providing a revocation reason, the unspecified reason is automatically included in the CRL.



**Note** For more information about certificate revocation reason codes, see RFC 3280.

## Case Study: Inspecting an X.509 Certificate

In this case study, you will examine a sample certificate and answer questions related to the fields and extensions included in the certificate.

### Opening the Certificate File

Use the following procedure to open the sample certificate file on the compact disc that accompanies this book.

1. Insert the compact disc in your CD-ROM drive.
2. Open Windows Explorer.
3. Open the folder CD:\Case Studies\Chapter2\
4. In the CD:\Case Studies\Chapter2 folder, double-click Samplecertificate.cer.
5. In the Certificate dialog box, click the Details tab.
6. From the resource materials for this chapter, open the Samplecertificate.cer file.

### Case Study Questions

1. What version is the certificate?
2. What is the name of the issuing CA?
3. What is the subject name of the certificate?
4. Are any other names included in the certificate for the subject?
5. What is the length of the public key associated with the certificate?
6. What other X.509 extensions are included in the sample certificate?
7. Where is the CRL published when revocation checking is performed against the certificate?

## Additional Information

- Microsoft Official Curriculum, Course 2821: “Designing and Managing a Windows® Public Key Infrastructure” (*[www.microsoft.com/traincert/syllabi/2821afinal.asp](http://www.microsoft.com/traincert/syllabi/2821afinal.asp)*)
- RFC 3280, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” (*<http://www.faqs.org/rfcs/rfc3280.html>*)

## Chapter 3

# Policies and PKI

A public key infrastructure (PKI) is only as secure as the policies and procedures that are implemented by an organization in conjunction with its PKI. Three policy documents directly affect PKI design:

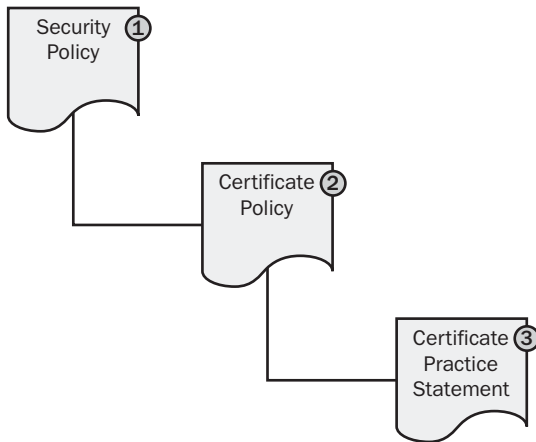
- **Security policy.** A security policy is a document that defines an organization's standards in regard to security. The policy usually includes the assets an organization considers valuable, potential threats to those assets, and, in general terms, measures that must be taken to protect these resources.
- **Certificate policy.** A certificate policy is a document that describes the measures an organization will use to validate the identity of a certificate's subject. Validation might require a requestor-provided account and password combination submitted to the organization's directory or photo identification and submission to a background check through a registration authority (RA) process.
- **Certificate practice statement (CPS).** A CPS is a public document that describes how a certification authority (CA) is managed by an organization to uphold its security and certificate policies. A CPS is published at a CA and describes the operation of the CA.

Security policies, certificate policies, and CPSs are typically created by members of an organization's legal, human resources, and information technology (IT) departments. The PKI design must enforce these policies.



**Warning** Certificate policies and CPSs are used by other organizations to determine how well they trust certificates issued by an organization's CA hierarchy. You trust a certificate from another organization when you allow that certificate to be used on your network for signing or encryption purposes. Deploying a PKI without implementing certificate policies and CPSs can result in a PKI that causes your organization to be deemed untrustworthy by other organizations.

A dependency exists between the security policy, certificate policy, and CPS in a PKI. (See Figure 3-1.)



**Figure 3-1** The dependency between the security policy, certificate policy, and certificate practice statement (CPS)

An organization must first develop a security policy, which defines the organization's security standards. Next, a certificate policy is drafted to enforce and reflect the organization's security policy. Finally, the CPS defines the CA's management procedures that enforce the certificate policy.



**Note** Security policies, certificate policies, and CPSs are typically legal documents that must be reviewed by an organization's legal department or legal representatives before publication to ensure that the documents are enforceable and do not misrepresent the organization's intent.

## Security Policy

The design of a PKI starts with an inspection of the organization's security policy. A PKI designer uses a security policy to answer the following questions:

- **What data should be secured with certificates?** Not all applications support certificate-based security. Typically, a security policy defines classes of data within the organization and measures that must be taken to protect that data when stored and when transmitted across a network. With a PKI in place, these measures can include the use of protocols such as Secure Sockets Layer (SSL) or Internet Protocol Security (IPSec) to protect transmitted data and Encrypting File System (EFS) to protect stored data.



- **What measures must be taken to protect the private keys associated with a certificate?** Measures can include storing the certificate on a smart card, protecting a CA's private key by implementing hardware security modules (HSMs), or preventing the export of a certificate's private key.
- **What measures must be taken to validate the identity of a certificate requestor?** Whoever has access to a certificate's private key is considered to be the person identified in the certificate's subject. An organization might want to use certificates for applications that require higher trust. For example, background checks can be required prior to issuance of a certificate used to digitally sign for high-value purchases.

## Defining Effective Security Policies

A security policy defines an organization's security standards. An organization typically has several security policy documents that provide comprehensive definitions of security issues, the risks and threats faced by the organization, and the measures that must be taken to protect the organization's data and assets.



**Note** An organization must do more than just define security policies. It must ensure that it deploys security solutions to enforce the security policies and it must ensure that employees are aware of those security policies and their roles and responsibilities in maintaining security.

Once an organization defines its security policies, an initial assessment must be performed to identify measures that enforce those policies. Once these measures are identified, a *gap analysis* determines whether additional measures should be implemented to meet the defined security policies. After proper planning, the security policy implementation process can begin.

An organization should periodically review its security policies and the measures taken to enforce them to determine whether modifications are necessary. Modifications might involve updating security policies or revising the processes and procedures that enforce them.

## Resources for Developing Security Policies

Two of the most commonly used resources for defining a security policy are ISO 17799/BS 7799, "Code of Practice for Information Security Management," and RFC 2196, "The Site Security Handbook."



**Note** ISO 17799 is an International Organization for Standardization document that is based on the British Standards 7799 document.

ISO 17799, available for purchase at <https://www.bspsl.com/secure/iso17799/software/cvm.cfm>, provides detailed information and recommendations for developing enforceable security policies. Several Web sites provide security policy samples based on the intent and recommendations of ISO 17799.

RFC 2196, “Site Security Handbook,” available at [www.ietf.org/rfc/rfc2196.txt](http://www.ietf.org/rfc/rfc2196.txt), is another guide for developing security policies. Although directed more toward computer security policies, the RFC describes several types of resources that should be covered in an overall security policy, as well as recommendations for securing those resources.

## Defining PKI-Related Security Policies

Using ISO 17799 as a guide for developing security policies, you should consider updating or creating security policies for the following areas:

- **Organizational security.** Establish enforceable security policies for an organization. ISO 17799 is especially helpful when an organization does not have security policies in place prior to starting a PKI design.
- **Organizational security infrastructure.** Ensure the existence of security policies that recommend the implementation of a single organization-wide PKI. An organizational PKI is easier to manage than several project-based CAs. For example, an organization should not deploy separate CA implementations for a virtual private network (VPN), Secure/Multipurpose Internet Mail Extensions (S/MIME), and wireless projects. An enterprise PKI that provides certificates for all applications and services is preferred.
- **Asset classification and control.** Identify classes of assets that require public key encryption, digital signing, or other PKI-related technologies to ensure security. PKI-related security can be applied to both data storage and transmission.
- **Personnel security.** Include job descriptions and requirements for members of the PKI administration team in security policies. Requirements can include mandatory background checks for all administrators, tasks and procedures that must be followed, and any agreements or policies that administrators must sign when accepting their positions.

- **Physical and environmental security.** Ensure that the security policy includes requirements for physical security measures to protect CAs and their deployment in a PKI. Different security measures can be required for offline versus online CAs.
- **Communications and operations management.** Define managerial and operational roles for your PKI. These can include CA administrators, certificate managers, backup operators, auditors, certificate template designers, and key recovery agents.
- **Access control.** Define what measures will be taken to secure access to a CA. These measures might include providing certificate enrollment access through controlling network interfaces on the CA, manually approving Web-based enrollment requests, or placing the physical CA in a server room with keycard access. Access control can dictate what forms of authentication are required to access data. For example, some asset classifications can require two-factor authentication (something you have and something you know) before access is permitted.
- **Change control process.** Establish what measures will be taken to maintain and modify a PKI after deployment.
- **Business continuity management.** Define measures that will ensure recovery of the PKI in the event of a disaster. These measures should include actions to be taken in advance of a catastrophe so that a CA can be recovered, what information must be documented about the CA configuration, and who will perform the recovery.
- **Compliance.** Provide recommendations to ensure that the implemented PKI enforces security policies that affect it. Nonconformance with security policies can devalue a PKI-issued certificate to the point that all certificates must be revoked and reissued to ensure compliance and trust of other organizations.

## Certificate Policy

A certificate policy describes the measures taken to validate a certificate's subject prior to certificate issuance. For many organizations, it is the certificate-issuance policy that determines whether the presented certificate will be trusted.

For example, an organization is more likely to trust a certificate issued after a requestor presents photo identification than a certificate issued based on a user knowing an account and password combination.

## Contents of a Certificate Policy

A certificate policy should include the following information:

- **How the user's identity is validated during certificate enrollment.** Is identity provided by an account and password combination or must requestors present themselves for face-to-face interviews? If interviews are required, what forms of identification must requestors present for validation?
- **The certificate's intended purpose.** Is the certificate used for authentication on the network or for signing purchase orders? If the certificate is used for signing purchase orders, is there a maximum value allowed? These questions should be addressed in the certificate policy.
- **The type of device upon which the certificate's private key is stored.** Is the private key stored on the computer's local disk in the user's profile or on a hardware device such as a smart card? Other measures such as implementing strong private key protection or requiring a password to access the private key can be described in conjunction with this information.
- **The subject's responsibility for the private key associated with the certificate in the event that the private key is compromised or lost.** Is the user responsible for any actions performed using the acquired private key if the private key is compromised or a backup of the private key is lost? This decision can lead to preventing the archiving or export of the private key associated with the certificate.
- **Revocation policies, procedures, and responsibilities.** Under what circumstances will your organization revoke an issued certificate before its validity period expires? This decision will determine what actions or events will lead to revocation of a certificate, how the revocation process is initiated, and who performs the actual revocation procedure.

## Certificate Policy Example

An excellent example of certificate policy is the X.509 Certificate Policy for the United States Department of Defense (DoD), available at [www.defenselink.mil/nii/org/sio/ia/pki/DoD\\_CP\\_V60\\_31May2002.pdf](http://www.defenselink.mil/nii/org/sio/ia/pki/DoD_CP_V60_31May2002.pdf).

The DoD defines five classes of certificates in its certificate policy document. The distinction between the various classes is based on the following variables:

- The measures taken to validate the subject's identity
- The value of transactions allowed for a certificate class
- The type of storage required for the private key material

A combination of these three variables leads to the following certificate classes:

- **DoD Class 2.** Users prove identity by providing a user name and password for an account in the organization's authoritative directory. Once a valid user name and password are provided, a certificate is issued. The certificate is typically stored on the hard drive of the computer where the certificate request is generated. A DoD Class 2 certificate can be used for:
  - Digital signatures for administrative data or day-to-day work on any network.
  - Key exchange for high-value data on an encrypted network or confidentiality of low-value information on nonencrypted networks.
- **DoD Class 3.** Users prove identity by providing at least one piece of official federal government photo identification or two credentials issued by other entities, with one of the documents being a photo ID (such as a driver's license). The private key associated with the certificate is still stored on the user's hard disk, but the increased subject validation allows the private key to be used for medium-value transactions on a public network.
- **DoD Class 3 Hardware.** A DoD Class 3 Hardware certificate uses the same subject validation process as a DoD Class 3 certificate. The difference is that the private key material and certificate are exported from the user's hard disk to a hardware token, such as a USB token. The movement of the private key to a hardware device increases the security of the private key.



**Note** Once the private key is successfully transferred to a hardware device, the private key should be deleted from the computer's hard drive to prevent unauthorized access.

- **DoD Class 4.** A DoD Class 4 certificate requires presentation of the same photo identification as the DoD Class 3 and DoD Class 3 Hardware certificates. The difference is that the private key pair is not generated on the local hard disk but on a hardware two-factor device, such as a smart card. The increased security of the key pair associated with the certificate results in the certificate being valid for high-value transactions on public networks.
- **DoD Class 5.** Currently, there is no PKI that meets the subject-identification requirements for a DoD Class 5 certificate. In the future, a DoD Class 5 certificate will require biometric validation of the certificate's subject. This can include retinal scans, fingerprint matches, or even DNA matching. A DoD Class 5 certificate can be used to secure classified materials on public networks.



**Note** The DoD classifications do not assign actual values to low-value, medium-value, or high-value transactions. Rather than providing predetermined values that can become dated, general terms are used to allow value modification without requiring certificate policy modification.

## Certificate Practice Statement (CPS)

A CPS defines the measures taken to secure CA operations and the management of CA-issued certificates. You can consider a CPS to be an agreement between the organization managing the CA and the people relying on the certificates issued by the CA.

By reviewing a CA's CPS—a public document that should be readily available to all participants on the Internet—a relying party can determine whether the certificates issued by that CA meet its security requirements. The CPS contains the following information:

- How the CA will enforce the measures necessary to validate the certificate's subject, as required by the certificate policy.
- The liability of the organization in the event that an act of fraud is performed against the service protected by the certificate and the fault is found to be associated with the certificate.
- The circumstances under which a certificate can be revoked before its expiration.

When a certificate is issued by a CA that follows a CPS, the CA's certificate (or that of its parent CA) includes a URL pointer to the CPS. In the CA's certificate, the CPS is viewed by clicking the Issuer Statement button on the General tab of the certificate, as shown in Figure 3-2.



**Figure 3-2** A CA certificate that references a CPS



**Note** When a CPS is included in a CA certificate, it is applicable to that CA and all subordinate CAs in the CA hierarchy. This means that the practices defined in the CPS must be implemented by that CA and all subordinate CAs.

RFC 2527, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework,” available at [www.ietf.org/rfc/rfc2527.txt](http://www.ietf.org/rfc/rfc2527.txt), recommends a standard CPS format to ensure compatibility between organizations and promote a stronger degree of trust of an organization’s CPS by other companies. The RFC recommends the following eight sections:

- Introduction
- General Provisions
- Identification and Authentication
- Operational Requirements
- Physical, Procedural, and Personnel Security Controls
- Technical Security Controls
- Certificate and Certificate Revocation List (CRL) Profiles
- Specification Administration



**Note** RFC 2527 recommends that the same format be used for both certificate policies and CPSs. The X.509 certificate policy for the United States Department of Defense implements the eight sections discussed here. Differences between the certificate policy and the CPS are mainly related to the documents’ focus. A certificate policy focuses on subject validation and is often compared between organizations to find similar policies, whereas a CPS describes the operations of the CA to enforce the implemented certificate policies.

## CPS: Introduction

The introduction provides an overview of the CA, as well as the types of users, computers, network devices, or services that will receive certificates. Should another organization have any questions regarding the information published in the CPS, the introduction also provides contact information.

## CPS: General Provisions

The general provisions provide legal definitions for:

- **The obligations of the company managing the CA, as well as the obligations of the certificate holders.** These obligations can include who is responsible for the private key material and the measures taken to identify the subject of the certificate.
- **The liability of the organization that manages the CA.** The liability defines the maximum value of transactions for which the CA-issued certificates can be used. For example, if the liability is defined as \$1,000, transactions for a greater value are insured only up to the maximum value of \$1,000.
- **The laws applicable to the operation and management of the CA.** For example, a CA can enforce the laws of the state of Nevada, rather than the state of New York. This defines how certain actions might be interpreted if brought to litigation.
- **The fees required to receive a certificate issued by the CA.** Some commercial CAs have a fee scale for the issuance of a certificate. If fees are involved, this section should detail the associated fees for each class of certificate offered by the CA.
- **How audits of the CA are performed to ensure that the CPS-defined tasks and measures are performed.** For example, if an independent auditing firm is brought in once a year to evaluate PKI-related processes, the CPS should define how often audits are performed and what tests are performed by the auditing firm.

## CPS: Identification and Authentication

This section describes the measures taken to validate a requestor's identity prior to certificate issuance. It must reflect the certificate policy or policies implemented at the CA and detail identification procedures for:

- **Initial registration for a certificate.** The measures taken to validate the identity of the certificate requestor.
- **Renewal of a certificate.** Are the measures used for initial registration repeated when a certificate is renewed? In some cases, possession of an existing certificate and private key is sufficient proof of identity to receive a new certificate at renewal time.
- **Replacement of a revoked certificate.** If a certificate must be replaced because of key compromise, such as a stolen laptop, what measures will be taken to ensure that the authorized user, not the person who stole the laptop, receives a new certificate?



- **Requests for revocation.** When a certificate must be revoked, what measures will be taken to ensure that the requestor is authorized to request revocation of a certificate?



**Note** A CA can implement more than one certificate policy, as long as the CA's procedures and operations allow enforcement of each certificate policy. To implement multiple certificate policies, separate subsections can be defined, one for each certificate policy.

## CPS: Operational Requirements

This section defines the operating procedures for CA management, issuance of certificates, and management of issued certificates. It is detailed in the description of the management tasks. Operating procedures described in this section can include the following:

- **Certificate application.** The application process for each certificate policy supported by a CA should be described. Applications can range from the use of autoenrollment to distribute certificates automatically to users or computers, to a detailed procedure that pends certificate requests until the requestor's identity is proven through ID inspection and background checks.
- **Certificate issuance.** Once the identity of a certificate requestor is validated, what is the procedure to issue the certificate? The process can range from simply issuing the certificate in the CA console to recording the certificate requestor's submitted identification in a separate database maintained by a registration.
- **Certificate acceptance.** When a certificate is issued to a computer or user, what procedures must be performed to install the certificate on the user's computer or a certificate-bearing device, such as a smart card?
- **Certificate suspension and revocation.** Under what circumstances will the issuing party revoke or suspend an issued certificate? This section should detail the obligations of the certificate holder, as well as actions that can lead to certificate revocation.
- **Security audit procedures.** What actions are audited at the CA and what managerial roles are capable of reviewing the audit logs for the CA?
- **Records archival.** What information is archived by the CA? This can include configuration information, as well as information about encryption private keys archived in the CA database. This section should detail the process necessary to recover private key material. For example, if the roles of certificate manager and key recovery agent are separated, a description of the responsi-

bilities of each role should be provided so the certificate holder is aware that a single person cannot perform private key recovery.

- **Key changeover.** What is the lifetime of the CA's certificate and how often is it renewed? This section should detail information about the certificate and its associated key pair. For example, is the key pair changed every time the CA's certificate is renewed, or only when the original validity period of the CA certificate elapses?
- **Compromise and disaster recovery.** What measures are taken to protect the CA from compromise? Likewise, if a CA fails, what measures are in place to ensure a quick recovery of the CA and its CA database?
- **CA termination.** What actions are taken when the CA is removed from the network? This section can include information about the CA's expected lifetime.

## CPS: Physical, Procedural, and Personnel Security Controls

This section describes physical, procedural, and personnel security controls implemented at the CA for key generation, subject authentication, certificate issuance, certificate revocation, audit, and archiving. These controls can range from limiting which personnel can physically access the CA to ensuring that an employee is assigned only a single PKI management role. For a relying party, these controls are critical in the decision to trust certificates because poor procedures can result in a PKI that is more easily compromised without the issuing organization recognizing the compromise.

## CPS: Technical Security Controls

This section defines the security measures taken by the CA to protect its cryptographic keys and activation data. For example, is the key pair for the CA stored on the local machine profile on a two-factor device, such as a smart card, or on a FIPS 140-2 Level 2 or Level 3 hardware device, such as a hardware security module (HSM)? When a decision is made to trust another organization's certificates, the critical factor is often the security provided for the CA's private key.

This section can also include technical security control information regarding key generation, user validation, certificate revocation, archival of encryption private keys, and auditing.



**Warning** The technical security control section should only provide high-level information to the reader and not serve as a guide to an attacker regarding potential weaknesses in the CA's configuration. For example, is it safe to disclose that the CA's key pair is stored on a FIPS 140-2 Level 2 or Level 3 HSM? It is not safe to describe the CA's management team members or provide specific vendor information about the HSM.

## CPS: Certificate and Certificate Revocation List (CRL) Profiles

This section is used to specify two types of information:

- **Information about the types of certificates issued by the CA.** For example, are CA-issued certificates for user authentication, EFS, or code signing?
- **Information about CRL publication.** This section should provide information about how frequently a CRL is published and whether delta CRLs are implemented. If the CA implements Online Certificate Status Protocol (OCSP), configuration information should be detailed here.

## CPS: Specification Administration

This section specifies ongoing maintenance of the CPS. For example, what circumstances drive the modification of the CPS? If the CPS is modified, who approves the changes? In addition, this section should specify how the modified CPS's contents are published and how the public is notified that the contents are modified.



**Note** In some cases, the actual modifications are slight, such as a recommended rewording by an organization's legal department. In these cases, the URL referencing the CPS need not be changed, just the wording of the documents referenced by the URL.

## Case Study: Planning Policy Documents

You are the head of security for Fabrikam Inc., a large manufacturing company. Your IT department has several PKI-related initiatives planned for the next 18 months, and you are responsible for the drafting of all related policy documents.

### Design Requirements

One of the applications planned by the IT department is the deployment of smart cards for both local and VPN authentication by all employees. During research for the smart card deployment, the IT department gathered the following information that will affect the policies you draft:

- Each employee will be issued a smart card on his or her first day with Fabrikam Inc.
- Existing employees will receive their smart cards on an office-by-office basis. Members of the IT department will travel to each major regional office and deliver the smart cards to all employees in that region.
- Fabrikam has a high employee turnover. In any given month, as many as 1,000 employees leave Fabrikam and are replaced with roughly 1,200 new employees.

## Case Study Questions

1. What is the relationship between a CPS, certificate policy, and security policy?
2. In what document would you define the methods used to identify the new hires when they start with Fabrikam?
3. Will the identification validation requirements for existing employees differ from those implemented for new employees of Fabrikam?
4. The high turnover of employees must be addressed in the CPS. Specifically, what sections must be updated to define the measures taken when an employee is terminated or resigns from Fabrikam?
5. You are considering modeling your certificate policies after the United States Department of Defense certificate policies. What certificate class would best match your deployment of smart cards?

## Additional Information

- Microsoft Official Curriculum, Course 2821: “Designing and Managing a Windows Public Key Infrastructure” ([www.microsoft.com/traincert/syllabi/2821afinal.asp](http://www.microsoft.com/traincert/syllabi/2821afinal.asp))
- ISO 17799, “Code of Practice for Information Security Management” (<https://www.bspsl.com/secure/iso17799software/cvm.cfm>)
- RFC 2196, “The Site Security Handbook” ([www.ietf.org/rfc/rfc2196.txt](http://www.ietf.org/rfc/rfc2196.txt))
- X.509 Certificate Policy for the United States Department of Defense (DoD) ([www.defenselink.mil/nii/org/sio/ia/pki/DoD\\_CP\\_V60\\_31May2002.pdf](http://www.defenselink.mil/nii/org/sio/ia/pki/DoD_CP_V60_31May2002.pdf))
- RFC 2527, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” ([www.ietf.org/rfc/rfc2527.txt](http://www.ietf.org/rfc/rfc2527.txt))
- The Information Security Policies/Computer Security Policies Directory (<http://www.information-security-policies-and-standards.com>)

## **Part II**

# **Establishing a PKI**



## Chapter 4

# Preparing an Active Directory Environment

When network administrators hear that their organization is going to deploy a Microsoft Windows Server 2003 public key infrastructure (PKI), several questions typically come to mind:

- **Do I have to upgrade all domain controllers in my forest to Windows Server 2003?** The answer is no. A Windows Server 2003 PKI is not dependent on Windows Server 2003 domain controllers. You can deploy a Windows Server 2003 PKI in a Windows 2000 Active Directory environment.
- **Do I have to upgrade my domain functional level or forest functional level to Windows Server 2003?** No again. A Windows Server 2003 PKI has no requirements for domain or forest functional levels. In fact, you can deploy a Windows Server 2003 PKI in a mixed-mode Windows 2000 Active Directory environment.
- **So what do I have to do to deploy a Windows Server 2003 PKI?** This chapter will describe the actions you must take to deploy a Windows Server 2003 PKI in a Windows 2000 Active Directory or Windows 2003 Active Directory environment.

## Preparing a Windows 2000 Active Directory Environment

Several preparations should be undertaken before installing a Windows Server 2003 enterprise certification authority (CA) in a Windows 2000 Active Directory environment. These preparations include:

- **Determining whether Microsoft Exchange Server 2000 is deployed in the Windows 2000 forest.** Exchange Server 2003 defines three non-RFC-compliant attributes for the *inetOrgPerson* object: *houseIdentifier*, *Secretary*, and *labeledURI*. To prevent mangling, the Lightweight Directory Access Protocol (LDAP) display names of these attributes must be modified *before* Windows Server 2003 schema modifications are performed. Mangling—the modification

of a display names from the correct name to a name with an autogenerated prefix and suffix—occurs when an existing attribute and a new attribute are configured with the same LDAP display name.

- **Ensuring that all domain controllers are running Windows 2000 Service Pack 3 or later.** Windows 2000 Service Pack 3 is the minimum required version when applying the Windows Server 2003 schema.
- **Ensuring that the schema naming context is replicated to all domain controllers in the forest.** The schema must replicate successfully to allow Windows Server 2003 schema updates.

## Microsoft Exchange Modifications

As mentioned, Exchange Server 2000 defines three non-RFC-compliant attributes for the *inetOrgPerson* object. The modifications shown in Table 4-1 prevent mangling of the LDAP display names for these attributes. If you do not modify these attributes before you apply the Windows Server 2003 schema update, the LDAP display name will be modified. For example, the LDAP display name for the MS-Exch-Assistant-Name attribute will change from *Secretary* to something similar to *DUP-secretary-c5a1240d-70c0-455c-9906-a4070602f85f*. The method for protecting yourself against the mangling of these attributes will be described later in this chapter.



**Note** For details on RFC-compliant definitions, see RFC 2798, “Definition of the inetOrgPerson LDAP Object Class,” available at <http://www.ietf.org/rfc/rfc2798.txt>.

**Table 4-1 Exchange Attribute Modifications**

Attribute	Original LDAP Display Name	Modified LDAP Display Name
Ms-Exch-Assistant-Name	<i>Secretary</i>	<i>msExchAssistantName</i>
Ms-Exch-LabeledURI	<i>labeledURI</i>	<i>msExchLabeledURI</i>
Ms-Exch-House-Identifier	<i>houseIdentifier</i>	<i>msExchHouseIdentifier</i>

### Incorrect Modification of the LDAP Display Names Does Not Occur When...

There are scenarios in which the incorrect modification of the three LDAP display names does not occur—for example, mangling does not occur when the three attributes in the directory are correctly defined *before* Exchange 2000 schema modifications are applied. These scenarios are:



- The inetOrgPerson kit is applied to a Windows 2000 forest before you apply Windows Server 2003 schema modifications.



**More Info** The inetOrgPerson kit is a schema update that adds the RFC-compliant definition of the *inetOrgPerson* object and its attributes to a Windows 2000 Active Directory schema. The inetOrgPerson kit is available at <http://www.microsoft.com/downloads/details.aspx?FamilyId=2C96869E-4CF3-40CC-97FE-7A68720F7D83&displaylang=en>.

- The Windows Server 2003 schema modifications are applied to the Windows 2000 forest before you install Exchange Server 2000 or Exchange Server 2003.
- Exchange Server 2000 or Exchange Server 2003 is installed into an existing Windows Server 2003 forest.



**Note** Exchange Server 2000 cannot be installed on a computer running Windows Server 2003, but it can be installed on a Windows 2000 Server that is a member of a Windows Server 2003 domain.

### Incorrect Modification of the LDAP Display Names Occurs When...

Incorrect modification of the LDAP display names occurs in the following scenarios:

- When you install Exchange Server 2000 or Exchange Server 2003 before you install Windows Server 2003 schema updates.
- When you install Exchange Server 2000 or Exchange Server 2003 before you apply the inetOrgPerson kit.
- When you install Windows Server 2003 schema updates before replication of the modifications to the LDAP display names is complete.



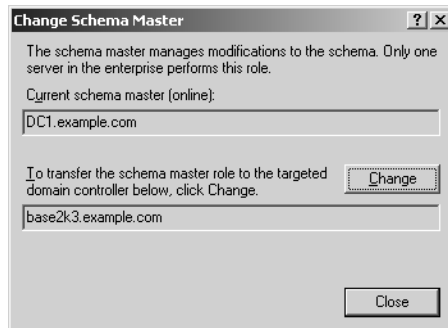
**Note** The processes to prevent mangling or to fix mangling described in the following sections are based on Microsoft Knowledge Base Article 314649, “Windows Server 2003 adprep /forestprep Command Causes Mangled Attributes in Windows 2000 Forests That Contain Exchange 2000 Servers,” available at <http://support.microsoft.com/?ID=314649>.

## Preventing Incorrect Modification of the LDAP Display Names

It is possible to prevent incorrect modification of the attributes by running a script that modifies the LDAP display names prior to the application of Windows Server 2003 schema modifications.

Use the following process to modify the Exchange Server 2000 attributes:

1. Identify the schema operations master for the forest. You can do this by performing the following steps:
  - a. Install the Adminpak.msi on a Windows XP or Windows Server 2003 domain member computer from the \i386 folder of the Windows Server 2003 installation media.
  - b. From a command prompt, type **Regsvr32 Schmmgmt.dll** and press ENTER.
  - c. From a command prompt, type **Schmmgmt.msc** and press ENTER.
  - d. In the console tree, right-click Active Directory Schema and click Operations Master.
  - e. Identify the current schema master in the Change Schema Master dialog box. In the example shown in Figure 4-1, the current schema operations master is DC1.example.com.



**Figure 4-1** Identifying the current schema operations master

- f. Click Close and then close the Schema Management console.
2. Log on locally at the schema operations master as a member of the Schema Admins group.
3. Open the Schmmgmt.msc console.
4. In the console tree, right-click Active Directory Schema and click Operations Master.
5. In the Change Schema Master dialog box, select the The Schema May Be Modified On This Domain Controller check box and click OK. (See Figure 4-2.)



**Figure 4-2** Enabling updates at the schema operations master

6. Create an LDAP Data Interchange Format (LDIF) text file named Exchange-Mod.ldf with the following content to modify the three LDAP display names:



**More Info** All scripts in this chapter are provided on the accompanying CD-ROM.

```
dn: CN=ms-Exch-Assistant-Name,CN=Schema,CN=Configuration,DC=X
changetype: Modify
replace: 1DAPDisplayName
1DAPDisplayName: msExchAssistantName
-
```

```
dn: CN=ms-Exch-LabeledURI,CN=Schema,CN=Configuration,DC=X
changetype: Modify
replace: 1DAPDisplayName
1DAPDisplayName: msExchLabeledURI
-
```

```
dn: CN=ms-Exch-House-Identifier,CN=Schema,CN=Configuration,DC=X
changetype: Modify
replace: 1DAPDisplayName
1DAPDisplayName: msExchHouseIdentifier
-
```

7. At a command prompt, type the following command to apply schema modifications:

```
ldifde -i -f ExchangeMod.ldf -c DC=X ForestRootDomain
```



**Note** The *ForestRootDomain* variable must be replaced with the LDAP distinguished name of the forest root domain. For example, if the forest root domain is *example.com*, the LDAP distinguished name is *DC=example,DC=com*.

8. Verify the modification of the LDAP display names for CN=MS-Exch-Assistant-Name, MS-Exch-LabeledURI, and CN=MS-Exch-House-Identifier by using an LDAP tool, such as LDP.exe or Adsiedit.msc from Windows Support Tools.



**Tip** To install Windows Support Tools, run *X:\support\tools\SUPTOOLS.MSI* (where *X* is your CD-ROM drive) from the Windows Server 2003, Enterprise Edition, compact disc on a Windows XP or Windows Server 2003 computer.

## Fixing Incorrect Modification of the LDAP Display Names

If you apply Windows Server 2003 schema updates and the three LDAP display names become mangled, you can fix the problem by running the *inetOrgPersonFix.ldf* script included in Windows Support Tools. This script will modify the LDAP display names to ensure that the correct display names are used for both the Exchange Server 2000 and *inetOrgPerson* attributes.

You can use the following procedure to fix mangled LDAP display names:

1. Log on locally at the schema operations master as a member of the Schema Admins group.
2. Open the *Schmmgmt.msc* console.
3. In the console tree, right-click Active Directory Schema and click Operations Master.
4. In the Change Schema Master dialog box (see Figure 4-2), select the The Schema May Be Modified On This Domain Controller check box and click OK.
5. From the Windows Server 2003 product CD, open *\Support\Tools\Support.cab*.
6. Extract the *inetOrgPersonFix.ldf* file from the *\Support\Tools\Support.cab* file.

7. In the CD:\Support\Tools\Support.cab window, right-click InetOrgPerson-Fix.ldf, and then click Extract.
8. In the Select a Destination window, select a folder on the local hard disk, and then click OK.

The text of the inetOrgPersonFix.ldf file follows:

```
# Fix the LDN of inetOrgPerson schema objects in case they were mangled.
```

```
dn: CN=secretary,CN=Schema,CN=Configuration,DC=X
changetype: Modify
replace: 1DAPDisplayName
1DAPDisplayName: secretary
-
```

```
dn: CN=labeledURI,CN=Schema,CN=Configuration,DC=X
changetype: Modify
replace: 1DAPDisplayName
1DAPDisplayName: labeledURI
-
```

```
dn: CN=houseIdentifier,CN=Schema,CN=Configuration,DC=X
changetype: Modify
replace: 1DAPDisplayName
1DAPDisplayName: houseIdentifier
-
```

```
dn: CN=ms-Exch-Assistant-Name,CN=Schema,CN=Configuration,DC=X
changetype: Modify
replace: 1DAPDisplayName
1DAPDisplayName: msExchAssistantName
-
```

```
dn: CN=ms-Exch-LabeledURI,CN=Schema,CN=Configuration,DC=X
changetype: Modify
replace: 1DAPDisplayName
1DAPDisplayName: msExchLabeledURI
-
```

```
dn: CN=ms-Exch-House-Identifier,CN=Schema,CN=Configuration,DC=X
changetype: Modify
replace: 1DAPDisplayName
1DAPDisplayName: msExchHouseIdentifier
-
```

```
dn:
changetype: Modify
add: schemaUpdateNow
schemaUpdateNow: 1
-
```

9. Open a command prompt and navigate to the folder with the inetOrgPerson-Fix.ldf file.

10. At the command prompt, type **ldifde -i -f inetOrgPersonFix.ldf -c DC=X ForestRootDomain**.



**Note** The *ForestRootDomain* variable must be replaced with the LDAP distinguished name of the forest root domain. For example, if the forest root domain is example.com, then the LDAP distinguished name is DC=example,DC=com.

## Extending the Schema

A Windows 2000 domain must be upgraded to the Windows Server 2003 schema to support some of the new features in a Windows Server 2003 PKI. These features include:

- **Support for version 2 certificate templates.** The Windows Server 2003 schema includes the definition of the version 2 certificate template object. Version 2 certificate templates allow customization of certificate content.
- **Support for delta certificate revocation lists (CRLs).** A delta CRL contains the certificates revoked since the publication of the last base CRL. This object type and its corresponding attributes are added in the Windows Server 2003 schema.
- **Support for key archival and recovery.** Properties of the CA object are extended by the Windows Server 2003 schema to allow the designation of a key recovery agent, which enables key archival and recovery at the CA.
- **Support for Cross Certification Authority certificates in Active Directory.** Cross Certification Authority certificates are implemented when you renew a CA certificate. A Cross Certification Authority certificate defines a relationship between the previous CA certificate and the new CA certificate to allow Windows XP and newer operating systems to continue to build chains with the previous CA certificate.
- **Support for custom object identifiers (OIDs) and OID name resolution in Active Directory.** The schema extensions add support for defining custom application policy and certificate policy OIDs in Active Directory and issued certificates. In addition, if a certificate contains an OID, the OID is resolved to meaningful text based on the OID definition in Active Directory.

Once the current schema is modified to prevent attribute mangling, you can upgrade to the Windows Server 2003 schema using the following procedure:

1. Log on locally at the schema operations master as a member of the Schema Admins and Enterprise Admins groups.

2. In the console tree, right-click Active Directory Schema and click Operations Master.
3. In the Change Schema Master dialog box, select the The Schema May Be Modified On This Domain Controller check box and click OK.
4. Insert the Windows Server 2003, Enterprise Edition, compact disc in the CD-ROM drive.
5. At a command prompt, type **X:\i386\adprep.exe /forestprep** (where X is the drive letter of the CD-ROM) and press ENTER.
6. When prompted, press C to continue with schema updates.
7. When modifications are complete, in the console tree, right-click Active Directory Schema and click Operations Master.
8. In the Change Schema Master dialog box, clear The Schema May Be Modified On This Domain Controller check box and click OK.

This procedure will update the schema from version 13 (Windows 2000) to version 30 (Windows Server 2003).



**Note** If you want to view the actual modifications made to the schema in detail, you can look at the schema update LDIF files in the \i386 folder of the Windows Server 2003, Enterprise Edition, compact disc. The files are named SCH##.ldf, where ## is a number between 14 and 30, representing the modifications made in each revision.

Once the update is complete, you must ensure that the modifications replicate fully to all domain controllers in the forest. You can view the replication status by using either the Replication Monitor (Replmon.exe) graphical tool or the Repadmin.exe command-line tool from Windows Support Tools.



**Note** Read the documentation on each of these tools for information on how to best ensure that replication completes for the schema modifications.

After modification of the schema is replicated to all domain controllers in the forest, you can prepare each domain to benefit from the Windows Server 2003 schema extensions. You can use the following procedure to prepare each domain in the forest:

1. Log on locally at the infrastructure master in the domain as a member of the Domain Admins group.
2. Insert the Windows Server 2003, Enterprise Edition, compact disc in the CD-ROM drive.
3. At a command prompt, type **X:\i386\adprep /domainprep** (where X is the drive letter of the CD-ROM) and press ENTER.
4. Repeat the process for every domain in the forest.



**Note** It is not necessary to run `adprep /domainprep` to install a Windows Server 2003 enterprise CA in the forest.

## Modifying Membership in Cert Publishers

The Cert Publishers group is assigned permission to read and write certificate information to the *userCertificate* attribute of user objects. Certificates published to these attributes are typically encryption certificates, allowing anyone to obtain the public key of a target's encryption certificate by querying Active Directory.

By default, the Cert Publishers group from a specific domain is allowed to read and write to the *userCertificate* attribute for objects in the same domain, which is fine if you have a single-domain forest. If your forest consists of two or more domains, however, you must modify permissions to allow each domain's Cert Publishers group read and write permissions to the *userCertificate* attribute.



**Note** If an enterprise CA does not have sufficient permissions to write a certificate to the *userCertificate* attribute, the following entry will appear in the application log:

Event ID: 11

Source: Cert Server Enterprise Policy

Application: Warning CA was unable to publish the certificate for the Domain\server. Server is not part of the Cert Publishers group. Privilege violation.

The Cert Publishers group exists in the CN=Users, *DomainName* container (where *DomainName* is the LDAP distinguished name of the domain) in each domain in a Windows 2000 forest. In a Windows 2000 domain, the scope of the Cert



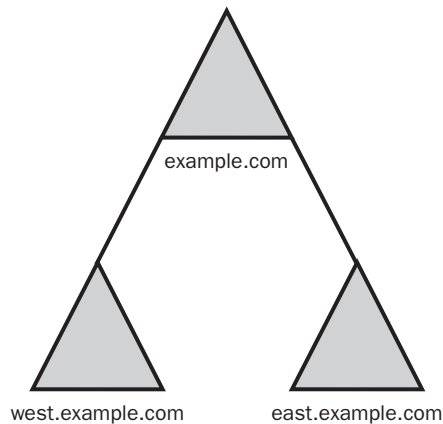
Publishers group is a global group. This means that only user accounts, computer accounts, and global groups from the same domain can have membership in the Cert Publishers group.

To modify permissions to allow enterprise CAs from other domains to publish information to the *userCertificate* attribute, use the following strategy:

- Assign each domain's Cert Publishers group the Read *userCertificate* permission in every domain in the forest.
- Assign each domain's Cert Publishers group the Write *userCertificate* permission in every domain in the forest.
- Assign each domain's Cert Publishers group the Read *userCertificate* permission at the CN=adminsdholder,CN=system,*DomainName* container in every domain in the forest.
- Assign each domain's Cert Publishers group the Write *userCertificate* permission at the CN=adminsdholder,CN=system,*DomainName* container in every domain in the forest.

You can script these permission assignments by using the DSACLs.exe command from Windows Support Tools.

For the next example, assume that the domain configuration shown in Figure 4-3 is implemented.



**Figure 4-3** A sample domain configuration

In this example, an enterprise CA exists in each domain in the forest: *example.com*, *east.example.com*, and *west.example.com*. You must add permissions for each domain's Cert Publishers group. The following script accomplishes these permission assignments:

```

:: Assign permissions to the example.com domain
dsacl "dc=example,dc=com" /I:S /G "East\Cert Publishers":RP;userCertificate,user
dsacl "dc=example,dc=com" /I:S /G "East\Cert Publishers":WP;userCertificate,user
dsacl "dc=example,dc=com" /I:S /G "West\Cert Publishers":RP;userCertificate,user
dsacl "dc=example,dc=com" /I:S /G "West\Cert Publishers":WP;userCertificate,user

```

```

:: Assign permissions to the east.example.com domain
dsacl "dc=east,dc=example,dc=com" /I:S /G
"Example\Cert Publishers":RP;userCertificate,user
dsacl "dc=east,dc=example,dc=com" /I:S /G
"Example\Cert Publishers":WP;userCertificate,user
dsacl "dc=east,dc=example,dc=com" /I:S /G
"West\Cert Publishers":RP;userCertificate,user
dsacl "dc=east,dc=example,dc=com" /I:S /G
"West\Cert Publishers":WP;userCertificate,user

```

```

:: Assign permissions to the west.example.com domain
dsacl "dc=west,dc=example,dc=com" /I:S /G
"Example\Cert Publishers":RP;userCertificate,user
dsacl "dc=west,dc=example,dc=com" /I:S /G
"Example\Cert Publishers":WP;userCertificate,user
dsacl "dc=west,dc=example,dc=com" /I:S /G
"East\Cert Publishers":RP;userCertificate,user
dsacl "dc=west,dc=example,dc=com" /I:S /G
"East\Cert Publishers":WP;userCertificate,user

```

```

:: Assign permissions to the Adminsdholder container in example.com
dsacl " cn=adminsdholder,cn=system,dc=example,dc=com" /G
"East\Cert Publishers":RP;userCertificate
dsacl " cn=adminsdholder,cn=system,dc=example,dc=com" /G
"East\Cert Publishers":WP;userCertificate
dsacl " cn=adminsdholder,cn=system,dc=example,dc=com" /G
"West\Cert Publishers":RP;userCertificate
dsacl " cn=adminsdholder,cn=system,dc=example,dc=com" /G
"West\Cert Publishers":WP;userCertificate

```

```

:: Assign permissions to the Adminsdholder container in east.example.com
dsacl " cn=adminsdholder,cn=system,dc=east,dc=example,dc=com" /G
"Example\Cert Publishers":RP;userCertificate
dsacl " cn=adminsdholder,cn=system,dc=east,dc=example,dc=com" /G
"Example\Cert Publishers":WP;userCertificate
dsacl " cn=adminsdholder,cn=system, dc=east,dc=example,dc=com" /G
"West\Cert Publishers":RP;userCertificate
dsacl " cn=adminsdholder,cn=system, dc=east,dc=example,dc=com" /G
"West\Cert Publishers":WP;userCertificate

```

```

:: Assign permissions to the Adminsdholder container in west.example.com
dsacl " cn=adminsdholder,cn=system,dc=west,dc=example,dc=com" /G
"Example\Cert Publishers":RP;userCertificate
dsacl " cn=adminsdholder,cn=system,dc=west,dc=example,dc=com" /G
"Example\Cert Publishers":WP;userCertificate
dsacl " cn=adminsdholder,cn=system, dc=west,dc=example,dc=com" /G
"East\Cert Publishers":RP;userCertificate
dsacl " cn=adminsdholder,cn=system, dc=west,dc=example,dc=com" /G
"East\Cert Publishers":WP;userCertificate

```



**Tip** To use this script in your environment, simply modify the domain names to match the domain names in your forest. You must assign permissions to the domain and the AdminSDHolder container for each domain in your forest.

## Preparing a Windows Server 2003 Active Directory Environment

If you are installing a Windows 2003 PKI in a Windows Server 2003 Active Directory environment, no modifications are required to allow installation because Active Directory is already configured with the Windows Server 2003 schema. Likewise, each domain in the forest already has the domain additions applied to each domain in the forest.



**Note** A Windows Server 2003 PKI has no requirements for a domain functional level or forest functional level.

Modification of the Cert Publishers groups is the only modification required in a multidomain Windows Server 2003 forest environment. In a Windows Server 2003 forest, the Cert Publishers group is a domain local group that exists in each domain in the forest.

To allow any enterprise CA in the forest to publish certificates to any user object in the current forest or to *Contact* objects in foreign forests, you must add the enterprise CA's computer account to the membership of each domain's Cert Publishers group. Because the scope of the Cert Publishers group is changed from a global group to a domain local group, the membership can now contain computer accounts from outside the domain where the Cert Publishers group resides.



**Note** If the forest was previously modified to add either an enterprise Cert Publishers universal group or individual Cert Publishers group entries to the domain and AdminSDHolder container, these extraneous entries should be removed once all domains are upgraded to Windows Server 2003 domains—that is, once every domain controller in the domain is running Windows Server 2003.

## Preparing Non-Active Directory Environments

It is not possible to deploy Windows Server 2003 enterprise CAs in non-Active Directory environments. An enterprise CA requires the existence of Active Directory for storage of configuration information and certificate publishing, as well as its security policy and authentication functionality. This does not mean that you cannot deploy a Windows Server 2003 PKI in a non-Active Directory environment. It only means that every CA in the PKI hierarchy must be a standalone CA.

In a standalone CA environment, the contents of the certificates are defined in the actual certificate request files, rather than using certificate templates in Active Directory to define the content of issued certificates. In addition, all certificate requests are set to a pending status by default, requiring a certificate manager to approve or deny every certificate request submitted to the standalone CA.

## Case Study: Preparing Active Directory

You are the network administrator for Tailspin Toys, a toy manufacturing company. Your organization's forest consists of two Windows 2000 domains: `tailspintoys.msft` and `wingtiptoys.msft`, as shown in Figure 4-4.



**Figure 4-4** The Tailspin Toys forest

The `tailspintoys` domain contains user and computer objects from North American operations, while `wingtiptoys.msft` contains user and computer objects from European operations. `Tailspintoys` is the forest root domain.

You are planning to implement a Windows 2003 PKI in your environment. You foresee issuing CAs running Windows Server 2003, Enterprise Edition, in both the `tailspintoys.msft` and `wingtiptoys.msft` domains. Tailspin Toys currently uses Windows XP, Professional Edition, for all desktops and runs Exchange 2000, Enterprise Edition, as the e-mail system. All desktop computers run Microsoft Outlook 2002 as their e-mail client.



**Note** Windows Server 2003, Enterprise Edition, and Windows Server 2003, Datacenter Edition, fully implement all features of Windows Server 2003 Certificate Services. Windows Server 2003, Standard Edition, offers a subset of the full feature set. The differences are discussed in detail in later chapters.

## Network Details

Table 4-2 shows the current operation master roles to help you determine what configuration changes are required for Active Directory before deploying a Windows Server 2003 PKI.

**Table 4-2 Operation Master Assignments**

<b>Computer</b>	<b>Schema Master</b>	<b>Domain Naming Master</b>	<b>RID Master</b>	<b>PDC Emulator</b>	<b>Infrastructure Master</b>
TailspinToys\NADC01	x				x
TailspinToys\NADC02			x	x	
TailspinToys\NADC03		x			
WingtipToys\EUDC01				x	
WingtipToys\EUDC02			x		
WingtipToys\EUDC03					x

## Case Study Questions

Answer the following questions based on the Tailspin Toys scenario:

1. Based on the current applications and configuration of the tailspintoys.msft forest, is there any possibility of attribute mangling when the Windows Server 2003 schema modifications are applied? Why or why not?
2. Assuming you use the Exchangemod.ldf script provided on the accompanying CD-ROM to apply the necessary schema modifications, what command line will you use to implement the scripted modifications?
3. What service pack level is required at each domain controller before applying the Windows Server 2003 schema modifications?
4. What computer will you use to run `adprep /forestprep`? What group membership(s) is/are required?
5. What computer(s) will you use to run `adprep /domainprep`? What group membership(s) is/are required?

6. After installing the issuing CAs, the following error appears intermittently in the application log:

*Event ID: 11*

*Source: Cert Server Enterprise Policy*

*Application: Warning CA was unable to publish the certificate for the Domain\server. Server is not part of the Cert Publishers group. Privilege violation.*

What configuration change is required to resolve this error?

7. How would the solution differ if the network implemented Windows Server 2003 Active Directory rather than Windows 2000 Active Directory?

## Additional Information

- Microsoft Official Curriculum, Course 2821: “Designing and Managing a Windows Public Key Infrastructure” ([www.microsoft.com/traincert/syllabi/2821afinal.asp](http://www.microsoft.com/traincert/syllabi/2821afinal.asp))
- RFC 2798, “Definition of the inetOrgPerson LDAP Object Class” (<http://www.ietf.org/rfc/rfc2798.txt>)
- inetOrgPerson Kit (<http://www.microsoft.com/downloads/details.aspx?FamilyId=2C96869E-4CF3-40CC-97FE-7A68720F7D83&displaylang=en>)
- “Best Practices for Implementing a Microsoft Windows Server2003 Public Key Infrastructure” (<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/us3pkibp.mspix>)
- “PKI Enhancements in Windows XP Professional and Windows Server 2003” (<http://www.microsoft.com/technet/prodtechnol/winxpupro/Plan/PKIEnh.asp>)
- Knowledge Base Article 219059: “Enterprise CA May Not Publish Certificates from Child Domain or Trusted Domain”
- Knowledge Base Article 300532: “Windows 2000 Enterprise CAs Not Added to Certificate Publishers Group in Windows Server 2003 Domain”
- Knowledge Base Article 314649: “Windows Server 2003 adprep /forestprep Command Causes Mangled Attributes in Windows 2000 Forests That Contain Exchange 2000 Servers”
- Knowledge Base Article 555040: “Common Mistakes When Upgrading a Windows 2000 Domain to a Windows 2003 Domain”



**Note** To find Microsoft Knowledge Base articles, go to <http://support.microsoft.com> and enter the article number in the Search the Knowledge Base text box.

## Chapter 5

# Designing a Certification Authority Hierarchy

Before deploying Microsoft Windows Server 2003 Certificate Services, an organization must spend time designing the certification authority (CA) hierarchy. Developing the correct structure involves investigating and processing related requirements for application, security, business and technology, and external forces. Hierarchy elements that will be covered in this chapter include:

- The number of tiers to use in a CA hierarchy.
- How the CAs will be arranged in a CA hierarchy.
- The types of certificates each CA will issue.
- The types of CAs to be deployed at each tier.
- Security measures to protect the CAs.
- Whether different certificate policies will be required.

## Determining the Number of Tiers in a CA Hierarchy

The number of tiers to include in the CA hierarchy is a basic consideration addressed in the design process. It is also necessary to determine how many individual CAs will be required at each tier. Most CA hierarchies consist of two to four tiers, though a single-tier CA can be appropriate in smaller organizations.

### A Single-Tier CA Hierarchy

Some organizations require only basic public key infrastructure (PKI) services. Typically, these are organizations with fewer than 300 user accounts in the directory service. Rather than deploying multiple CAs, a single CA is installed as an enterprise root CA.

The enterprise root CA is not removed from the network. Instead, the computer is a member of the domain and is always available to issue certificates to requesting computers, users, services, or networking devices.

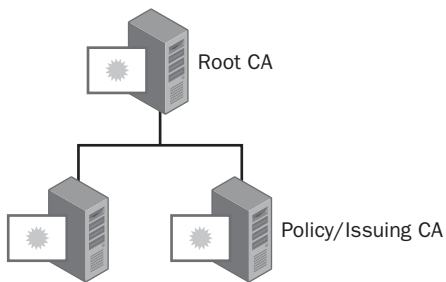
A single-tier CA hierarchy is easy to manage because it involves administration of only a single CA. A problem with this design is the lack of redundancy. If the CA

fails, Certificate Services will not be available to process incoming certificate requests, certificate renewals, or certificate revocation list (CRL) publishing until the CA is restored to service.

Single-tier CA hierarchies are generally used only when simple administration is required, costs must be minimized, and the organization's security policy does not prevent a PKI deployment with a single point of failure.

## A Two-Tier CA Hierarchy

A two-tier hierarchy comprises an offline root CA and one or more issuing CAs. The issuing CAs are a combination of policy CAs and issuing CAs. (See Chapter 3 for a review of issuing CAs.) Figure 5-1 shows a two-tier CA hierarchy.



**Figure 5-1** A two-tier CA hierarchy

To ensure security in a two-tier hierarchy, the root CA is deployed as a stand-alone root CA. This allows an organization to deploy the root CA offline—that is, the CA is removed from the network to provide the computer with additional physical security.



**Note** A standalone CA does not require domain membership. This allows the computer to never be connected to the organization's network to communicate and maintain a computer account in Active Directory.

In a multi-tier CA hierarchy, it does not matter which second-tier CA issues the certificates to computers, users, services, or network devices. All that matters is that the certificate issued by the second-tier CA chains to a trusted root CA—the offline root CA in this configuration.

To enhance the availability of Certificate Services, two or more issuing CAs must exist at the second tier. This prevents Certificate Services from being unavailable due to a single point of failure. The number of issuing CAs depends on the organization's requirements. For example, a CA hierarchy can have different CAs for



each geographic region, each sector or business unit, or each identified certificate policy used to validate a certificate's subject.

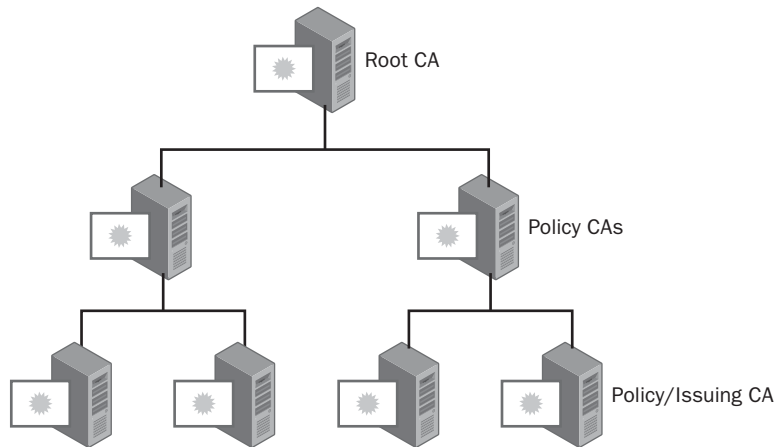


**Note** The design of issuing CAs is discussed in more detail later in this chapter.

## A Three-Tier CA Hierarchy

A three-tier CA hierarchy provides the best security and flexibility. A three-tier CA hierarchy, shown in Figure 5-2, consists of:

- An offline root CA installed as a standalone root CA.
- One or more offline policy CAs installed as standalone subordinate CAs.
- One or more issuing CAs installed as enterprise subordinate CAs or occasionally as subordinate standalone CAs.



**Figure 5-2** A three-tier CA hierarchy

A three-tier hierarchy is recommended in the following scenarios:

- Strong physical security of the CA hierarchy is mandated by the security policy. The removal of the root and policy CA tiers from the network protects computers from network-sourced attacks.
- Two or more different certificate policies are required for certificate issuance. The policy CA tier allows you to define different certificate practice statements (CPSs) and related certificate policies at each policy CA defined at the second tier.

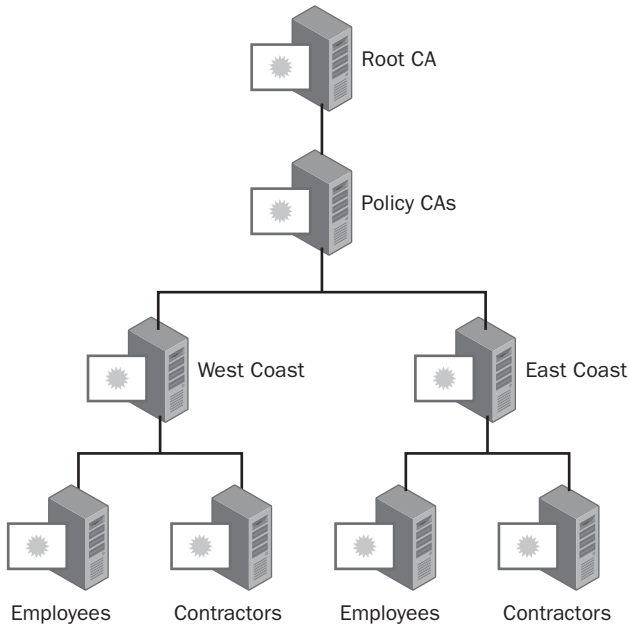
- Management of the CA hierarchy is split among different network administration teams—for example, one PKI management team manages the Europe CAs, while a separate team manages the Asia CAs. In this scenario, each team is responsible for defining the CPS for their policy CAs. (See Chapter 3 for a review of defining the CPS.)



**Note** Remember that a CPS is effective at the CA where the CPS is defined in the CA certificate, as well as at any CAs that are subordinate to that CA in the hierarchy.

## A Four-Tier CA Hierarchy

More than three tiers in the CA hierarchy might be required in some cases, but deploying more than four layers is not recommended. In a four-tier CA hierarchy, issuing CAs reside at both the third and fourth levels of the hierarchy. Figure 5-3 shows an example with two regional CAs at the third level of the CA hierarchy and different CAs (for employees and contractors) at the fourth level.

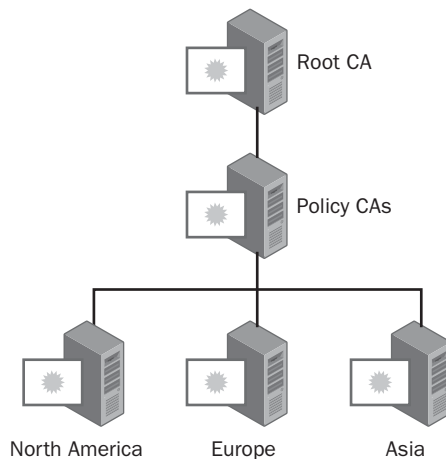


**Figure 5-3** A four-tier CA hierarchy

## Organizing Issuing CAs

Management of issuing CAs for a network should be based on the following factors:

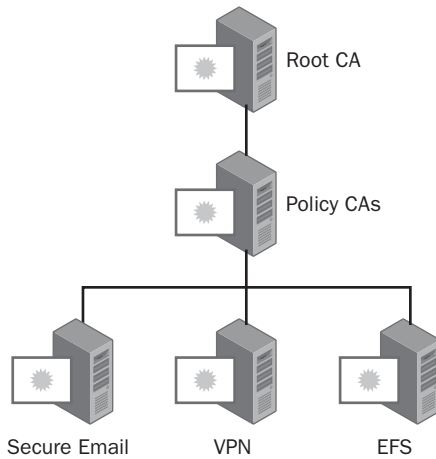
- **The number of certificates that will be issued.** The more certificates a CA hierarchy issues to users, computers, services, or network devices, the higher the number of issuing CAs required in the CA hierarchy.
- **Availability requirements in a wide area network (WAN) environment.** In a WAN environment, there is a possibility of network outages. To prevent the failure of Certificate Services, CAs can be placed at major network hub sites. For example, Figure 5-4 shows a CA hierarchy in which issuing CAs are placed at a North American hub site, a European hub site, and an Asian hub site.



**Figure 5-4** A CA hierarchy that distributes CAs by geographic hub sites

This geographic configuration might also require multiple policy CAs if different subject-identification processes or other PKI management processes are implemented for each region.

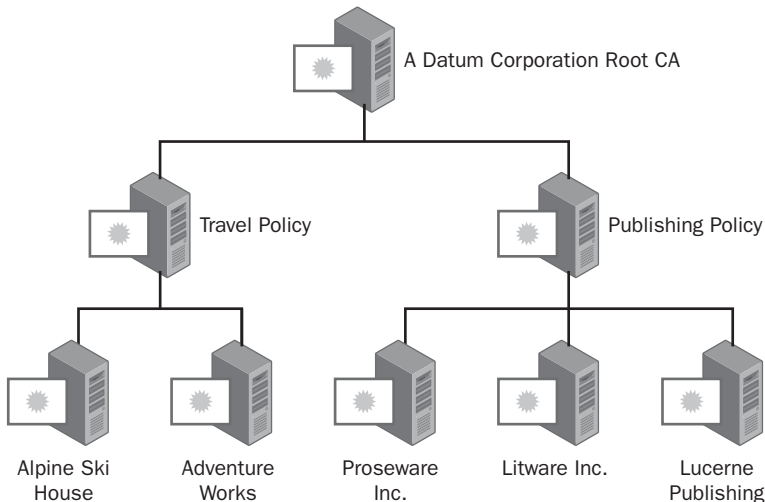
- **The PKI management model.** Some companies use separate teams to manage projects for PKI-enabled applications. For example, one team manages all certificates related to virtual private networking, and another team manages certificates related to secure e-mail. Figure 5-5 shows an example of a CA hierarchy based on decentralized certificate distribution.



**Figure 5-5** A CA hierarchy that distributes CAs by PKI management

In this example, separate CAs exist for each PKI-enabled project. The Secure Email CA issues the required certificates for Secure/Multipurpose Internet Mail Extensions (S/MIME); the VPN CA issues the required certificates for a virtual private network (VPN) solution; and the EFS CA issues the required certificates for Encrypting File System (EFS) encryption.

- **The structure of the company hosting the PKI.** In some cases, an organization is a member of a conglomerate of several organizations. For example, if A Datum Corporation is a holding company that includes several autonomous but related companies, the CA hierarchy can include separate policy and issuing CAs for each company within the umbrella group. (See Figure 5-6.)



**Figure 5-6** A CA hierarchy that distributes CAs by company structure

In this example, there are two policy CAs: one for the travel agency arm and one for the publication arm of A Datum Corporation. Below the policy CAs, there are separate issuing CAs for each company within the A Datum Corporation umbrella. The issuing CAs must enforce the policies and procedures defined at their respective policy CAs.

- **Employee categories.** It is also common to have different CAs for each employee category within an organization. The creation of separate CAs for each employee category allows certificate management to be delegated to different groups. This architecture also allows different methods of subject identification for each employee category—for example:
  - **By citizenship.** Some U.S. military organizations, such as defense contractors, require delegation according to citizenship or nationality in which different subject-identification requirements exist for U.S. citizens, U.S. green card holders, and everyone else (referred to as foreign nationals). In this type of environment, a CA hierarchy is created that implements separate issuing CAs for each citizenship category.
  - **By employee type.** Some organizations classify employees according to organizational hiring status. For example, separate issuing CAs can be required for employees, contractors, external consultants, and interns.



**Note** This is not a complete list; it is only a partial set of common factors.

## Choosing an Architecture

There is no simple formula for choosing an architecture. Factors to consider when designing the CA hierarchy include:

- **Organization size.** The more certificates you must distribute, the more CAs you require. This is especially true if an organization is geographically dispersed across continents or regions. A common design places issuing CAs at major hub sites in the network topology to provide regional site availability.
- **The management model.** The CA hierarchy can include fewer CAs in an organization with centralized management. In decentralized organizations, however, a common approach is to issue separate CAs for individual management teams. For example, in a project-based management scheme, separate CAs are used for each project team. (See Figure 5-5.) Similarly, if an organization is composed of several sectors, separate CA management can be defined by each sector in the organization. (See Figure 5-6.)

- **Industry regulations.** Industry regulations sometimes require specific management techniques. For example, a bank might have to follow industry regulations for private key protection for customer data on the network. These requirements can result in a separate set of certificate policies, requiring either a separate policy CA/issuing CA combination or a separate policy CA in addition to associated issuing CAs.

## Gathering Required Information

The process of gathering information will help you design your organization's CA hierarchy. You must collect the following data:

- Application requirements
- Security requirements
- Technical requirements
- Business requirements
- External requirements

## Identifying PKI-Enabled Applications

A PKI deployment is typically launched when an organization introduces one or more applications that are dependent on the existence of a PKI. This leads to defining requirements as to who will manage the applications, the number of users, the certificate distribution, and how certificates are used by the applications.

### PKI-Enabled Applications

Applications and technologies that can trigger an organization to deploy a PKI include:

- **802.1x port-based authentication.** 802.1x authentication allows only authenticated users or computers to access either an 802.11 wireless network or a wired Ethernet network. It provides centralized user identification and authentication by using Remote Authentication Dial-In User Service (RADIUS) on the back end.



**Note** Technically, 802.1x port authentication is Extended Authentication Protocol with Transport Layer Security (EAP/TLS). This form of authentication allows the use of digital certificates when authenticating with a RADIUS server.

- **Digital signatures.** Secure Internet transactions by providing a method for verifying who sent the data and that content was not modified in transit. Depending on how a certificate is issued, digital signatures also provide non-repudiation or content commitment. In other words, data signers cannot deny that they are the data senders, as they are the only users with access to the certificate's private key.
- **Encrypting File System (EFS).** Encrypts data by using a combination of symmetric and asymmetric encryption methods. EFS provides two methods of recovery when using a Windows 2003 enterprise CA: data recovery, in which a designated data recovery agent can open all encrypted files in the domain; and key recovery, wherein a key recovery agent can recover the archived private key from the CA database.
- **Web authentication and encryption.** The distribution of Secure Sockets Layer (SSL) certificates to a Web server on either an intranet or the Internet; allows a Web client to authenticate the Web server's identity and encrypt all data sent to and from the Web server. Alternatively, client authentication certificates can be distributed to Web clients, allowing them to present a certificate as their form of authentication to the Web server. This provides mutual authentication of the Web client and the Web server.
- **IP security.** Certificates can be used to authenticate the two endpoints in an Internet Protocol Security (IPSec) association. Once authenticated, IPSec can be used to encrypt and digitally sign all communications between the two endpoints. Certificates do not play a part in the actual encryption and signing of IPSec-protected data—they are only used to authenticate the two endpoints.
- **Secure e-mail.** Provides confidential communication, data integrity, and nonrepudiation for e-mail messages. You can enhance e-mail security by using certificates to verify a sender's credentials, the message's point of origin, and message authenticity.
- **Smart card logon.** Provides increased security by using two-factor authentication. To authenticate with the network, a user must have access to the smart card and know the Personal Identification Number (PIN) for the smart card.
- **Software code signing.** Protects computers from installation of unauthorized controls, drivers, or applets. Once the content is signed, applications that support code signing, such as Microsoft Internet Explorer, can block access to unsigned controls.
- **VPNs.** Remote users connect to a private network using tunneling protocols, such as Point-to-Point Tunneling Protocol (PPTP) or Layer 2 Tunneling Protocol (L2TP). Certificates increase the strength of user authentication and can provide authentication for IPSec if using L2TP with IPSec encryption.

## Identifying Certificate Recipients

Once you have determined what PKI-enabled applications your organization is deploying, you must decide which certificates are required for each application. Typically, certificates are deployed to the following subjects:

- **Users.** A digital certificate uniquely identifies a user to a PKI-enabled application. A user can be assigned a single certificate that enables all applications or can receive application-specific certificates, such as an EFS encryption certificate that can be used for one purpose only.
- **Computers.** A digital certificate uniquely identifies the computer when a user or computer connects to the computer where the certificate is installed. The certificate becomes the computer's identifier and is stored in the Local Machine certificate store. If the Client Authentication Object Identifier (OID) is included in the certificate in either the Enhanced Key Usage (EKU) extension or the Application Policies extension, the computer certificate can be used to initiate connections. If the Server Authentication OID is included in the certificate in the EKU or Application Policies extension, the certificate can be used to authenticate the computer's identity when a client application connects.
- **Network devices.** Several devices on a network allow the installation of certificates for client/server authentication. These devices include VPN appliances, firewalls, and routers. The actual process used to install a certificate on a network device is subject to the type of operating system and interfaces of the actual network device.
- **Services.** Some services require computer certificates for either authentication or encryption. Certificates are not actually issued to a service. Instead, the service certificate is stored either on the Local Machine store or in the user's profile of the associated service account. For example, if a certificate is installed for the World Wide Web (WWW) service of a Web server, the certificate is stored in the Local Machine store. On the other hand, the EFS recovery agent certificate for the EFS service is stored in the user profile of the designated EFS recovery agent.

## Determining Security Requirements

An organization should have a security policy that defines its security standards. This document (described in greater detail in Chapter 3) provides the security requirements for a PKI design. Some of the possible requirements include:

- **Physical security for offline CAs.** To increase the security of the root CA in a two-tier hierarchy and the root and policy CAs in a three-tier hierarchy, you can remove the CAs from the network and store them in a physically secure



location. In some organizations, only the hard disks are removed from the offline CAs and stored in a safe. This allows the offline CA computer's chassis to be used for other projects when the CA is removed from the network. Alternatively, you can simply locate the CA computers in a server room with restricted access.

- **Additional security for online CAs.** To secure an online CA, you can place the physical computer in a secure server room that requires keycard access. In addition, you should minimize services at an issuing CA. In other words, dedicate the computer as an issuing CA, rather than installing the issuing CA on an existing domain controller.



**Note** If you are implementing a Windows Server 2003 server as an online certification authority, Certificate Services are the only services required. If you deploy the Certificate Services Web Enrollment pages on the same computer, however, a minimal installation of Internet Information Services (IIS) is also necessary. The required IIS components are covered in greater detail in Chapter 6.

- **Protection for the CA's private key.** An organization's security policy can require specific security measures for a CA's private key. For example, an organization might have to implement Federal Information Processing Standards (FIPS) 140-2 protection of the CA's private key to meet industry or organizational security requirements.



**More Info** FIPS 140-2, "Security Requirements for Cryptographic Modules," can be found at <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>.

Measures you can take to protect the CA's private key include:

- **Using a software cryptographic service provider (CSP).** A software CSP, such as the Microsoft Strong Cryptographic Provider, stores the CA's private key material on the computer's local hard disk. While physical security measures can increase the protection of this key material, be aware that *any* member of the local Administrators group can export and reuse the private key material.



**Note** CSPs define how a certificate's private key is protected and accessed. A CSP determines where to generate the certificate's key pair when the certificate is requested, and implements mechanisms to protect access to the private key. For example, a CSP can require the input of a PIN to access a smart card's private key.

- **Using a smart card CSP.** A smart card CSP stores the CA's private key material on a two-factor authentication device. When the private key material is accessed, a user must type in the smart card's PIN.
- **Using a hardware security module (HSM).** An HSM provides the strongest protection of a CA's private key by storing the private key on a physical security device. The HSM provides additional security measures to protect the private key from tampering and, in some cases, destroys the private key if an attack against the HSM occurs.
- **Different issuance requirements for certificates.** An organization can issue certificates that require different issuance requirements. For example, some certificates are issued based on the user's account and password combination, while others are set to a pending state to allow validation of the user's identity through presentation of photo identification. To allow the validation of identity, separate issuing CAs or separate policy CAs can exist in the CA hierarchy.

## Determining Technical Requirements

Technical requirements affect the structure of a CA hierarchy. Technical issues that should be considered during a PKI design process include:

- Defining PKI management staff.
- Minimizing risk of CA failure.
- Determining certificate validity periods.

### Defining PKI Management Staff

Windows Server 2003 PKI allows you to define PKI management staff for each CA. If technical requirements lead you to delegate administration to a specific office or region, you can accomplish this by deploying a separate issuing CA and delegating management to users at that location.

Windows Server 2003 supports the definition of the following Common Criteria roles for PKI management:

- **CA administrator.** Responsible for managing the configuration of the CA computer, including defining the CA's property settings and certificate managers. A user is delegated this role through the assignment of the Manage CA permission at the CA.
- **CA officer.** Responsible for certificate management. Also known as the certificate manager. Tasks include certificate revocation, issuance, and deletion. In addition, the certificate manager extracts archived private keys for recovery by a key recovery agent. A user is given this role through the assignment of the Issue and Manage Certificates permission at the CA.
- **Backup operator.** Responsible for the backup and recovery of the CA database and CA configuration settings. A user is delegated this role through the assignment of the Back Up Files and Directories or the Restore Files and Directories user rights at the Group Policy Object (GPO) assigned to the CA or in the CA's local security policy.
- **Auditor.** Responsible for defining the events audited at the CA and for reviewing the security log for events related to PKI management and operations. A user is given this role through the assignment of the Manage Auditing and Security Log user right at the GPO assigned to the CA or in the CA's local security policy.



**More Info** For more information on Common Criteria role separation, see the "Certificate Issuing and Management Components Protection Profile" at [http://csrc.nist.gov/pki/documents/CIMC\\_PP\\_final-corrections\\_20010126.pdf](http://csrc.nist.gov/pki/documents/CIMC_PP_final-corrections_20010126.pdf).



**Note** The CA administrator and CA officer roles are defined as CA permissions, whereas the backup operator and auditor roles are user rights and are not limited to Certificate Services. Rather, they are applicable to all applications running on the computer hosting Certificate Services.

You can define separate CA administrators, CA officers (certificate managers), backup operators, and auditors for each CA in the hierarchy.

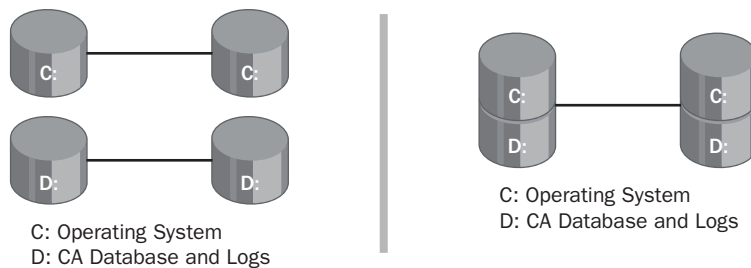


**Warning** Windows Server 2003, Enterprise Edition, allows you to enforce the Common Criteria roles through role separation. With role separation enabled, a user can hold only one of four roles. Individual users who hold two or more of these roles are blocked from all PKI-management activities.

## Minimizing Risk of CA Failure

Your PKI hierarchy design can include measures to prevent the failure of Certificate Services, such as defining hardware specifications that prevent common forms of failure. For example, you can ensure that the CA database's disk partition is on a RAID 5 or RAID 0+1 disk array to ensure the best performance and recoverability in the event of disk failure. Likewise, the CA log files can be placed on a RAID 1 mirror set to protect against disk failure. You can also ensure that disk partitions are large enough to store the volume of certificates for the expected certificate enrollment activity.

Hardware requirements are less demanding for an offline CA than for an online issuing CA. For example, Figure 5-7 shows two disk configurations that can be used to provide recoverability yet minimize the costs spent on hard disks for the offline CA.



**Figure 5-7** Disk configuration recommendations for offline CAs

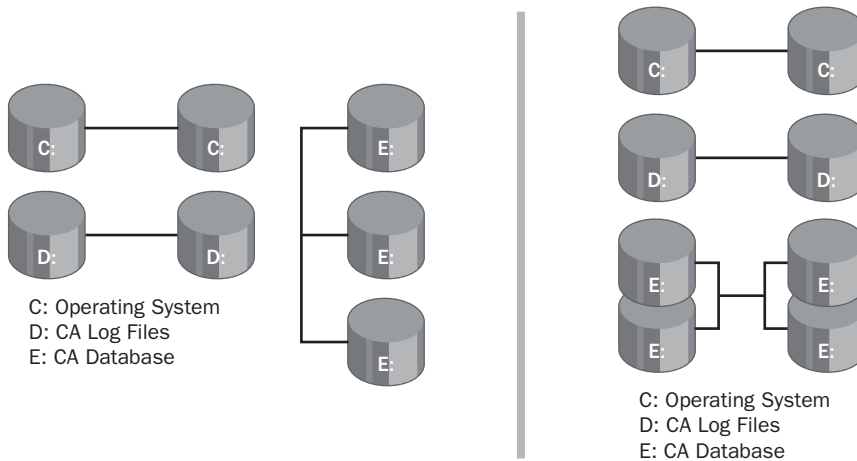
In the left configuration, separate mirror sets are implemented for the operating system and the CA database and logs. This configuration separates all CA data from the operating system volume.

In the right configuration, one mirror set is installed at the offline CA with two partitions. The C partition is dedicated to the operating system, and the D partition is dedicated to the CA database and logs.



**Note** The decision to use one or the other of these two configurations is often based on the number of disks supported by the server that hosts the offline CA or an organization's requirements for installing the operating system on a dedicated partition separate from application data such as the Certificate Services database and log files.

For an online CA, the disk activity performed by Certificate Services is far greater than that of an offline CA when it is turned on. It is recommended that a combination of RAID 1 mirrors and RAID 5 or RAID 0+1 volumes be used to store Certificate Services data. (See Figure 5-8.)



**Figure 5-8** Disk configuration recommendations for an online CA

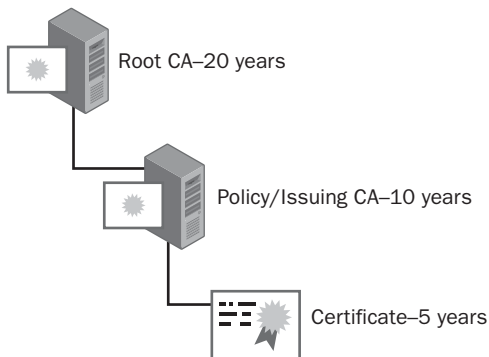
On the left side, the disk configuration is shown using RAID 1 mirror sets for the C drive for the operating system and for the D drive for the CA database log files. The CA database is stored on a RAID 5 stripe set with parity. This configuration provides good performance for reading data from the CA database.

On the right side, the disk configuration is shown using the same RAID 1 mirror sets for the operating system and for CA database log files. In this example, a RAID 0+1 set is used for the CA database. RAID 0+1 mirrors two RAID 0 stripe sets. RAID 0+1 provides higher input/output rates than RAID 5 and is often selected by organizations that foresee large volumes of certificate enrollment traffic on the CA database.

## Determining Certificate Validity Periods

A certificate has a predefined validity period that comprises a start date and time and an end date and time. An issued certificate's validity period cannot be changed after certificate issuance. Determining the validity period at each tier of the CA hierarchy, including the validity period of the certificates issued to users, computers, services, or network devices, is a primary step when defining a CA hierarchy.

The recommended strategy for determining certificate validity periods is to start with the certificates issued to users, computers, services, or network devices by issuing CAs. The main point to remember is that a CA should not issue a certificate that exceeds the remaining lifetime on the CA certificate. Although allowed by the standards, this scenario can lead to certificates with remaining validity periods to expire when the issuing CA's certificate expires. You should ensure that the CA has enough remaining lifetime on its certificate to issue certificates with the required validity periods. A good rule of thumb is to make the CA certificate validity period at least twice as long as the maximum validity period of any CA-issued certificates. Figure 5-9 shows an example of a two-tier CA hierarchy that issues certificates with a maximum validity period of five years.



**Figure 5-9** Determining CA validity periods

In this example, it is known that the maximum validity period for certificates issued by the policy/issuing CA is five years. To ensure that the remaining validity period of the policy/issuing CA does not affect the validity period of the issued certificates, you must double the validity period value of the policy/issuing CA to 10 years.

In addition to doubling the validity period, you can also follow best practices and ensure that the CA renews its CA certificate value at half of the remaining validity period. The first time you renew a CA certificate (after a period of five years in this scenario), you renew with the original key pair. After the next five years pass, you renew the CA certificate with a new key pair. This ensures that the same key pair is never used for a period longer than the intended original validity period of 10 years.

Likewise, the validity period of the root CA certificate should be double the validity period of the policy/issuing CA certificate. In this example, the validity period of the root CA certificate would be 20 years, double the 10-year validity period of the issuing policy CA. As with the policy/issuing CA, it is recommended to renew the root CA certificate at half of its validity period—10 years—by using the same key pair. Again, at the full validity period—20 years—you renew the root CA certificate with a new key pair.

You should not go to extremes with the validity period. The longer a certificate's key pair is valid, the more time an attacker has to try and determine the value of the private key based on public key and examples of the encryption performed by the private key. The risk of determining the private key is even higher if the key length is shorter in length (1024 bits) versus longer in length (4096 bits). Implementing a root CA with a validity period longer than 20 years is not recommended.

## Determining Publication Points

The final technical requirement that must be met in your hierarchy design is determining publication points for both CRLs and CA certificates. The certificate-chaining engine can use the URLs stored in the CRL Distribution Point (CDP) and Authority Information Access (AIA) extensions to determine a certificate's revocation status.



**Note** An application can use other methods for building certificate chains and determining revocation lists. For example, some applications store the files on the local file system while others can hard code URLs for the CRL and CA certificate in their configuration.

At each CA in the hierarchy, you must define publication points for certificates issued by that CA. These publication points allow access to *that* CA's certificate and CRL. The following protocols can be used when defining publication points:

- **Hypertext Transfer Protocol (HTTP) URLs.** HTTP URLs are used for both internal and external publication points. The advantage of HTTP URLs is that there is little lag time between publication and availability. Once you publish an updated CRL or CA certificate to an HTTP URL, it is immediately available for download by PKI-enabled applications. In addition, HTTP URLs can typically be downloaded by clients behind firewalls and those who are not full Active Directory clients, including those running an operating system earlier than Windows 2000 and non-Microsoft clients.

- **Lightweight Directory Access Protocol (LDAP) URL.** A CA certificate or CRL that is published to an LDAP URL is by default published into the configuration naming context of Active Directory. This means that the CRL or CA certificate is available at all domain controllers in the forest. There are three disadvantages to using an LDAP URL:
  - It can take some time for CRLs or CA certificates to fully replicate to all domain controllers in the forest. The actual time depends on your network's replication latency, especially when the replication must take place between sites rather than only between domain controllers in the same site.
  - Nonsupport of the Active Directory–related LDAP URLs can lead to delays in CRL or CA certificate retrieval. If the LDAP URL is the first URL in the URL listing, a non–Active Directory enabled client will time out for 10 seconds before it moves on to the next available URL.



**Note** When multiple URLs exist in the URL listing, the first URL in the list is given 10 seconds to attempt to connect. Each subsequent CDP location will use a maximum of one half of the remaining time to connect to that specific CRL object before continuing to the next location. The maximum time allotted for retrieval is 20 seconds for Windows XP. The time spent attempting to connect to the LDAP URL is dependent on the order of the URL listing.

- **File Transfer Protocol (FTP) URLs.** A CA certificate or CRL can be published to an FTP server for download by PKI-enabled applications. As with HTTP URLs, FTP URLs can be downloaded by clients behind a firewall.
- **File URLs.** A file URL is either a reference to a local file location on the actual CA computer or a reference to a share on a remote file server. File URLs are only recognized by clients who have a redirector loaded that enables communications with the remote file server.



**More Info** More information on choosing publication points can be found in the “Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure” document at <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws3pkibp.mspx>.



The decision as to which protocols to implement for CRL or CA certificate publication depends on the frequency at which you publish URLs, the protocols allowed to traverse network firewalls, and your network's operating systems. To ensure maximum availability, the URLs should be ordered so that the most common protocol used for CRL or CA certificate retrieval is listed first in the CDP extension. Other protocols are then listed in their order of usage.



**Note** Methods for defining CRL and CA certificate publication URLs are discussed in detail in Chapter 6.

## Determining Business Requirements

Business requirements define an organization's goals. Typically, they define how an organization expects the PKI to improve its processes. For example, the following business requirements can affect a CA hierarchy design:

- **Minimizing PKI-associated costs.** When reviewing CA hierarchy designs, you might have to choose a CA hierarchy that deploys the fewest CAs. For example, some organizations combine the roles of policy CAs and issuing CAs into a single CA in the hierarchy, deploying a two-tier hierarchy rather than a three-tier hierarchy.
- **High availability of certificates.** An organization can require that a certificate be consistently available to ensure that no certificate requests fail due to a CA being down for any reason. To ensure that a certificate is consistently available, you must publish the certificate template at more than one CA in the CA hierarchy, protecting against the failure of a single CA. In addition, you can choose to deploy CAs at major hub sites on your network so that certificate requestors can request the certificate from a local CA, rather than one separated by several WAN links.
- **Liability of PKI participants.** A CA hierarchy includes policy CAs that define the liability of the CA in the CPS. The liability should provide sufficient coverage for transactions that use CA-issued certificates. This liability definition must be reviewed by your organization's legal department to ensure that the definitions are legally correct and binding upon all participants in the PKI.

## Determining External Requirements

Not all requirements are defined by an organization. In some cases, especially if you expect to use certificates in conjunction with other organizations, you might have to

meet external requirements, such as those defined by other organizations or by the governments of countries in which your organization conducts business.

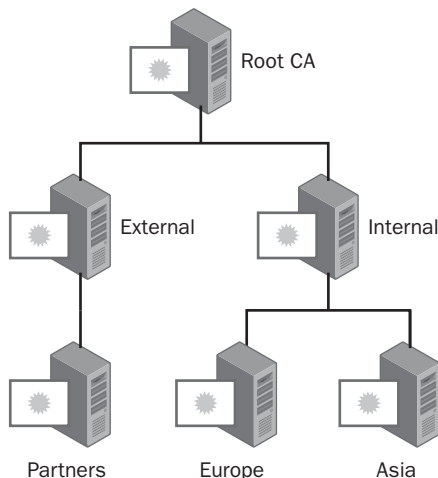
Examples of external requirements include:

- **Enabling external organizations to recognize employee-used certificates.** Different solutions exist for this scenario. You can choose to not deploy an internal PKI and simply obtain certificates from commercial CAs, such as VeriSign or RSA. Alternatively, you can use cross-certification or qualified subordination to define which external certificates you trust.



**Note** Cross-certification and qualified subordination are discussed in detail in Chapter 13.

- **Using your organization's certificate at partner organizations.** In some cases, the certificates issued by your CA hierarchy will be used by your employees for encryption or signing purposes at another organization. You might have to create custom certificates to meet the requirements of the other organization. One solution is to implement a CA hierarchy that defines separate internal and external policy CAs. (See Figure 5-10.)



**Figure 5-10** Implementing separate policy CAs for internal and external use

In this example, all certificates for use with partners are issued by the Partners CA. If different issuance policies are required for these certificates, the issuance policies are defined in the CPS deployed at the external policy CA.

- **Industry or government legislation.** Several countries have legislation that affects the design of a CA hierarchy. For example, Canada recently passed

the Personal Information Protection and Electronic Documents Act. This act regulates the management of a customer's personal information when held by a private-sector company. The act requires that someone be accountable for compliance—and this person should be involved in the deployment and design of the CA hierarchy to ensure that all requirements of the Act are enforced in the design.



**More Info** You can obtain a copy of Canada's Personal Information Protection and Electronic Documents Act at <http://laws.justice.gc.ca/en/p-8.6/91355.html>.

- **Certificates for nonemployees.** If you issue certificates to nonemployees, you must ensure that the CPS outlines nonemployee responsibilities and clearly defines the revocation policy in case you must revoke a certificate. Using a CA hierarchy like the one defined in Figure 5-10, you can deploy a separate certificate policy that includes greater detail for external clients.
- **Validating certificates on external networks.** When designing the configuration of each CA, you must ensure that the CRL and CA certificate are published to externally accessible locations, such as a Web server in a demilitarized zone (DMZ). This allows certificate validation to take place from the external network when using applications, such as extranet Web servers and VPN solutions when connections originate from the Internet.

## Case Study: Identifying Requirements

In this case study, you will identify the technical and business requirements of Fabrikam Industries. These requirements will determine the design of your CA hierarchy.

Fabrikam Industries plans to deploy several PKI-enabled applications, instigating the organization to deploy its own PKI. The design committee for the PKI has identified the following business requirements for the PKI-enabled applications:

- The corporate headquarters are in Atlanta. All network services are managed from that location.
- Fabrikam Industries has international hub sites in Frankfurt, Singapore, and Lima. Several smaller offices connect to the nearest international hub on their continent, and each regional office has its own network services team responsible for network services implemented in that region.
- The international hub sites are connected to the Atlanta site by T3 lines.

- Smaller offices are connected to the nearest international hub with lines between 128 KB and 512 KB.
- The Active Directory structure for Fabrikam is a single forest with four domains: fabrikam.com, americas.fabrikam.com, europe.fabrikam.com, and apac.fabrikam.com.
- Fabrikam.com is an empty forest root domain. Only default accounts exist in the domain in order to separate forest administrative accounts into their own domains.
- Fabrikam implements a Service Level Agreement (SLA) that requires all critical network services to be available at all times. The PKI is a critical network service that must honor the SLA.
- Fabrikam places a high value on security, and the organization has a written security policy. The following sections in the security policy will influence the CA hierarchy's design:
  - Enterprise servers are stored in secure network locations.
  - Private keys for CAs must be protected from tampering and theft.
  - Fabrikam implements a decentralized management structure, and the local administration staff performs management of enterprise servers.
- Fabrikam uses a Web-based factory tracking system. All communications must be protected from interception. In addition, all authentication must implement a two-factor methodology.
- The corporate Web site allows customers to input private information for record-keeping. All private customer information must be protected from interception when input into the corporate Web site.
- Europe and Asia have privacy laws that ensure that all information collected to identify a subscriber is protected against distribution against the wishes of the subscriber. Fabrikam collects information on the subscriber when issuing smart card certificates. The CA hierarchy must provide descriptions of how Fabrikam enforces these privacy laws.

## Case Study Questions

1. How many tiers are required in the Fabrikam CA hierarchy?
2. What additional security measures are required for all CAs?
3. Are there any external requirements for the CA hierarchy?
4. Is role separation required in your CA hierarchy design? If so, how do you implement it?

5. How many policy CAs are required for the CA hierarchy?
6. What CA hierarchy design best fits the organization's requirements?
  - a. A design based on certificate use.
  - b. A design based on geography.
  - c. A design based on company departments.
  - d. A design based on a combination of certificate use and geography.
7. If offline CAs are implemented at the first and second levels of the CA hierarchy, where will you locate the offline CAs?
8. In what domain will the root CA's computer account exist?
9. In what domain will you place policy CA computer accounts?
10. In what domain will you place issuing CA computer accounts?
11. Based on the requirements presented in this case study, draw your proposed CA hierarchy for Fabrikam Industries.
12. Assuming that your design resulted in a three-tier CA hierarchy and the maximum validity period of a certificate issued to users, computers, services, or network devices is five years, what is the validity period of the root CA certificates, the policy CA certificate(s), and the issuing CA certificates?

## Additional Information

- Microsoft Official Curriculum, course 2821: "Designing and Managing a Windows Public Key Infrastructure" ([www.microsoft.com/traincert/syllabi/2821afinal.asp](http://www.microsoft.com/traincert/syllabi/2821afinal.asp))
- Security Requirements for Cryptographic Modules (<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>)
- Certificate Issuing and Management Components Protection Profile ([http://csrc.nist.gov/pki/documents/CIMC\\_PP\\_final-corrections\\_20010126.pdf](http://csrc.nist.gov/pki/documents/CIMC_PP_final-corrections_20010126.pdf))
- Best Practices for Implementing a Microsoft Windows Server2003 Public Key Infrastructure (<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/maintain/operate/ws3pkibp.asp>)
- Personal Information Protection and Electronic Documents Act (<http://laws.justice.gc.ca/en/p-8.6/91352.html>)
- Designing a Public Key Infrastructure ([http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dssch\\_pki\\_overview.asp](http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dssch_pki_overview.asp))



## Chapter 6

# Implementing a CA Hierarchy

Once you design your PKI hierarchy, it's time to install a certification authority (CA) hierarchy that follows the design. Implementation of a CA hierarchy always begins at the root CA and proceeds to the direct subordinates of the root CA. The process continues until all CAs in the hierarchy are installed.

This chapter will provide detailed instructions for installing a CA hierarchy. The instructions can be used to build a hierarchy with a single CA or a hierarchy with two or more tiers.

### How to Use This Chapter

---

This chapter is divided into sections based on the number of tiers in a CA hierarchy. Table 6-1 outlines the chapter sections you should read based on the number of tiers in your CA hierarchy.

**Table 6-1 Road Map for Installation**

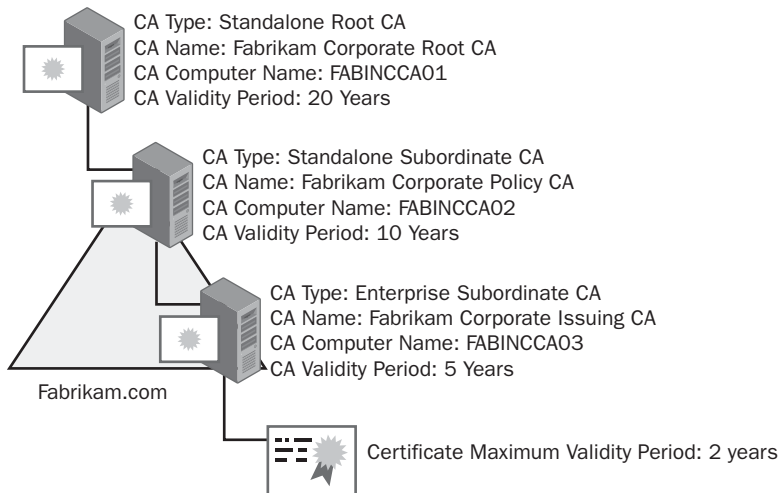
---

Type of CA Hierarchy	Recommended Sections
One tier	“Preparing Configuration Scripts for Installation” “Implementing an Enterprise Root CA” “Verifying Installation”
Two tiers	“Preparing Configuration Scripts for Installation” “Implementing a Standalone Root CA” “Implementing an Online Issuing CA” “Verifying Installation”
Three tiers	“Preparing Configuration Scripts for Installation” “Implementing a Standalone Root CA” “Implementing an Offline Policy CA” “Implementing an Online Issuing CA” “Verifying Installation”

---

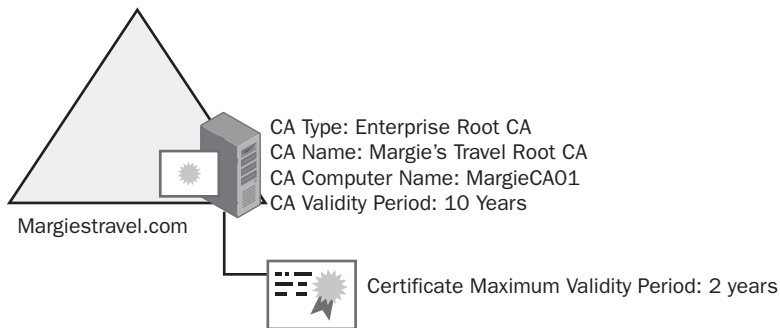
The first section, “Preparing Configuration Scripts for Installation,” is applicable to all CA hierarchy designs, as it introduces the configuration and script files essential to ensuring that the CAs in your hierarchy are configured correctly. By using script files, you can: ensure that desired settings are reproducible, provide documentation on each CA’s configuration, and secure the ability to recover a CA’s configuration in the event of a failure.

I’ll use a three-tier CA hierarchy built for Fabrikam Industries Inc. as the primary example in the chapter. (See Figure 6-1.)



**Figure 6-1** Fabrikam’s three-tier CA hierarchy

This chapter will also discuss a single-tier CA, suitable for a smaller company—Margie’s Travel in the example—where certificates are issued primarily for internal purposes. (See Figure 6-2.)



**Figure 6-2** A single-tier CA hierarchy for Margie’s Travel



# Preparing Configuration Scripts for Installation

During CA installation, you must define configuration files and scripts accurately. This section provides background information on these configuration files and scripts so you can tailor them to your organization.

## CAPolicy.inf File

The CAPolicy.inf file provides Certificate Services configuration information, which is read during initial CA installation and whenever you renew a CA certificate. The CAPolicy.inf file defines settings specific to root CAs, as well as settings that affect all CAs in the CA hierarchy. The CAPolicy.inf file provides the following information for a root CA:

- **Certificate revocation list (CRL) publication points.** When validating a certificate chain, the certificate chaining engine must validate every certificate in the chain. Rather than using the default CRL publication points, you can define custom revocation points based on your network's configuration. The actual order of the publication points is important because a client attempts to retrieve the CRL in the order defined in the CAPolicy.inf file.
- **CA certificate publication points.** The certificate chaining engine might have to download the root CA's certificate. This section of the CAPolicy.inf file defines the publication points for the root CA's certificate. The actual order of the publication points is important because a client attempts to retrieve the CA certificate in the order defined in the CAPolicy.inf file.
- **Enhanced Key Usage.** The CAPolicy.inf file can limit the application purposes of certificates issued by the CA. For example, if you limit the CA to issuing certificates for client authentication, server authentication, or secure e-mail, the CA cannot issue any certificates for the purpose of code signing.
- **The renewal configuration.** The CAPolicy.inf defines the renewal key length and validity period for the root CA's certificate. Typically, this section of the CAPolicy.inf file is configured to match the initial key length and validity period defined for the root CA. Matching the initial key length and validity period ensures that the designed settings are not modified when the CA's key pair is renewed.



**Note** You can only designate the cryptographic service provider (CSP) used by the CA at installation time. You cannot change the CSP by modifying the CAPolicy.inf file.

The CAPolicy.inf file is also used in the installation of subordinate CAs in the hierarchy. The following settings in the file can be defined for both root and subordinate CAs:

- **Certificate practice statement (CPS) information.** The CPS defines the operating procedures and practices employed at the CA, as well as at subordinate CAs, which enforce the certificate policies implemented at the CAs. The CPS is typically applied at:
  - The root CA in a single-tier CA hierarchy.
  - The combination policy CA/issuing CA in a two-tier CA hierarchy.
  - The policy CAs in a three-tier CA hierarchy.



**Note** A CPS is considered to be effective for the CA in which the CPS is defined and for all subordinate CAs.

- **CRL publication interval.** The base CRL is published at the interval defined in the CAPolicy.inf file.
- **Delta CRL publication interval.** The delta CRL is published at the interval defined in the CAPolicy.inf file. If the interval is defined as a value of zero, the publication of delta CRLs is disabled at the CA.
- **Basic Constraints.** Limitations can be set on the number of certificates allowed below the CA in which the CAPolicy.inf file is defined. Basic Constraints protect against complex hierarchies that implement long certificate chains. They also indicate whether the certificate is issued to a CA or to an end entity other than a CA.

## Creating the CAPolicy.inf File

By default, the CAPolicy.inf file does not exist when you install Microsoft Windows Server 2003. You must manually create the file in the Windows operating system folder (%windir% folder). When you install Certificate Services, the operating system applies any settings defined in the CAPolicy.inf file.



**Warning** Be sure the file is named CAPolicy.inf and is stored in the %windir% folder. It is a common mistake to create the file in Notepad and save the file as CAPolicy.inf.txt. To prevent this, change the file type to All Files from the default of Text Document (\*.txt).

## Sample CAPolicy.inf Contents

You can implement defined settings when you create a CAPolicy.inf file, depending on which CA in the CA hierarchy you apply the file to. A template for the CAPolicy.inf file follows:

```
[Version]
Signature= "$Windows NT$"

[PolicyStatementExtension]
Policies = LegalPolicy
Critical = 0

[LegalPolicy]
OID = 1.3.6.1.4.1.311.21.43
Notice = "Legal policy statement text."
URL = "http://www.example.com/certdata/cps.asp"

[AuthorityInformationAccess]
Empty = true
;URL = http://%1/Public/My CA.crt
;URL = ftp://ftp.example.com/Public/MyCA.crt
;URL = file://\%1\Public\My CA.crt
Critical = false

[CRLDistributionPoint]
Empty = true
;URL = http://%1/Public/My CA.crl
;URL = ftp://%1/Public/MyCA.crl
;URL = file://\%1\Public\My CA.crl
Critical = true

[EnhancedKeyUsageExtension]
OID = 1.3.6.1.4.1.311.21.6 ; szOID_KP_KEY_RECOVERY_AGENT
OID = 1.3.6.1.4.1.311.10.3.9 ; szOID_ROOT_LIST_SIGNER
OID = 1.3.6.1.4.1.311.10.3.1 ; szOID_KP_CTL_USAGE_SIGNING
Critical = false

[basicconstraintsextension]
pathlength = 4
critical=false

[certsrv_server]
renewalkeylength=4096
RenewalValidityPeriodUnits=20
RenewalValidityPeriod=years
CRLPeriod = days
CRLPeriodUnits = 2
CRLDeltaPeriod = hours
CRLDeltaPeriodUnits = 4
```



**More Info** A sample CAPolicy.inf file is included with the materials related to this chapter on the accompanying CD-ROM.

## CAPolicy.inf File Sections

Within the CAPolicy.inf file, there are several predefined sections, each of which defines specific settings for Certificate Services. These sections and related decisions regarding their contents are outlined here, as well as whether the section applies to root CA installations, subordinate CA installations, or to both root and subordinate CA installations.

### [Version]

The [Version] section defines that the .inf file uses the Windows NT format. This section must exist for both root and subordinate CA installations. It contains a single line:

```
Signature= "$Windows NT$"
```

### [PolicyStatementExtension]

The [PolicyStatementExtension] section defines a CA's CPSs and certificate policies. This section's inclusion depends on the number of tiers in the CA hierarchy.

In a single-tier CA hierarchy, the [PolicyStatementExtension] and related [*Policy-Name*] sections are defined at the root CA. In a two-tier CA hierarchy, you should include the [PolicyStatementExtension] and related [*PolicyName*] sections at each issuing CA in the hierarchy. In a three-tier CA hierarchy, the [PolicyStatementExtension] and related [*PolicyName*] sections should be defined at the policy CAs on the second tier. If different CPSs are required, they are defined at each policy CA.

In the [PolicyStatementExtension] section, you define one or more subsections. Within the subsections, you define a minimum of three settings:

- **Object identifier (OID).** An object identifier can be applied to each CPS. The OID is an identifier that is tied to the CPS or, if multiple policies are defined, to each CA's certificate policy.



**Note** There is a practical limit to the number of certificate policies that can be included in a CA certificate. The Active Directory schema only allows a maximum string length of 4,096 bytes for all CPS information, including OID, notification text, and URL. The total length of the certificate policy entries must be less than 4,096 bytes.

## Where Do I Get an OID?

An OID is a unique sequence of numbers that identifies a specific directory object or attribute. You can define an OID for a CPS as either a public OID or a private OID.

If your organization plans to use PKI-enabled applications in conjunction with other organizations, you must obtain an OID from a public number-assignment company to ensure that your OID will be unique on the Internet. Sources for public OIDs include:

- **The Internet Assigned Numbers Authority (IANA).** This source issues free OIDs under the Private Enterprises arc. Every OID assigned by the IANA begins with the numbers 1.3.6.1.4.1 representing iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).

**Note** An *arc* is the term used to reference a specific path in the global OID tree maintained by the International Organization for Standardization (ISO) and the International Telecommunication Union (ITU). This global OID tree is sometimes referred to as the joint ISO/ITU-T tree. For example, the Private Enterprises arc contains all OIDs that begin with 1.3.6.1.4.1.

- **The American National Standards Institute (ANSI).** This source issues OIDs for purchase under the U.S. Organizations arc of the ANSI OID tree. Every OID assigned by the ANSI begins with the numbers 2.16.840.1 representing joint-iso-itu-t(2).country(16).US(840).US company arc(1).
- **Other countries.** Each country has its own OID-management organization. The easiest way to find the organization for a given country is to perform a Google search ([www.google.com](http://www.google.com)) with the search phrase *Country* (where *Country* is the name of the given country) and “Object Identifier.” Here are some examples of the arcs available within the joint ISO/ITU-T tree:
  - Canada: joint-iso-itu-t(2).country(16).canada(124)
  - Netherlands: joint-iso-itu-t(2).country(16).netherlands(528)
  - Switzerland: joint-iso-itu-t(2).country(16).switzerland(756)
  - Thailand: joint-iso-itu-t(2).country(16).thailand(764)

- **Notice.** The Notice line provides the text that appears when a user clicks the Issuer Statement button when the CA's certificate is displayed. The Issuer Statement is typically the title of the CPS and does not display any details about the CPS. Remember that you are limited to 4,096 bytes of data in the Certificate Policies extension—including the entire CPS in the Notice line will result in a very large CA certificate with the entire text of the CPS in the CA certificate.
- **URLs.** Multiple URLs can be provided for the CPS. The URLs provide links to the actual text of the CPS. When you view the Notice text, a button labeled More Info opens a browser window that displays the content of the URL specified in the URL line. Typically, the URL is a Hypertext Transfer Protocol (HTTP) or File Transfer Protocol (FTP) URL.

You can also generate a private OID based on your forest's globally unique identifier (GUID) within the Microsoft IANA-assigned tree. If you decide to use these OIDs, you will have an OID assigned from 1.3.6.1.4.1.311.21.8.*a.b.c.d.e*.1.402 (where *a.b.c.d.e* is a unique string of numbers based on your forest's GUID).



**Note** Use this private OID tree only if you do not foresee using the OIDs in conjunction with other organizations and your organization is unwilling to obtain a free OID from the IANA. If you plan on using PKI-enabled applications within other organizations, obtain a free OID tree from the IANA or buy a tree from the ANSI.



**Tip** You can obtain your forest's private OID by opening the Certificate Templates (certtmpl.msc) console as a member of the Enterprise Admins group. In the console tree, right-click Certificate Templates and click View Object Identifiers. In the resulting dialog box, you can choose the High Assurance Object Identifier and click the Copy Object Identifier button. Once you copy the OID, you can plug your forest's values into the placeholders *a.b.c.d.e* and remove any trailing digits.

### **[AuthorityInformationAccess] and [CRLDistributionPoint]**

The [AuthorityInformationAccess] and [CRLDistributionPoint] sections specify the publication points for a root CA's certificate and CRL. Subordinate CAs disregard these sections because the CRL and CA certificate distribution points are defined in the configuration of the parent CA, not at subordinate CAs.

There are two strategies you can use when designing the CA certificate and CRL publication points for a root CA. Choosing which strategy to follow depends on your organization's security policy and the PKI-enabled applications it deploys.

The first strategy is to not publish CA certificate and CRL retrieval URLs in the root CA's certificate. By excluding the Authority Information Access (AIA) and CRL Distribution Point (CDP) extensions from the root CA certificate, you block the certificate chaining engine from checking the root CA certificate's revocation status. The root CA certificate is designated as trusted by adding the certificate to the trusted root CA store at client computers. If the root CA certificate is compromised, you must redeploy your entire PKI rather than just revoke the root CA certificate.

Most applications do not check revocation status of the root CA certificate unless it contains a CDP extension. Removing the AIA and CDP extensions from the root CA certificate ensures that *all* applications bypass revocation checking on the root CA certificate.

To prevent the inclusion of the AIA and CDP extensions in the root CA certificate, include the following lines in your CAPolicy.inf file:

```
[AuthorityInformationAccess]
Empty = true

[CRLDistributionPoint]
Empty = true
```



**Note** Alternatively, you can just add [AuthorityInformationAccess] and [CRLDistributionPoint] with no entries in the sections to suppress the inclusion of AIA and CDP extensions in the root CA certificate.

The second strategy is to define the exact URLs where you publish the root CA's certificate and CRL. The order in which you define the URLs is important for the cryptoAPI, as it dictates the search order that a Windows client uses when downloading the CA certificate or CRL.



**Note** Design considerations for the URL order of the AIA and CDP extensions are discussed in detail in Chapter 9.

If you decide to define AIA and CDP URLs for the root CA certificate, you can use predefined variables, rather than coding the actual URLs. Windows Server 2003 provides the variables shown in Table 6-2 for defining AIA and CDP URL paths.

**Table 6-2 AIA and CDP Variable Definitions**

Variable	Name	Description
%1	<i>ServerDNSName</i>	The CA computer's DNS name
%2	<i>ServerShortName</i>	The CA computer's NetBIOS name
%3	<i>CAName</i>	The CA's logical name
%4	<i>CertificateName</i>	The name of the CA's certificate file
%5	<i>DomainDN</i>	Not used in the Windows Server 2003 PKI
%6	<i>ConfigDN</i>	The Lightweight Directory Access Protocol (LDAP) path of the forest's configuration naming context for the forest
%7	<i>CATruncatedName</i>	The CA's "sanitized" name
%8	<i>CRLNameSuffix</i>	The CRL's renewal extension
%9	<i>DeltaCRLAllowed</i>	Indicates whether delta CRLs are supported by the CA
%10	<i>CDPObjectClass</i>	Indicates that the object is a CDP object in Microsoft Active Directory
%11	<i>CAObjectClass</i>	Indicates that the object is a CA certificate object in Active Directory

When variables are used in the CAPolicy.inf file, the installation of Certificate Services parses the file and replaces the variables with the actual names implemented by the CA. For example, if you do not define a [CRLDistributionPoint] section, a root CA implements the following default paths for CRL publication:

- %windir%\System32\CertSrv\CertEnroll\%3%8%9.crl
- ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10
- http://%1/CertEnroll/%3%8%9.crl
- file://\%1\CertEnroll\%3%8%9.crl

Likewise, if you do not define an [AuthorityInformationAccess] section within a CAPolicy.inf file, a root CA implements the following default paths for CA certificate publication:

- %windir%\system32\CertSrv\CertEnroll\%1\_%3%4.crt
- ldap:///CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11
- http://%1/CertEnroll/%1\_%3%4.crt
- file://\%1\CertEnroll\%1\_%3%4.crt





**Note** Although presented here, including AIA and CDP extensions in the root CA certificate is not recommended. You can leverage this information on using variables when defining publication points for CRLs and CA certificates for subordinate CAs.

### [EnhancedKeyUsageExtension]

This section is used to restrict the types of certificates a CA can issue. For example, if you want to restrict a CA to issuing certificates for Client Authentication, Server Authentication, and Secure Email, you would define the [EnhancedKeyUsageExtension] as shown here:

```
[EnhancedKeyUsageExtension]
OID = 1.3.6.1.5.5.7.3.2 ; Client Authentication
OID = 1.3.6.1.5.5.7.3.1 ; Server Authentication
OID = 1.3.6.1.5.5.7.3.4 ; Secure Email
```



**Note** These OIDs are predefined by the IANA or by Microsoft. You can view the list of predefined OIDs in the Certificate Templates console using the same method you use to identify your forest's privately assigned OID tree.

### [BasicConstraintsExtension]

The [BasicConstraintsExtension] section allows you to define path-length restrictions. A path-length restriction allows you to limit the depth of your CA hierarchy. For example, if you only want one more tier below the current CA, you can define the [BasicConstraintsExtension] section as shown here:

```
[BasicConstraintsExtension]
pathlength = 4
```



**Note** All CA certificates have a Basic Constraints extension, even if you do not define the section in the CAPolicy.inf file. The Basic Constraints extension indicates whether the certificate is issued to a CA or to a user, computer, service, or network device. CA certificate identification allows the chaining engine to determine whether the certificate can be used to sign other certificates.

**[certsrv\_server]**

The [certsrv\_server] section has entries that apply to all CAs in the CA hierarchy. The following entries can be defined in this section:

- **RenewalKeyLength.** The requested length of the CA's private key and public key when the CA certificate is renewed. The value should match the value assigned to the CA's key length during initial installation, unless you decide to modify the length of the CA's certificate at renewal time.
- **RenewalValidityPeriod.** The validity period's unit of measurement. Accepted values are years, weeks, and days, though use of anything other than years is uncommon.
- **RenewalValidityPeriodUnits.** The specific number of units for the validity period. For example, if you configure a CA with a 15-year validity period, the RenewalValidityPeriodUnits value is 15.



**Note** You cannot set the initial CA key length and validity period in the CAPolicy.inf file. The value at installation is configured in the installation wizard for a root CA and is defined by the parent CA for all subordinate CAs. The CAPolicy.inf file only contains the values used when you renew the CA certificate for all CAs in the CA hierarchy.

- **CRLPeriod.** The CRL publication interval's unit of measurement. The default value is days, but years, weeks, days, and hours are acceptable.
- **CRLPeriodUnits.** The specific number of units for the CRL publication interval. The default value is seven, but this value is typically changed based on the CA's design.
- **CRLDeltaPeriod.** The unit of measurement for the delta CRL publication interval. The default unit or value is days, but years, weeks, days, and hours are acceptable.
- **CRLDeltaPeriodUnits.** The specific number of units for the delta CRL publication interval. The default value is 1, but this value is typically changed based on the CA's design.

## Pre-Installation Scripts

When installing subordinate CAs in a multi-tier CA hierarchy, you must manually install your root CA certificate so that the subordinate CA considers the root CA to be a trusted root CA. In addition, you might have to publish the root CA's CRL so that the subordinate CA can perform CRL checking on any root CA-issued certificates.

If the subordinate CA is at the third or lower tier of the CA hierarchy, you might have to install intermediate CA certificates and CRLs for the CAs that exist between the subordinate and root CAs. Rather than installing these certificates to the trusted root store, the certificates are installed to the intermediate CA store.



**Note** If you do not install the certificates and CRLs before installation of the subordinate CA, you might receive an error message when you install the subordinate CA certificate stating that the CA cannot determine the revocation status of the CA certificate.

### Publishing Certificates and CRLs to the Local Computer Store

You must be a member of the local Administrators group to add CRLs and certificates to the local computer store. The combination of certificates and CRLs that must be installed depends on the where the target CA exists in the CA hierarchy:

- If the new CA is installed at the second tier of the hierarchy, you only have to install the root CA's certificate and CRL.
- If the new CA is at the third tier of the hierarchy or lower, you must install all CA certificates and CRLs in the certificate chain above the new CA.

To add a root CA's certificate to the trusted root CA store of the computer, you can use the following command:

```
certutil -addstore -f Root CACertificateFile.crt,
```

where *CACertificateFile* is the file name of the root CA's certificate file.

Use the following command to add a root CA's CRL to the trusted root CA store:

```
certutil -addstore -f Root CACRLFile.crl,
```

where *CACRLFile* is the file name of the root CA's CRL file.

To add a subordinate CA's certificate to the intermediate CA store, you can use the following command:

```
certutil -addstore -f CA CACertificateFile.crt,
```

where *CACertificateFile* is the file name of the subordinate CA's certificate file.

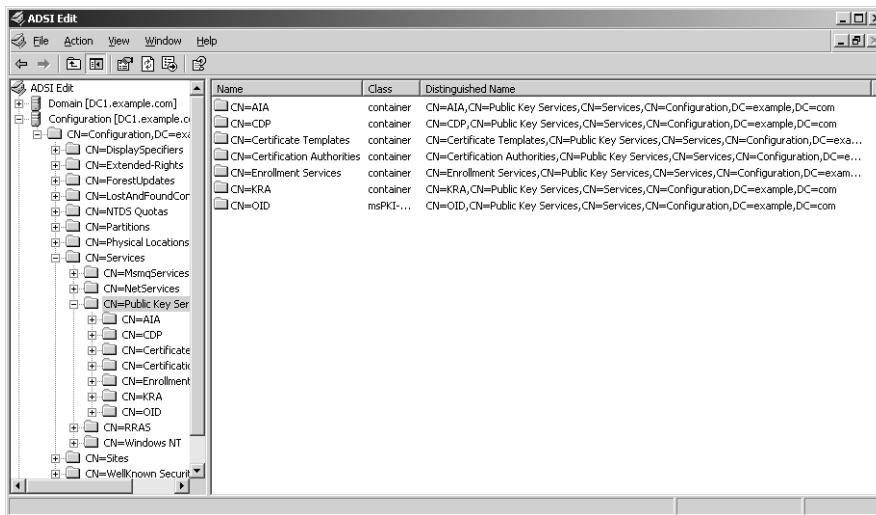
Use the following command to add a subordinate CA's CRL to the intermediate CA store:

```
certutil -addstore -f CA CACRLFile.crl,
```

where *CACRLFile* is the file name of the subordinate CA's CRL file.

## Publishing Certificates and CRLs to Active Directory

In addition to publishing the CA certificates and CRLs to the local machine store of subordinate CAs, you can publish CA certificates and CRLs for any offline CAs to Active Directory. By publishing the CA certificates to Active Directory, you ensure the automatic propagation of CA certificates and CRLs to all Windows 2000, Windows XP, and Windows Server 2003 forest members. The published CA certificates and CRLs are automatically downloaded to the Windows 2000, Windows XP, and Windows Server 2003 forest members through Group Policy application. The application of Group Policy triggers the autoenrollment mechanism, initiating the automatic download of any certificates or CRLs published in Active Directory to the forest members. Figure 6-3 shows where the CA certificates and CRLs are published when they are published into Active Directory.



**Figure 6-3** Active Directory publication locations

In Figure 6-3, CA certificates are published into the following locations:

- All CA certificates are published into the CN=AIA,CN=Public Key Services, CN=Services,CN=Configuration,*ForestRootDomain* (where *ForestRootDomain* is the LDAP distinguished name of your organization's forest root domain) container.
- Root CA certificates are also published into the CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration,*ForestRootDomain* container.
- Enterprise CA certificates are published into the CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,DC=*ForestRootDomain* object.



**Note** The AIA container and Certification Authorities container are used by the certificate chaining engine to acquire certificates for chain building. For example, subordinate CA certificates are only included in the AIA container, while root CA certificates are included in both the AIA and Certification Authorities container. The NTAuthCertificates container indicates CAs that can issue certificates used for smart card logon.

Figure 6-3 shows how CRLs are published into unique containers within the `CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,ForestRootDomain` container. For example, the CRL for the server with the NetBIOS name `GAXGPCA01PK` is published within the `CN=GAXGPCA01PK,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,ForestRootDomain` container.

Use the following `certutil.exe` command line to publish a CA's CRL into Active Directory:

```
certutil -dspublish -f CAName.crl,
```

where *CAName* is the logical name of the root CA.



**Note** If the CA certificate file's name contains spaces, you must delimit the file name with quotes. For example, the command line to publish the Fabrikam root CA certificate would be **`certutil -dspublish -f "Fabrikam Corporate Root CA.crt" RootCA`**.

When adding a CA's CRL into Active Directory, there is no difference between publishing a root CA and a subordinate CA CRL. Use the following command to publish the CRL:

```
certutil -dspublish -f CACRLFile.crl,
```

where *CACRLFile* is the file name of the CA's CRL file.



**Note** If publication fails, an error in the CRL might contain insufficient LDAP information regarding the CRL publication location. You can force publication into Active Directory by adding the CA's NetBIOS name to the publication command. For example, if the NetBIOS name of Fabrikam's root CA is `FABINCCA01`, the command to publish the Fabrikam root CA's CRL is **`certutil -dspublish -f "Fabrikam Corporate Root CA.crl" FABINCCA01`**.

Once the CA certificates and CRLs are published into Active Directory, you can force their propagation at each client computer using the Group Policy application to trigger the autoenrollment engine, resulting in the propagation of the certificates and CRLs to the client computer.

- At Windows 2000 computers, a user can type **secedit /refreshpolicy machine\_policy /enforce**.
- At Windows XP and Windows Server 2003 computers, a user can type **gpupdate /target:computer /force**.

Alternatively, publication also takes place the next time the computer restarts. The restart forces the triggering of the autoenrollment engine. If you do not want to restart the computer, you could wait for a period of 90 minutes for the default Group Policy application to trigger the autoenrollment period.

## Post-Installation Scripts

Once Certificate Services is installed, you can complete configuration by scripting several certutil.exe commands. The benefit of using the certutil commands in a batch file is that the configuration is reproducible, and it allows you to validate the configuration and fix any errors.

Some of the configuration areas to include in the post-installation script are described in this chapter.



**Note** Although reviewed separately, the next chapter sections are combined in a single script file on the CD-ROM for post-installation configuration. This book does not show every possible configuration using the certutil command in a script.

## Declaring the Configuration Naming Context

One of the first tasks required for a post-installation script file is to declare the forest's configuration naming context. The configuration naming context replicates to all domain controllers in the forest and contains the publication points for all CA certificates and CRLs. (See Figure 6-3.)

To define the configuration naming context for your forest, use the following certutil command, where *ForestRootDomain* is the LDAP distinguished name of your organization's forest. This command defines the variable %6:

```
certutil -setreg CA\DSConfigDN CN=Configuration,ForestRootDomain
```

## Defining CRL Publication Intervals

A post-installation script is commonly used to ensure that CRL and delta CRL publication intervals are defined correctly. Although you can define these settings in the CAPolicy.inf file, adding the settings to a post-installation script ensures consistent application of the required settings.

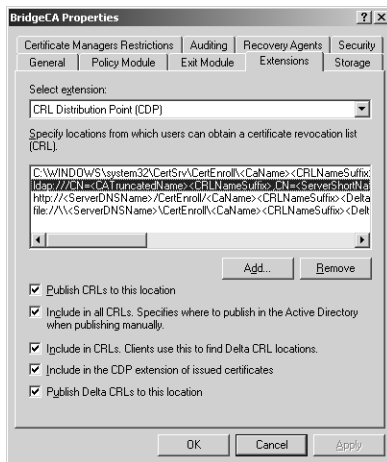
Adding the following entries to a post-installation script ensures that Certificate Services implements the desired publication intervals:

```
::Define CRL Publication Intervals
certutil -setreg CA\CRLPeriodUnits 26
certutil -setreg CA\CRLPeriod "Weeks"
certutil -setreg CA\CRLDeltaPeriodUnits 0
certutil -setreg CA\CRLDeltaPeriod "days"
```

In this example, the CRL publication interval is set to every 26 weeks and the publication of delta CRLs is disabled with its interval set to zero days.

## Defining Publication Points

One of the key tasks after installing Certificate Services is defining publication points for a CA's certificate and CRL. The publication points can be configured in the CA console in the CA's Properties dialog box. (See Figure 6-4.)



**Figure 6-4** Defining CRL distribution points

This dialog box allows you to choose between CDP URLs and AIA URLs. In both cases, you must also choose the URL path where the CRL or AIA will be referenced.

Table 6-3 shows the options available for CRL publication locations.

**Table 6-3 CRL Publication Options**

<b>Display Name</b>	<b>Description</b>	<b>Label</b>	<b>Value</b>
Publish CRLs to this location.	Identifies locations to which the CA should automatically or manually publish the physical CRL files.	<i>ServerPublish</i>	1
Include in all CRLs. Specifies where to publish in Active Directory when publishing manually.	Used for providing the LDAP URL where the CRL is stored in Active Directory. Commonly used to designate the LDAP URL for offline CA CRLs.	<i>AddtoCertCDP</i>	2
Include in CRLs. Clients use this to find delta CRL locations.	Places a URL for delta CRL retrieval in a base CRL. This publication point is stored in the freshest CRL extension of a CRL and is only retrieved during the CRL checking process.	<i>AddtoFreshestCRL</i>	4
Include in the CDP extension of issued certificates.	Places a URL in the CDP extension of a certificate issued by the CA to allow the relying party certificate chaining engine to download the latest CRL version.	<i>AddtoCRLCDP</i>	8
Publish delta CRLs to this location.	If the CA is configured to enable delta CRLs, the delta CRL files are published to this location.	<i>ServerPublishDelta</i>	64

For each location, you can choose to enable any combination of check boxes by adding the numbers in the Value column. For example, if you want to enable the publication of CRLs and delta CRLs, a value of 65 will accomplish this.

Likewise, there are specific entries for CA certificate publication locations. When you enable these options, the URLs are placed in the AIA extension of issued certificates. Table 6-4 shows the values that are available for AIA publication URLs.

**Table 6-4 AIA Publication Options**

<b>Display Name</b>	<b>Description</b>	<b>Label</b>	<b>Value</b>
Publish CRLs to this location.	Identifies locations to which the CA should automatically or manually publish the physical CRL files.	<i>ServerPublish</i>	1
Include in the AIA extension of issued certificates.	Includes the URLs for the CA certificate in all issued certificates.	<i>AddtoCertCDP</i>	2
Include in the online certificate status protocol (OCSP) extension.	Includes the HTTP URL for the designated OCSP server in all issued certificates.	<i>AddtoCertOCSP</i>	32



As with the CDP extensions, you can determine which check boxes to enable for each AIA extension by referencing the numbers in the Value column and adding the numbers.

### Defining CRL Distribution Points

You can define a CA's CDP URLs by using the `certutil` command to edit the *CRL-PublicationURLs* registry entry. The command allows you to designate one or more URLs, as well as which CRL publication options are enabled for each URL.

For example, consider the following `certutil` command that defines the CDP extension:

```
certutil -setreg CA\CRLPublicationURLs "1:%windir%\system32\CertSrv\
CertEnroll\%3%8%9.crl\n2:http://www.fabrikam.com/CertData/%3%8%9.crl\
n10:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10"
```

This command defines three separate URLs. The URL order is important when implementing Windows clients, as it defines the order in which the certificate chaining engine searches URLs when retrieving an updated CRL version. Likewise, the number that precedes each URL represents the enabled options for each URL.



**Note** Each URL is separated by `\n`. This character combination is the line separation indicator used for multi-valued registry entries.

- **1:%windir%\system32\CertSrv\CertEnroll\%3%8%9.crl.** This URL ensures that the CRL file is copied to the local file system every time the CRL is automatically or manually published.
- **2:http://www.fabrikam.com/CertData/%3%8%9.crl.** This URL ensures that the URL *www.fabrikam.com/CertData/%3%8%9.crl* is included in the CDP extension of all issued certificates.
- **10:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10.** This URL enables two values: 2 to designate the CRL's publication point in Active Directory and 8 to include the CDP URL in all CA-issued certificates.



**Note** Notice that the variables used in the `certutil` commands are the same as those used in the `CAPolicy.inf` file. The only difference is that the variables are prefixed with `%`, rather than `%`. The additional `%` character is an escape character required by `certutil`.

## Defining CA Certificate Distribution Points

As with the CDP extension, you can modify the AIA extension to designate CA certificate publication points. This is accomplished by using the `certutil` command to modify the `CACertPublicationURLs` registry entry, as shown here:

```
::Modify the AIA Extension URLs
certutil -setreg CA\CACertPublicationURLs "1:%windir%\system32\CertSrv\
CertEnroll\%1_%3%4.crt\n2:http://www.fabrikam.com/CertData/
%1_%3%4.crt\n2:ldap:///CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11"
```

The example places three entries in the registry value:

- **1:%windir%\system32\CertSrv\CertEnroll\%1\_%3%4.crt.** Ensures that the CA certificate is published to the local file system.
- **2:http://www.fabrikam.com/CertData/%1\_%3%4.crt.** Ensures that the HTTP URL is included in the AIA extension of all issued certificates.
- **2:ldap:///CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11.** Ensures that the LDAP URL is included in the AIA extension of all issued certificates.

## Defining Validity Periods for Issued Certificates

Another CA configuration option that can be defined with `certutil` is the maximum validity period for any CA-issued certificate. The manner in which the validity period for issued certificates is applied depends on whether the CA is a standalone CA or an enterprise CA.

In the case of a standalone CA, the definition of a validity period defines the validity period for all CA-issued certificates. In the case of an enterprise CA, the maximum validity period acts as a maximum value for any CA-issued certificates. An issued certificate is always assigned the lesser value of the remaining validity period of the CA certificate and the configured maximum validity period. In other words, if you define the maximum validity period as four years and the CA only has three years remaining in its certificate's validity period, the validity period of a newly issued certificate is three years.

In the case of an enterprise CA, another variable enters the picture. Enterprise CAs issue certificates based on certificate templates. Each certificate template has its own configured validity period. The applied validity period for certificates issued by an enterprise CA is the minimum value of the CA certificate's remaining validity period, the CA's maximum validity period setting, and the certificate template's validity period.

To configure the maximum validity period for issued certificates, two `certutil` commands are required to modify the two related registry entries: *ValidityPeriodUnits* and *ValidityPeriod*. The following example shows the combination to set the maximum validity period to 10 years.

```

::Set Validity Period for Issued Certificates
certutil -setreg CA\ValidityPeriodUnits 10
certutil -setreg CA\ValidityPeriod "Years"

```

## Enabling Auditing at the CA

You can enable auditing on a CA in Windows Server 2003 to provide an audit log for all Certificate Services management tasks. To enable auditing, you must ensure that both success and failure auditing are applied to either the Local Security Policy of an offline CA or a Group Policy object (GPO) applied to the organizational unit (OU) containing the CA's computer account for an online CA. All Certificate Services auditing is reported to the security log in Event Viewer.

### PKI Auditing Categories

The following auditing categories can be enabled or disabled on a CA-by-CA basis.

- **Back up and restore the CA database.** Any attempt to back up or restore the CA database is logged to the Windows security log.
- **Change CA configurations.** Any attempt to modify CA configurations is logged. This can include attempts to define AIA and CDP URLs or a key recovery agent.
- **Change CA security settings.** Any attempt to modify CA permissions is logged. This can include adding CA administrators or certificate managers.
- **Issue and manage certificate requests.** Logs any attempt by a certificate manager to approve or deny certificate requests with subject approval pending.
- **Revoke certificates and publish CRLs.** Logs any attempt by a certificate manager to revoke an issued certificate or by a CA administrator to publish an updated CRL.
- **Store and retrieve archived keys.** Logs any attempt by the enrollment process to archive private keys in the CA database or by certificate managers to extract archived private keys from the CA database.
- **Start and stop Certificate Services.** Any attempt by the CA administrator to start or stop Certificate Services is logged.



**Note** To modify these settings in the properties of the CA, you must be assigned the Manage Auditing and Security Log user right at the CA.

**PKI Auditing Details**

Table 6-5 summarizes the security log entries related to Certificate Services auditing.

**Table 6-5 Certificate Services Event IDs**

<b>Event ID</b>	<b>Event Description</b>
772	The certificate manager denied a pending certificate request.
773	Certificate Services received a resubmitted certificate request. This means that a certificate manager issued a certificate that was pending.
774	Certificate Services revoked a certificate.
775	Certificate Services received a request to publish the CRL.
776	Certificate Services published the CRL.
777	A certificate request extension changed.
778	One or more certificate request attributes changed.
779	Certificate Services received a request to shut down.
780	Certificate Services backup started.
781	Certificate Services backup completed.
782	Certificate Services restore started.
783	Certificate Services restore completed.
784	Certificate Services started.
785	Certificate Services stopped.
786	Security permissions for Certificate Services changed.
787	Certificate Services retrieved an archived key.
788	Certificate Services imported a certificate into its database.
789	The audit filter for Certificate Services changed.
790	Certificate Services received a certificate request.
791	Certificate Services approved a certificate request and issued a certificate.
792	Certificate Services denied a certificate request.
793	Certificate Services set the status of a certificate request to pending.
794	The certificate manager settings for Certificate Services changed.
795	A configuration entry changed in Certificate Services.
796	A property of Certificate Services changed.
797	Certificate Services archived a key.
798	Certificate Services imported and archived a key.
799	Certificate Services published the CA certificate to Active Directory.
800	One or more rows have been deleted from the certificate database.
801	Role separation enforcement is enabled. If role separation enforcement is enabled, the event log entry will state Yes. If it is disabled, the event log entry will state No.

Once you have enabled object access auditing for successes and failures, the following lines in a post-installation script ensure that all auditing categories are enabled:

```
::Enable all auditing events for the CA
certutil -setreg CA\AuditFilter 127
```

### Publishing an Updated CRL

Once all of the configuration changes are made to a CA, including the definition of CDP and AIA extensions, you must restart Certificate Services to enable the changes. Because the CDP extension allows you to modify the CRL location, it is advisable to copy the CRL to a floppy disk when configuring offline CAs. The following combination of commands enables the restart of Certificate Services, publishes an updated CRL, and copies the updated CRL to the floppy drive.

```
net stop certsvc & net start certsvc
Sleep 5
Echo Insert a Floppy disk in Drive A:
certutil -CRL
sleep 5
copy /y %windir%\system32\certsrv\certenroll\*.crl a:\
```



**Note** This script also utilizes the Sleep utility from the Windows Server 2003 Resource Kit. This command will pause a batch file for the indicated number of seconds—five seconds in this case. You might have to increase the sleep time depending on the size of your CA database and CRL.

## Implementing an Enterprise Root CA

Some organizations do not require the security enhancements of a multi-tier CA hierarchy. They only use a CA to issue certificates for the computers, users, services, and network devices on their network. There is no need for redundancy or to provide a high-assurance trust model.

In these circumstances, a CA hierarchy consisting of a single CA can be deployed. An example of this is the CA hierarchy for Margie's Travel. (See Figure 6-2.)



**Note** It is always recommend to use Windows Server 2003, Enterprise Edition, when installing an enterprise CA. Windows Server 2003, Enterprise Edition, enables advanced features not available in Windows Server 2003, Standard Edition, such as the issuing of version 2 certificate templates, private key archival, and role separation enforcement.

## Creating a CAPolicy.inf File

Even though you are deploying a single CA for the network, it is still recommended that you create a CAPolicy.inf file. The reason for this is to ensure that the configuration settings, which are defined only in the CAPolicy.inf file, are applied to the enterprise root CA.



**Note** This example of implementing an enterprise root CA assumes that Margie's Travel has an existing Active Directory deployment with a single domain named margiestravel.com. It does not matter whether the domain is a Windows 2000 or a Windows Server 2003 domain, as long as the Active Directory modifications discussed in Chapter 4, "Preparing an Active Directory Environment," are applied.

The CAPolicy.inf file for Margie's Travel makes the following assumptions:

- The root CA uses a key length of 2,048 bits.
- The validity period of the root CA certificate is 10 years.
- Base CRLs are published every two days.
- Delta CRLs are published every 12 hours.
- The root CA does not contain a CDP or AIA extension to prevent revocation checking of the root CA certificate.
- A CPS is not necessary.

Based on these assumptions, the following CAPolicy.inf file can be installed in the %windir% of the MargieCA01 computer.

```
[Version]
Signature="$Windows NT$"

[certsrv_server]
renewalkeylength=2048
RenewalValidityPeriodUnits=10
RenewalValidityPeriod=years

CRLPeriod=days
CRLPeriodUnits=2
CRLDeltaPeriodUnits=12
CRLDeltaPeriod=hours

[CRLDistributionPoint]
Empty=True

[AuthorityInformationAccess]
Empty=True
```

## Installing Internet Information Services

If you want to implement the Certificate Services Web Enrollment pages, you must install Internet Information Services (IIS) on either the CA computer or a front-end Web server.



**Important** An enterprise CA does not require IIS for operation. IIS is only required if you are hosting the Certificate Services Web Enrollment pages on the CA computer.

The following steps allow a member of the local Administrators group to install IIS with the minimum requirements for the Certificate Enrollment Web site. This ensures that no services beyond those required by the Web Enrollment Web pages are enabled on the IIS Server.

1. From the Start menu, click Control Panel and click Add or Remove Programs.
2. In the Add or Remove Programs window, click Add/Remove Windows Components.
3. In the Windows Components Wizard, select Application Server and click Details.



**Warning** Do not select the check box next to Application Server; just select the entire item. This prevents the selection of default components.

4. In the Application Server dialog box, click the Internet Information Services (IIS) check box (the Enable Network COM+ Access check box is automatically enabled as well, but it can be cleared) and click Details.
5. In the Internet Information Services (IIS) dialog box, ensure that the following subcomponents are selected:
  - Common Files
  - Internet Information Services Manager
  - World Wide Web Service
6. In the Internet Information Services (IIS) dialog box, select World Wide Web Service and click Details.

7. In the World Wide Web Service dialog box, enable the following subcomponents:
  - Active Server Pages
  - World Wide Web Service
8. In the World Wide Web Service dialog box, click OK.
9. In the Internet Information Services (IIS) dialog box, click OK.
10. In the Application Server dialog box, click OK.
11. On the Windows Components page, click Next.
12. Click Finish.
13. Close Add or Remove Programs.

## Installing Certificate Services

To install Windows Server 2003 Certificate Services as an enterprise CA, a user who is a member of both the Enterprise Admins group of the forest and the local Administrators group of the MargieCA01 computer must perform the install.



**Note** This installation procedure assumes that the naming conventions used in Figure 6-2 and the assumptions made for the creation of the CAPolicy.inf file are still in effect. In addition, it assumes that the enterprise CA will be installed on a computer with a single disk drive.

You can use the following procedure to perform the installation of the CA:

1. From the Start menu, click Control Panel and click Add or Remove Programs.
2. In the Add or Remove Programs window, click Add/Remove Windows Components.
3. In the Windows Components Wizard, in the Windows Components list, click the Certificate Services check box.
4. In the Microsoft Certificate Services dialog box, click Yes.
5. On the Windows Components page, click Next.
6. On the CA Type page, click Enterprise Root CA, enable the Use Custom Settings To Generate the Key Pair and CA Certificate check box, and click Next.



7. On the Public and Private Key Pair page, set the following options:
  - CSP: Microsoft Strong Cryptographic Service Provider
  - Allow the CSP to interact with the desktop: Disabled.
  - Hash algorithm: SHA-1
  - Key length: 2,048
8. On the Public and Private Key Pair page, click Next.
9. On the CA Identifying Information page, enter the following information:
  - Common Name for this CA: **Margie's Travel Root CA**
  - Distinguished name suffix: **O=Margie's Travel,C=US**
  - Validity Period: **10 Years**
10. On the CA Identifying Information page, click Next.
11. On the Certificate Database Settings page, accept the default settings and click Next.
12. In the Microsoft Certificate Services dialog box, click Yes to create the necessary folders.
13. If prompted, insert the Windows Server 2003, Enterprise Edition, CD in the CD-ROM drive and choose the \i386 folder.
14. In the Microsoft Certificate Services dialog box, click Yes to temporarily stop IIS.
15. On the Completing the Windows Components Wizard page, click Finish.
16. Close the Add or Remove Programs dialog box.

## Post-Installation Configuration

Once the installation of Certificate Services is complete, you should run a post-installation script to ensure that the correct settings are defined for the enterprise root CA.

You can use the following script to meet the objectives defined earlier in this section and to apply the default CRL and AIA publication points:

```

::Declare Configuration NC
certutil -setreg ca\DSConfigDN CN=Configuration,DC=margiestravel,DC=com

::Define CRL Publication Intervals
certutil -setreg CA\CRLPeriodUnits 2
certutil -setreg CA\CRLPeriod "Days"
certutil -setreg CA\CRLDeltaPeriodUnits 12
certutil -setreg CA\CRLDeltaPeriod "Hours"

```

```

::Apply the default CDP Extension URLs
certutil -setreg CA\CRLPublicationURLs "65:%windir%\system32\CertSrv\
CertEnroll\%3%8%9.cr1\n79:ldap:///
CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10\n6:http://%1/
CertEnroll/%3%8%9.cr1\n0:file://\%1\CertEnroll\%3%8%9.cr1"

::Apply the default AIA Extension URLs
certutil -setreg CA\CACertPublicationURLs "1:%windir%\system32\CertSrv\
CertEnroll\%1_%3%4.crt\n3:ldap:///
CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11\n2:http://%1/CertEnroll/
%1_%3%4.crt\n0:file://\%1\CertEnroll\%1_%3%4.crt"

::Enable all auditing events for the enterprise root CA
certutil -setreg CA\AuditFilter 127

::Set Validity Period for Issued Certificates
certutil -setreg CA\ValidityPeriodUnits 2
certutil -setreg CA\ValidityPeriod "Years"

::Restart Certificate Services
net stop certsvc & net start certsvc
sleep 5
certutil -cr1

```

## Enabling Auditing

The post-installation script enables all auditing events for Certificate Services. These auditing events depend on enabling success and failure auditing for Object Access. Because the enterprise root CA is a member of a domain, you should define auditing settings in a GPO applied to the OU where the CA's computer account resides. Use the following procedure to define the GPO at a domain controller in the domain where the enterprise root CA's computer account resides:

1. From Administrative Tools, open Active Directory Users and Computers.
2. In the console tree, expand the OU structure, right-click the OU where the CA's computer account exists, and click Properties.



**Note** If the computer account exists in the Computers container, the Group Policy definition must take place at the domain, or the computer account must be moved to an OU.

3. In the OU Properties dialog box, on the Group Policy tab, click New.
4. Name the new Group Policy **CA Audit Settings** and click Edit.

5. In the console tree, navigate to the following container: Computer Settings \Windows Settings\Security Settings\Local Policies\Audit Policy and enable the following auditing settings based on the Windows Server 2003 Security Guide (<http://go.microsoft.com/fwlink/?LinkId=14846>):
  - Account Logon: Success, Failure
  - Account Management: Success, Failure
  - Directory Service Access: Failure
  - Logon Events: Success, Failure
  - Object Access: Success, Failure
  - Policy Change: Success, Failure
  - Privilege Use: Failure
  - Process Tracking: No auditing
  - System Events: Success, Failure
6. Close the Group Policy Editor.
7. In the OU Properties dialog box, click OK.
8. Close Active Directory Users and Computers.



**Note** If you have an existing GPO that enables these recommended auditing settings, you can link to it rather than define another GPO with the same settings.

## Implementing a Standalone Root CA

If you are implementing a multi-tier CA hierarchy, you should implement an offline root CA, which requires that Certificate Services be installed as a standalone root CA. This allows the computer to remain as a workgroup member so that the computer can be removed from the network for long periods of time.



**Note** You can use Windows Server 2003, Standard Edition, for all offline CAs. The benefit of installing Windows Server 2003, Enterprise Edition, is entirely focused on the enterprise CA implementation.

## Creating a CAPolicy.inf File

It is imperative that you implement a CAPolicy.inf file when installing the root CA in a multi-tier CA hierarchy. The CAPolicy.inf file is the only way to define specific configuration settings, such as implementing an empty CDP and AIA extension in the root CA certificate.



**Note** This example assumes that Fabrikam Industries Inc. has an existing Active Directory deployment with a single domain named fabrikam.com. It does not matter if the domain is a Windows 2000 or a Windows Server 2003 domain as long as the Active Directory modifications discussed in Chapter 4, “Preparing an Active Directory Environment,” are applied.

This CAPolicy.inf file for Fabrikam Industries Inc. makes the following assumptions:

- The root CA uses a key length of 4,096 bits.
- The validity period of the root CA certificate is 20 years.
- Base CRLs are published every 26 weeks.
- Delta CRLs are disabled.
- The root CA does not contain a CDP or an AIA extension to prevent revocation checking of the root CA certificate.

Based on these assumptions, the following CAPolicy.inf file can be installed in the %windir% of the FABINCCA01 computer:

```
[Version]
Signature="$Windows NT$"

[certsrv_server]
renewalkeylength=4096
RenewalValidityPeriodUnits=0x20
RenewalValidityPeriod=years

CRLPeriod=weeks
CRLPeriodUnits=26
CRLDeltaPeriodUnits=0
CRLDeltaPeriod=days

[CRLDistributionPoint]
Empty=True

[AuthorityInformationAccess]
Empty=True
```

## Installing Certificate Services

Once the CAPolicy.inf file is installed, you can install Certificate Services on the root CA computer. The installation must be performed by a member of the local Administrators account on the CA computer, and the computer must not be a member of a domain. This will allow the computer to be removed from the network for long periods of time.

The following assumptions are made about the root CA computer:

- The naming of the computer uses the naming scheme defined in Figure 6-1.
- The computer has two mirrored partitions—drive C for the operating system and drive D for the CA database and log files.



**Note** IIS is not required for the installation of an offline root CA. The only certificate requests submitted to the root CA are for subordinate CA certificates, and these can be submitted by using the Certification Authority console.

You can use the following procedure to install the root CA:

1. Ensure that the date and time on the root CA computer is correct.
2. From the Start menu, click Control Panel and click Add or Remove Programs.
3. In the Add or Remove Programs window, click Add/Remove Windows Components.
4. In the Windows Components Wizard, in the Windows Components list, click the Certificate Services check box.
5. In the Microsoft Certificate Services dialog box, click Yes.
6. On the Windows Components page, click Next.
7. On the CA Type page, click Standalone Root CA, enable the Use Custom Settings To Generate the Key Pair and CA Certificate check box, and click Next.
8. On the Public and Private Key Pair page, set the following options:
  - CSP: Microsoft Strong Cryptographic Service Provider
  - Allow the CSP to interact with the desktop: Disabled
  - Hash algorithm: SHA-1
  - Key length: 4,096

9. On the Public and Private Key Pair page, click Next.
10. On the CA Identifying Information page, enter the following information:
  - Common Name for this CA: **Fabrikam Corporate Root CA**
  - Distinguished name suffix: **O=Fabrikam Inc.,C=US**
  - Validity Period: **20 Years**
11. On the CA Identifying Information page, click Next.
12. On the Certificate Database Settings page, provide the following settings and click Next:
  - Certificate database: D:\CertDB
  - Certificate database log: D:\CertLog
  - CA configuration: D:\CAConfig
13. In the Microsoft Certificate Services dialog box, click Yes to create the necessary folders.
14. If prompted, insert the Windows Server 2003, Standard Edition, CD in the CD-ROM drive and choose the \i386 folder.
15. In the Microsoft Certificate Services dialog box, click OK to identify that IIS is not installed.
16. On the Completing the Windows Components Wizard page, click Finish.
17. Close the Add or Remove Programs dialog box.

## Post-Installation Configuration

Once the Root CA is installed, you must ensure that the root CA's registry settings are configured correctly. The following assumptions are made in regard to the Fabrikam network:

- All client and server computers are running Windows 2000, Windows XP, or Windows Server 2003 and are members of the Fabrikam.com domain.
- There is a Web server named *www.fabrikam.com*. A virtual directory named CertData contains CRL and AIA information for all CAs in the CA hierarchy. This Web server is accessible internally and externally.
- The subordinate CA below the root CA has a 10-year validity period.
- The root CA certificate and CRL are copied to a floppy disk to allow publication to Active Directory and to the *www.fabrikam.com* server.
- Sleep.exe from the Windows Server 2003 Resource Kit is installed on the root CA computer.

You can use the following post-installation script to configure the root CA to implement these design assumptions and the assumptions stated earlier in this chapter:

```

::Declare Configuration NC
certutil -setreg CA\DSConfigDN CN=Configuration,DC=fabrikam,DC=com

::Define CRL Publication Intervals
certutil -setreg CA\CRLPeriodUnits 26
certutil -setreg CA\CRLPeriod "Weeks"
certutil -setreg CA\CRLDeltaPeriodUnits 0
certutil -setreg CA\CRLDeltaPeriod "Days"

::Apply the required CDP Extension URLs
certutil -setreg CA\CRLPublicationURLs "65:%windir%\system32\CertSrv\CertEn-
roll\%3%8%9.cr1\n79:ldap:///
CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10\n
6:http://www.fabrikam.com/CertData/ %3%8%9.cr1"

::Apply the required AIA Extension URLs
certutil -setreg CA\CACertPublicationURLs "1:%windir%\system32\CertSrv\CertEn-
roll\%1_%3%4.crt\n3:ldap:///
CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11\n
2:http://www.fabrikam.com/CertData/%1_%3%4.crt"

::Enable all auditing events for the Fabrikam Corporate Root CA
certutil -setreg CA\AuditFilter 127

::Set Validity Period for Issued Certificates
certutil -setreg CA\ValidityPeriodUnits 10
certutil -setreg CA\ValidityPeriod "Years"

::Restart Certificate Services
net stop certsvc & net start certsvc
sleep 5
certutil -cr1
::Copy the Root CA certificates and CRLs to the Floppy Drive
Echo Insert a Floppy disk in Drive A:
sleep 5
copy /y %windir%\system32\certsrv\certenroll\*.cr? a:\

```

## Object Access Auditing

The post-installation script enables all auditing events for Certificate Services. These events depend on enabling success and failure auditing for Object Access. Because the offline policy CA is not a member of a domain, auditing must be enabled in the Local Security Policy using the following procedure:

1. From Administrative Tools, open Local Security Policy.
2. In Security Settings\Local Policies\Audit Policy, enable the following auditing settings:
  - Account Logon: Success, Failure
  - Account Management: Success, Failure

- Directory Service Access: Failure
  - Logon Events: Success, Failure
  - Object Access: Success, Failure
  - Policy Change: Success, Failure
  - Privilege Use: Failure
  - Process Tracking: No auditing
  - System Events: Success, Failure
3. Close the Local Security Policy console.
  4. Close all windows.

## Implementing an Offline Policy CA

Once the offline root CA is established, installation of the offline policy CA can begin with the certificate request submitted to the root CA so that the certificate chain is formed correctly.



**Note** This section assumes you are installing a three-tier CA hierarchy. If you are installing a two-tier hierarchy, consider using the CAPolicy.inf file (with different CRL and delta CRL publication intervals) so that the issuing CA acts as both a policy and issuing CA.

## Pre-Installation Configuration

Before installing Certificate Services on the policy CA, you must ensure that the policy CA machine account trusts the root CA. This is accomplished by manually installing the root CA certificate (stored on a floppy disk) in the local computer's trusted root store. In addition, the root CA's CRL should be published to ensure that CRL checking is performed correctly.

The following script publishes the root CA certificate and CRL in the local machine store:

```
@echo off
a:
cd \
for %%c in (*.crt) do certutil -addstore -f Root "%%c"
for %%c in (*.crl) do certutil -addstore -f Root "%%c"
```

This batch file supports later revisions to the root CA certificate and will publish all versions of the root CA's certificate and CRL.



## Creating a CAPolicy.inf File

Once the root CA's certificate and CRL are published in the local machine's trusted root store, you must prepare a CAPolicy.inf file for the policy CA. The CAPolicy.inf file must define the CPS in a three-tier CA hierarchy. As mentioned, the CPS is defined by an OID, notice text, and a URL where the CPS is stored for retrieval.

The following assumptions apply to the Fabrikam Industries Inc. policy CA:

- It implements a single CPS, with the CPS published at *www.fabrikam.com/CPS/CPStatement.asp*.
- OID 1.3.6.1.4.1.311.509.3.1 is assigned to the CPS.
- The key length for the private key is 2048 bits.
- The validity period of the policy CA certificate is 10 years.
- Base CRLs are published every 26 weeks.
- Delta CRLs are disabled.

Based on these assumptions, the following CAPolicy.inf file can be installed in the %windir% of the Fabrikam Industries Inc. policy CA computer:

```
[Version]
Signature="$Windows NT$"

[PolicyStatementExtension]
Policies=FabrikamCPS

[FabrikamCPS]
OID=1.3.6.1.4.1.311.509.3.1
NOTICE=Fabrikam Industries Certificate Practice Statement
URL=http://www.fabrikam.com/CPS/CPStatement.asp

[certsrv_server]
RenewalKeyLength=2048
RenewalValidityPeriodUnits=10
RenewalValidityPeriod=years

CRLPeriod=weeks
CRLPeriodUnits=26
CRLDeltaPeriodUnits=0
CRLDeltaPeriod=days
```

## Installing Certificate Services

After the CAPolicy.inf file is in place, you can install Certificate Services. Because the policy CA's certificate request is submitted to the root CA, the issuance of the subordinate CA certificate takes place at the root CA.

The following assumptions are made about the root CA computer:

- It uses the naming scheme defined in Figure 6-1.
- It has two mirrored partitions—drive C for the operating system and drive D for the CA database and log files.



**Note** IIS is not required for the installation of an offline policy CA. The only certificate requests submitted to the policy CA are for subordinate CA certificates, which can be submitted using the Certification Authority console.

To start the process of installing Certificate Services, perform the following tasks at the policy CA:

1. Synchronize the date and time with the root CA.
2. From the Start menu, click Control Panel and click Add or Remove Programs.
3. In the Add or Remove Programs window, click Add/Remove Windows Components.
4. In the Windows Components Wizard, in the Windows Components list, click the Certificate Services check box.
5. In the Microsoft Certificate Services dialog box, click Yes.
6. On the Windows Components page, click Next.
7. On the CA Type page, click Standalone Subordinate CA, enable the Use Custom Settings To Generate the Key Pair and CA Certificate check box, and click Next.
8. On the Public and Private Key Pair page, set the following options:
  - CSP: Microsoft Strong Cryptographic Service Provider
  - Allow the CSP to interact with the desktop: Disabled
  - Hash algorithm: SHA-1
  - Key length: 2,048
9. On the Public and Private Key Pair page, click Next.
10. On the CA Identifying Information page, enter the following information:
  - Common Name for this CA: **Fabrikam Corporate Policy CA**
  - Distinguished name suffix: **O=Fabrikam Industries,C=US**
  - Validity Period: **Determine by Parent CA**

11. On the CA Identifying Information page, click Next.
12. On the Certificate Database Settings page, provide the following settings and click Next.
  - Certificate database: D:\CertDB
  - Certificate database log: D:\CertLog
  - Shared folder: D:\CAConfig
13. In the Microsoft Certificate Services dialog box, click Yes to create the necessary folders.
14. On the CA Certificate Request page, click Save the Request To a File. In the Request File box, type **A:\policyca.req** and click Next.
15. If prompted, insert the Windows Server 2003, Standard Edition, CD in the CD-ROM drive and choose the \i386 folder.
16. In the Microsoft Certificate Services message box, acknowledge that the CA installation is incomplete, and click OK.
17. In the Microsoft Certificate Services dialog box, click OK to identify that IIS is not installed.
18. On the Completing the Windows Components Wizard page, click Finish.
19. Close the Add or Remove Programs dialog box.
20. Remove the floppy disk containing the certificate request file from the floppy drive.

The floppy disk must now be transported to the root CA computer to submit the certificate request and to copy the issued certificate back to the policy CA. Use the following process at the policy CA:

1. Insert the floppy disk containing the certificate request file.
2. From the Start menu, click Administrative Tools and click Certification Authority.
3. In the console tree, right-click Fabrikam Corporate Root CA, point to All Tasks and click Submit New Request.
4. In the Open Request File dialog box, in the File Name box, type **A:\PolicyCA.req** and click Open.
5. In the console tree, expand Fabrikam Corporate Root CA and click Pending Requests.
6. In the details pane, right-click the certificate request, point to All Tasks and click Export Binary Data.

7. In the Export Binary Data dialog box, in the Columns That Contain Binary Data drop-down list, select Binary Request and click OK.
8. Review the request detail for accuracy:
  - Verify that the Subject name is Fabrikam Corporate Policy CA.
 

```
Subject:
CN=Fabrikam Corporate Policy CA
O=Fabrikam Industries
C=US
```
  - Ensure Public Key Length is 2,048 bits.
 

```
Public Key Length: 2048 bts
```
  - Ensure that the Basic Constraints indicate Subject type=CA.
 

```
Basic Constraints
Subject type=CA
```
  - Verify that the Certificate Policy statement is correctly configured with the Policy Identifier OID set to 1.3.6.1.4.1.1204.509.3.1, the Notice Text set to “Fabrikam Industries Certificate Practice Statement,” and the CPS Qualifier set to *www.fabrikam.com/CPS/CPStatement.asp*.
 

```
Certificate Policies
[1] Certificate Policy:
Policy Identifier=1.3.6.1.4.1.1204.509.3.1
[1,1]Policy Qualifier Info:
Policy Qualifier Id=User Notice
Qualifier:
Notice Text=Fabrikam Industries Certificate Practice Statement
[1,2]Policy Qualifier Info:
Policy Qualifier Id=CPS
Qualifier:
http://www.fabrikam.com/CPS/CPStatement.asp
```
  - Verify that the signature matches the public key.
 

```
Signature matches Public Key
```
9. Close the Binary Request window.
10. In the details pane, right-click the pending SubCA certificate, point to All Tasks and click Issue.
11. In the console tree, click Issued Certificates.
12. In the details pane, double-click the issued certificate.
13. In the Certificate dialog box, click the Details tab.
14. In the Details tab, click Copy to File.

15. In the Certificate Export Wizard, click Next.
16. On the Export File Format page, click Cryptographic Message Syntax Standard—PKCS #7 Certificates (.P7B), enable the Include All Certificates in the Certification Path If Possible check box, and click Next.
17. On the File to Export page, in the File Name box, type **A:\policyca.p7b** and click Next.
18. On the Completing the Certificate Export Wizard page, click Finish.
19. In the Certificate Export Wizard message box, click OK.
20. In the Certificate dialog box, click OK.
21. Close the Certification Authority console.
22. Remove the floppy disk containing the certificate request file.

Once the certificate is exported to the floppy disk, you can use the following procedure to complete installation of the policy CA by installing the subordinate CA certificate at the policy CA:

1. Insert the floppy disk containing the PKCS#7 file.
2. From the Start menu, click Administrative Tools and click Certification Authority.
3. In the console tree, right-click Fabrikam Corporate Policy CA, point to All Tasks and click Install CA Certificate.
4. In the Select File to Complete CA Installation dialog box, in the File Name box, type **A:\policyca.p7b** and then click Open.
5. In the console tree, right-click Fabrikam Corporate Policy CA, point to All Tasks and click Start Service.



**Note** At this point, Certificate Services starts and allows you to view and configure the policy CA. If the service does not start, the most common problem is time configuration. Ensure that the time and time zone are correct and synchronized with the root CA.

## Post-Installation Configuration

Once the policy CA installation is complete, you must ensure that the policy CA's registry settings are configured correctly. The following assumptions are made regarding the Fabrikam network:

- All client and server computers are running Windows 2000, Windows XP, or Windows Server 2003 and are members of the Fabrikam.com domain.
- There is a Web server named *www.fabrikam.com*. A virtual directory named CertData contains CRL and AIA information for all CAs in the CA hierarchy. This Web server is accessible internally and externally.
- The subordinate CA below the policy CA has a validity period of five years.
- The policy CA certificate and CRL are copied to a floppy disk to allow publication to Active Directory and to the *www.fabrikam.com* server.
- Sleep.exe from the Windows Server 2003 Resource Kit is installed on the policy CA computer.

To configure the policy CA to implement these design decisions and the assumptions stated previously, the following post-installation script can be used:

```
::Declare Configuration NC
certutil -setreg CA\DSConfigDN CN=Configuration,DC=fabrikam,DC=com

::Define CRL Publication Intervals
certutil -setreg CA\CRLPeriodUnits 26
certutil -setreg CA\CRLPeriod "Weeks"
certutil -setreg CA\CRLDeltaPeriodUnits 0
certutil -setreg CA\CRLDeltaPeriod "Days"

::Apply the required CDP Extension URLs
certutil -setreg CA\CRLPublicationURLs "65:%windir%\system32\CertSrv\CertEn-
roll\%3%8%9.crl\n79:ldap:///
CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10\n
6:http://www.fabrikam.com/CertData/ %3%8%9.crl"

::Apply the required AIA Extension URLs
certutil -setreg CA\CACertPublicationURLs "1:%windir%\system32\CertSrv\CertEn-
roll\%1_%3%4.crt\n3:ldap:///
CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11\n
2:http://www.fabrikam.com/CertData/%1_%3%4.crt"

::Enable all auditing events for the Fabrikam Corporate Policy CA
certutil -setreg CA\AuditFilter 127

::Set Validity Period for Issued Certificates
certutil -setreg CA\ValidityPeriodUnits 5
certutil -setreg CA\ValidityPeriod "Years"

::Restart Certificate Services
net stop certsvc & net start certsvc
sleep 5
```

```
certutil -crl
::Copy the policy CA certificates and CRLs to the Floppy Drive
Echo Insert a Floppy disk in Drive A:
sleep 5
copy /y %windir%\system32\certsrv\certenroll\*.cr? a:\
```

## Object Access Auditing

The post-installation script enables all auditing events for Certificate Services. These auditing events depend on enabling success and failure auditing for Object Access. Because the offline policy CA is not a member of a domain, auditing must be enabled in the Local Security Policy as described earlier in this chapter.

## Implementing an Online Issuing CA

The process for installing online CAs is slightly different than the process for installing offline CAs.

### Pre-Installation Configuration

Before installing Certificate Services on the issuing CA, you must ensure that the issuing CA trusts the root CA and is able to download the policy CA certificate and CRL for certificate revocation checking.

This is accomplished by manually installing or publishing the root CA and policy CA certificates stored on a floppy disk to the following locations:

- **The local computer's trusted root store and intermediate CA store.** This location is required if you are unable to publish the certificate into Active Directory or to the HTTP URL referenced in the AIA and CDP extensions of certificates issued by the root or policy CA. This location is also required if the issuing CA is a standalone CA.
- **Active Directory.** The root and policy CA certificate and CRLs can be published into Active Directory. Publication into Active Directory enables the automated download of the certificates to all Windows 2000, Windows XP, and Windows Server 2003 computers that are members of the forest.
- **HTTP URLs referenced in the AIA and CDP extensions.** The root and policy CA certificates and CRLs must be manually published to these locations to enable download of the CA certificates and CRLs to all clients using these URLs for chain building and revocation checking.

### Publishing Certificates at the Issuing CA

If you have not published the root and policy CA certificates into Active Directory or to the HTTP URLs included in the certificates issued by the root and policy CAs, you can manually publish the certificates into the issuing CA's local machine store. This process is similar to the one used to publish the root CA certificate and CRL at the

policy CA. The difference is that both root and intermediate CA certificates are published at an issuing CA.

The following script publishes the root CA certificate and CRL into the local machine store:

```
@echo off
a:
cd \
for %%c in ("FABINCCA01*.crt") do certutil -addstore -f Root "%%c"
for %%c in ("Fabrikam Corporate Root*.crl") do certutil -addstore -f Root "%%c"
for %%c in ("FABINCCA02*.crt") do certutil -addstore -f CA "%%c"
for %%c in ("Fabrikam Corporate Policy*.crl") do certutil -addstore -f CA "%%c"
```

This batch file supports later revisions to the root or policy CA certificates and publishes all versions of the root and policy CA certificates and CRLs.



**Tip** When using this script in your environment, modify each line's search pattern to a pattern that uniquely describes the CA computer name for \*.crt files and the CA logical name for \*.crl files.

## Publishing Certificates into Active Directory

The preferred method of publishing root and policy CA certificates and CRLs in a forest environment is to publish them into Active Directory. When published into Active Directory, the CA certificates and CRLs are published in the configuration naming context and are automatically downloaded to all forest members running Windows 2000, Windows XP, or Windows Server 2003 through autoenrollment.

You can use the following script, which must be run by a member of the Enterprise Admins group, to publish the root and policy CA certificates and CRLs:

```
@echo off
a:
cd \
for %%c in ("FABINCCA01*.crt") do certutil -dspublish -f "%%c" RootCA
for %%c in ("FABINCCA02*.crt") do certutil -dspublish -f "%%c" SubCA
for %%c in ("Fabrikam Corporate Root*.crl") do certutil -dspublish -f "%%c"
for %%c in ("Fabrikam Corporate Policy*.crl") do certutil -dspublish -f "%%c"
gpupdate /force
```

The next time Group Policy is applied to a computer that is a member of the forest, certificates will be automatically added to the trusted root or intermediate CA store of the local machine through the autoenrollment mechanism.





**Tip** When using this script in your environment, modify each line's search pattern to a pattern that uniquely describes the CA computer name for \*.crt files and the CA logical name for \*.crl files.

## Publishing Certificates to HTTP Locations

If you include HTTP URLs in the AIA or CDP extensions, you must ensure that the offline CA certificates and CRLs are manually copied to these locations. The method you use for publication cannot be predefined, as many factors affect the decision, including:

- **The Web server's location in your network infrastructure.** If the Web server is hosted in a demilitarized zone (DMZ), a firewall can prevent manual duplication of the file or restrict the copy procedure to specific protocols.
- **The Web server's domain or workgroup membership.** If the Web server is in a different domain, forest, or workgroup, a trust relationship can be required to allow duplication to the Web server's local disk system.
- **The Web server's operating system.** There are other Web servers in the world. The Web server you are publishing to might be an open source solution, such as Apache. In this case, you might have to use other protocols, such as FTP or Secure Shell (SSH), to transfer the files to the Web server.

In any of these scenarios, you must ensure that the CA certificates are available at the URL paths defined in the AIA extension of certificates and that the CA CRLs are available at the URL paths defined in the CDP extension of certificates.

## Creating a CAPolicy.inf File

Once the root and policy CA certificates and CRLs are downloaded to the local machine's trusted root store, you must prepare a CAPolicy.inf file for the issuing CA. The CAPolicy.inf file for an issuing CA must define certificate-renewal and CRL publication settings.

The following assumptions apply to the Fabrikam issuing CA:

- The key length for the private key is 2,048 bits.
- The policy CA certificate's validity period is five years.

- Base CRLs are published every three days.
- Delta CRLs are published every 12 hours.

```
[Version]
Signature="$Windows NT$"

[certsrv_server]
renewalkeylength=2048
RenewalValidityPeriodUnits=5
RenewalValidityPeriod=years

CRLPeriod=3
CRLPeriodUnits=days
CRLDeltaPeriod=12
CRLDeltaPeriodUnits=hours
```

## Installing IIS

If you are planning to utilize the Certificate Services Web Enrollment pages, you must install IIS on the Issuing CA. As discussed earlier in this chapter, you do not have to install all IIS components, only those required by the Certificate Services Web Enrollment pages.

## Installing Certificate Services

Once the CAPolicy.inf file and IIS are in place, you can install Certificate Services. Because the issuing CA's certificate request is submitted to the policy CA, the issuance of the subordinate CA certificate occurs at the policy CA.

The following assumptions are made about the issuing CA computer:

- It uses the naming scheme defined in Figure 6-1.
- It has two mirrored partitions and a RAID 5 array: drive C for the operating system; drive D for the CA log files; and drive E, a RAID 5 array, for the CA database.

To begin installing Certificate Services, ensure you are logged on as a member of the Enterprise Admins group. In addition, ensure that the Enterprise Admins group is a member of the local Administrators group in the local account database of the enterprise CA. You can use the following procedure to install the enterprise CA.



**Note** If installing a two-tier CA hierarchy, replace all instances of the policy CA with the root CA in the upcoming steps.

1. Ensure that the enterprise CA is a member of a domain in the forest.
2. Ensure that the date and time are correctly set.
3. From the Start menu, click Control Panel and click Add or Remove Programs.
4. In the Add or Remove Programs window, click Add/Remove Windows Components.
5. In the Windows Components Wizard, in the Windows Components list, click the Certificate Services check box.
6. In the Microsoft Certificate Services dialog box, click Yes.
7. On the Windows Components page, click Next.
8. On the CA Type page, click Enterprise Subordinate CA, and enable the Use Custom Settings To Generate the Key Pair and CA Certificate check box and click Next.
9. On the Public and Private Key Pair page, set the following options:
  - CSP: Microsoft Strong Cryptographic Service Provider
  - Allow the CSP to interact with the desktop: Disabled
  - Hash algorithm: SHA-1
  - Key length: 2,048
10. On the Public and Private Key Pair page, click Next.
11. On the CA Identifying Information page, enter the following information:
  - Common Name for this CA: **Fabrikam Corporate Issuing CA**
  - Distinguished name suffix: **O=Fabrikam Industries,C=US**
12. On the CA Identifying Information page, click Next.
13. On the Certificate Database Settings page, provide the following settings and click Next.
  - Certificate database: E:\CertDB
  - Certificate database log: D:\CertLog
14. In the Microsoft Certificate Services dialog box, click Yes to create the necessary folders.
15. On the CA Certificate Request page, click Save the Request to a File. In the Request File box, type **A:\IssuingCA.req** and click Next.
16. In the Microsoft Certificate Services dialog box, click Yes to temporarily stop IIS.

17. If prompted, insert the Windows Server 2003, Enterprise Edition, CD in the CD-ROM drive and choose the \i386 folder.



**Note** Always use Windows Server 2003, Enterprise Edition, for enterprise CAs to allow use of version 2 certificate templates, enable key archival, and enforce role separation. These features are not available on Windows Server 2003, Standard Edition.

18. In the Microsoft Certificate Services message box, acknowledge that the CA installation is incomplete and click OK.
19. If the Microsoft Certificate Services dialog box appears, click Yes to enable Active Server Pages.
20. On the Completing the Windows Components Wizard page, click Finish.
21. Close the Add or Remove Programs dialog box.
22. Close all windows.
23. Remove the floppy disk containing the certificate request file.

The floppy disk now must be transported to the policy CA computer to submit the certificate request and to copy the issued certificate back to the issuing CA. You can use the following process at the policy CA:

1. Insert the floppy disk containing the certificate request file.
2. From the Start menu, click Administrative Tools and click Certification Authority.
3. In the console tree, right-click Fabrikam Corporate Policy CA, point to All Tasks and click Submit new request.
4. In the Open Request File dialog box, in the File Name box, type **A:\IssuingCA.req** and click Open.
5. In the console tree, expand Fabrikam Corporate Policy CA and click Pending Requests.
6. In the details pane, right-click the certificate request, point to All Tasks and click Export Binary Data.
7. In the Export Binary Data dialog box, in the Columns That Contain Binary Data drop-down list, select Binary Request and click OK.

8. Review the request detail for accuracy:

- Verify that the subject name is Fabrikam Corporate Issuing CA.

```
Subject:
CN=Fabrikam Corporate Issuing CA
O=Fabrikam Industries
C=US
```

- Ensure Public Key length is 2,048 bits.

```
Public Key Length: 2048 bts
```

- Ensure that the Basic Constraints indicate that the Subject Type=CA.

```
Basic Constraints
Subject type=CA
```

- Verify that the signature matches the public key.

```
Signature matches Public Key
```

9. Close the Binary Request window.
10. In the details pane, right-click the pending SubCA certificate, point to All Tasks and click Issue.
11. In the console tree, click Issued Certificates.
12. In the details pane, double-click the issued certificate.
13. In the Certificate dialog box, click the Details tab.
14. In the Details tab, click Copy to File.
15. In the Certificate Export Wizard, click Next.
16. On the Export File Format page, click Cryptographic Message Syntax Standard—PKCS #7 Certificates (.P7B), enable the Include All Certificates in the Certification Path If Possible check box, and click Next.
17. On the File to Export page, in the File Name box, type **A:\IssuingCA.p7b** and click Next.
18. On the Completing the Certificate Export Wizard page, click Finish.
19. In the Certificate Export Wizard message box, click OK.
20. In the Certificate dialog box, click OK.
21. Close the Certification Authority console.
22. Remove the floppy disk containing the certificate request file.



**Note** At this point, the root and policy CAs can be turned off. Additional security measures for offline CAs are discussed in Chapter 7, “Securing a CA Hierarchy.”

Once the certificate is exported to the floppy disk, you can use the following procedure to finish installing the issuing CA by installing the subordinate CA certificate at the issuing CA:

1. Insert the floppy disk containing the PKCS#7 file in the floppy drive.
2. From the Start menu, click Administrative Tools and click Certification Authority.
3. In the console tree, right-click Fabrikam Corporate Issuing CA, point to All Tasks and click Install CA Certificate.
4. In the Select File to Complete CA Installation dialog box, in the File Name box, type **A:\IssuingCA.p7b** and then click Open.
5. In the console tree, right-click Fabrikam Corporate Issuing CA, point to All Tasks and click Start Service.

## Post-Installation Configuration

Once the issuing CA is installed, you must ensure that the issuing CA's registry settings are configured correctly. The following assumptions are made regarding the Fabrikam network:

- All client and server computers are running Windows 2000, Windows XP, or Windows Server 2003 and are members of the Fabrikam.com domain.
- The issuing CA's certificate and CRL are published in Active Directory, on the issuing CA's Web service, and at an externally accessible Web server.
- There is a Web server named *www.fabrikam.com*. A virtual directory named CertData contains CRL and AIA information for all CAs in the CA hierarchy. This Web server is accessible internally and externally.
- The issuing CA issues certificates—with a maximum two-year validity period—to users, computers, services, and network devices.
- The issuing CA certificate and CRL are copied to a floppy disk to allow publication to the *www.fabrikam.com* Web server.
- Wait.exe from the Windows Server 2003 Resource Kit is installed on the issuing CA computer.
- CRL and CA certificate retrieval should take place in the following order:
  1. Active Directory
  2. Externally accessible Web server
  3. The issuing CA's Web service
  4. The issuing CA's Universal Naming Convention (UNC) file share



**Note** The order to use for CA certificate and CRL retrieval is discussed greater detail in Chapter 9, “Certificate Validation.”

Use the following post-installation script to configure the issuing CA to implement these design decisions and the assumptions stated previously:

```
::Declare Configuration NC
certutil -setreg CA\DSConfigDN CN=Configuration,DC=fabrikam,DC=com

::Define CRL Publication Intervals
certutil -setreg CA\CRLPeriodUnits 3
certutil -setreg CA\CRLPeriod "Days"
certutil -setreg CA\CRLDeltaPeriodUnits 12
certutil -setreg CA\CRLDeltaPeriod "Hours"

::Apply the required CDP Extension URLs
certutil -setreg CA\CRLPublicationURLs "65:%windir%\system32\CertSrv\
CertEnroll\%3%8%9.cr1\n79:ldap:///
CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10\n
6:http://www.fabrikam.com/CertData/%3%8%9.cr1\n6:http://%1/CertEnroll/
%3%8%9.cr1 \n0:file://\%1/CertEnroll\%3%8%9.cr1"

::Apply the required AIA Extension URLs
certutil -setreg CA\CACertPublicationURLs "1:%windir%\system32\CertSrv\
CertEnroll\%1_%3%4.crt\n3:ldap:///
CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11\n
2:http://www.fabrikam.com/CertData/%1_%3%4.crt\n2:http://%1/CertEnroll/
%1_%3%4.crt \n0:file://\%1\CertEnroll/%1_%3%4.crt "

::Enable all auditing events for the Fabrikam Corporate Issuing CA
certutil -setreg CA\AuditFilter 127

::Set Maximum Validity Period for Issued Certificates
certutil -setreg CA\ValidityPeriodUnits 2
certutil -setreg CA\ValidityPeriod "Years"

::Restart Certificate Services
net stop certsvc & net start certsvc
sleep 5
certutil -cr1
::Copy the issuing CA certificates and CRLs to the Floppy Drive
Echo Insert a Floppy disk in Drive A:
sleep 5
copy /y %windir%\system32\certsrv\certenroll\*.cr? a:\
```

## Object Access Auditing

The post-installation script enables all auditing events for Certificate Services. These auditing events depend on enabling success and failure auditing for Object Access.

Because the online issuing CA is a member of a domain, auditing must be enabled in a Group Policy object linked to the OU where the CA's computer account exists in Active Directory, as described earlier in this chapter.

## Verifying Installation

Once you install the CA hierarchy—whether it is a single-tier or a multi-tier hierarchy—you must ensure that the AIA and CDP URLs are configured correctly before you start issuing certificates.

If the URLs are configured incorrectly, the certificate chaining engine might encounter errors when it attempts to download CA certificates and CRLs from the referenced URLs. In addition, you cannot go back and edit issued certificates. As discussed in Chapter 2, “Primer to PKI,” a certificate is a signed object and cannot be modified without invalidating the signature included in the thumbprint extension of the certificate.

The PKI Health Tool—included in the Windows Server 2003 Resource Kit and on this book's CD-ROM—evaluates every URL included in the AIA and CDP extensions of the certificates in the CA hierarchy. The tool attempts to connect to each referenced URL and reports whether the certificate or CRL is reachable, as well as whether the current version is reaching expiration.

You must run the PKI Health Tool on a Windows Server 2003 computer that is a member of the forest. You can use the following procedure to use the tool:

1. Install the Windows Server 2003 Resource Kit tools.



**More Info** The Windows Server 2003 Resource Kit tools are available for download at <http://www.microsoft.com/downloads/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cffd&displaylang=en>.

2. From the Start menu, click Run, type **pkiview.msc** and click OK.
3. In the console tree, click each CA in the hierarchy. In the details pane, review the status of each CRL and AIA location.

If a publication point is configured correctly, the Status column will report a value of OK. If the publication point is configured incorrectly or if the CA certificate or CRL is not copied correctly to the publication point, the Status column reports a status of Unable to Download. Finally, if the CA certificate or CRL is near expiration, the Status column will report a value of Expiring.





**More Info** For more information on troubleshooting CRLs and certificate status, see the “Troubleshooting Certificate Status and Revocation” white paper referenced in the “Additional Information” section of this chapter.

## Case Study: Deploying a PKI

You are the network administrator for Fabrikam Industries Inc. Based on the design requirements, you have decided to deploy the CA hierarchy shown in Figure 6-1.

To assist you in configuring the CAPolicy.inf files, pre-installation batch files, and post-installation batch files, the following design requirements are provided:

### ■ Root CA

- The root CA must use a key length of 2,048 bits for its public and private key pair.
- The root CA certificate must have a 20-year lifetime.
- The root CA will publish its base CRL twice a year.
- The root CA will not implement a delta CRL.
- The root CA certificate will not include an AIA or CDP extension.
- The root CA will issue subordinate CA certificates with a 10-year lifetime.
- The root CA certificate and CRL are published in Active Directory to allow automatic distribution to all Windows 2000 and later client computers.
- The root CA must issue subordinate CA certificates that have an AIA extension with the first URL referencing the Active Directory publication point and the second URL as *http://www.fabrikam.com/certdata/RootCACertificate* (where *RootCACertificate* is the default name of the Root CA’s certificate file).
- The root CA must issue subordinate CA certificates that have a CDP extension with the first URL referencing the Active Directory publication point and the second URL as *http://www.fabrikam.com/certdata/RootCACRL* (where *RootCACRL* is the default name of the Root CA’s CRL file).

### ■ Policy CA

- The certificate practice statement (CPS) for the Fabrikam PKI is published at the URL *www.fabrikam.com/CPS/Fabrikampolicy.asp*.
- The OID assigned to the Fabrikam CPS is 1.3.6.1.4.1.311.509.4.1.

**■ Issuing CA**

- The issuing CA will host the Certificate Services Web Enrollment pages.
- The issuing CA will publish a base CRL daily and a delta CRL every eight hours.

**Case Study Questions**

The questions for this case study are divided into sections related to configuration of the Fabrikam Corporate Root CA, the Fabrikam Corporate Policy CA, and the Fabrikam Corporate Issuing CA.

**Fabrikam Corporate Root CA**

Answer the following questions related to configuration of the Fabrikam Corporate Root CA based on information provided in the design requirements:

1. How do you define the key length of 2,048 bits for the root CA during installation of the root CA?
2. How do you ensure that the key length will remain 2,048 bits when the root CA's certificate is renewed?
3. What entries are required in the CAPolicy.inf file to define the required base CRL and delta CRL publication intervals?
4. How would you suppress the inclusion of an AIA and CDP extension in the root CA certificate?
5. After configuring the CAPolicy.inf file, you note that none of the settings are applied to the root CA when you install Certificate Services. You check and find that the file is located in the C:\temp folder. Why did the installation not apply the settings in the CAPolicy.inf file?
6. How do you configure the root CA to issue subordinate CA certificates with a lifetime of 10 years?
7. How do you define the location in Configuration naming context for publishing the root CA certificate and CRL to Active Directory? (Assume that the forest root domain is the same as shown in Figure 6-1.)
8. What command is required to define the AIA publication URLs for the certificates issued by the root CA?
9. What command is required to define the CDP publication URLs for the certificates issued by the root CA?

## Fabrikam Corporate Policy CA

Answer the following questions related to configuration of the Fabrikam Corporate Policy CA based on the information provided in the design requirements:

1. On the first attempt to install the policy CA, you receive the error that the CA is unable to determine the revocation status for the policy CA certificate. What must you do to ensure that the policy CA recognizes the root CA certificate as a trusted root certificate and can determine the revocation status for the policy CA certificate?
2. What command do you use to add the root CA certificate as a trusted root CA certificate on the Fabrikam Corporate Policy CA, assuming that the name of the root CA certificate is FABINCCA01\_ Fabrikam Corporate Root CA.crt?
3. What command do you use to allow the policy CA to access the root CA CRL, assuming that the name of the root CA certificate is Fabrikam Corporate Root CA.crl?
4. How do you configure the CAPolicy.inf file on the policy CA to include the CPS and related OID?

## Fabrikam Corporate Issuing CA

Answer the following questions related to configuration of the Fabrikam Corporate Policy CA based on the information provided in the design requirements:

1. What commands do you use to ensure that the root CA and policy CA certificates are automatically added to the local machine store of all Windows 2000, Windows XP, and Windows Server 2003 domain members?
2. What commands do you use to ensure that the root CA and policy CA CRLs are automatically added to the local machine store of all Windows 2000, Windows XP, and Windows Server 2003 domain members?
3. On the first attempt to install the issuing CA, you receive the error that the CA is unable to determine the revocation status for the policy CA certificate. Assuming that you have successfully published the root and policy CA information to Active Directory, what must you do to ensure that the issuing CA can determine the revocation status for the issuing CA certificate?
4. What are the minimum components of the World Wide Web Service required to install the Certificate Services Web Enrollment pages?
5. What commands are required at the issuing CA to publish the base CRL daily and the delta CRL every eight hours?

## Additional Information

- Microsoft Official Curriculum, Course 2821: “Designing and Managing a Windows Public Key Infrastructure” (<http://www.microsoft.com/traincert/syllabi/2821afinal.asp>)
- “Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure” (<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws3pkibp.mspix>)
- “Troubleshooting Certificate Status and Revocation” (<http://www.microsoft.com/technet/prodtechnol/winxp/psd/support/tsbtcr1.mspix>)
- Windows Server 2003 Resource Kit Tools (<http://www.microsoft.com/downloads/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cffd&displaylang=en>)
- Knowledge Base Article 272555: “Certificate Services in a Non-Active Directory Environment: Installation and Issuing Certificates”
- Knowledge Base Article 246242: “Information About Renewing a Certification Authority Certificate in Windows 2000”
- Knowledge Base Article 231881: “HOW TO: How to Install/Uninstall a Public Key Certificate Authority for Windows 2000”



**Note** Microsoft Knowledge Base articles can be found at <http://support.microsoft.com>. Enter the article number in the Search the Knowledge Base text box.

## Chapter 7

# Securing a CA Hierarchy

A certification authority (CA) hierarchy is only as secure as the security measures that an organization takes to protect the CAs in the hierarchy. These measures can be categorized as either

- CA configuration measures  
or
- Physical security measures

and can range from limiting which security groups can log on locally at the CA console to keeping the CA computer in a secured location. Your security plan must include measures to protect each CA's private key from compromise.

## Designing CA Configuration Security Measures

CA configuration security measures refer to the configuration of Certificate Services or the configuration of the Microsoft Windows Server 2003 operating system. Measures you can take to configure CA configuration security include:

- **Defining security templates for both offline and online CAs.** Security templates allow you to define baseline security configuration for a category of server computers, such as CAs.



**Note** Security templates are created using the Security Templates snap-in in the Microsoft Management Console (MMC). For more information on creating and using security templates, see Chapter 11, “Configuring Security Templates,” in the Microsoft Windows Security Resource Kit.

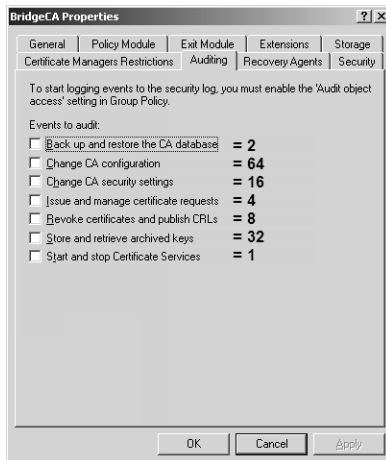
Settings that should be considered for inclusion in a CA security template are:

- **Disable unnecessary services.** A CA should only function as a CA. Do not allow the implementation of other network services or applications such as Microsoft Exchange Server, Dynamic Host Configuration Protocol (DHCP) services, or domain controllers on the CA computer.

- **Define restricted groups.** You can define what memberships are allowed in CA management groups, such as custom groups for the CA administrator or CA manager role.
  - **Assign user rights.** The Manage Auditing and Security Log must be assigned to the holders of the Auditor Common Criteria role, and the Backup Files and Directories and the Restore Files and Directories user right must be assigned to the holders of the Backup Operator Common Criteria role. Also consider limiting the Allow Log on Locally and Allow Log on Using Terminal Services user rights to Common Criteria role holders only.
  - **Auditing.** Ensure that both success and failure auditing is enabled for object access so that the specific CA auditing events are captured to the Windows Security event log.
- **Enable all auditing options in the properties of the Certification Authority.** By enabling all auditing options for the CA, you ensure that the Windows security log will contain all relevant security events related to Certificate Services operations.

## Scripting the Configuration of Auditing Settings

The command `certutil -setreg CA\AuditFilter #`, where `#` is the sum of the values assigned to each audit setting on the Auditing tab. Figure 7-1 shows the Auditing tab of a CA, as well as the values associated with each check box on the tab.



**Figure 7-1** The values assigned to each check box on the Auditing tab of a CA's properties

For example, if you want to enable auditing to Back up and restore the CA database (2), Revoke certificates and publish CRLs (8), and Store and retrieve archived keys (32), the sum of these options is 2+8+32, which is equal to 42. This means that to enable only these auditing options, you must run the command `certutil -setreg CA\AuditFilter 42`.

- **Limiting membership in the local Administrators group.** If you implement the CA using any of the Microsoft cryptographic service providers (CSPs), the private key for the CA is stored in the Local Machine store. By default, all members of the local Administrators group can access the private key and export the private key to a PKCS #12 file. By limiting membership in the administrative groups, you can limit the number of users that could access the CA's private key.



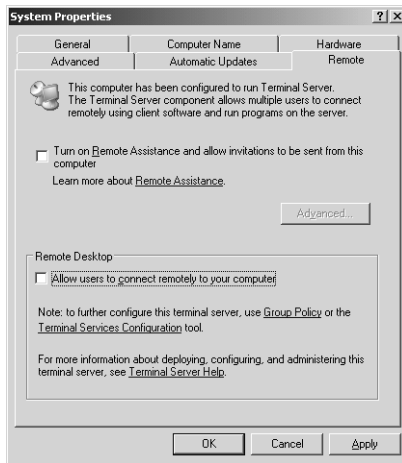
**Note** Alternatively, storing the private key on a hardware security module (HSM) will prevent this type of security issue, as the security mechanisms of the HSM will protect against a single local Administrator gaining access to the CA's private key.

- **Enforcing role separation.** Enforcing role separation ensures that a single person cannot hold multiple Common Criteria roles. A user can hold only one of the following roles: CA administrator, certificate manager, auditor, or backup operator. Assignment of two or more of these roles results in the user being blocked from *all* certificate management actions.



**Note** Common Criteria role separation is enforced by running `certutil -setreg CA\RoleSeparationEnabled 1` at a command prompt and then restarting Certificate Services. Remember that any user who is assigned two or more administrative roles will be blocked from all CA management activities from this point forward, unless you disable enforcement of Common Criteria role separation by running `certutil -delreg CA\RoleSeparationEnabled`, and then restarting Certificate Services.

- **Preventing terminal services administration of the CA computer.** You can prevent terminal services administration of a CA computer by ensuring that the Remote Desktop feature on the CA computer is disabled. This option is set on the Remote tab in the System Properties dialog box. (See Figure 7-2.)



**Figure 7-2** Preventing remote desktop Connections to the CA



**Note** This feature is disabled by default, but you should ensure that it remains disabled.

In addition to disabling the Remote Desktop feature, you can also assign the Everyone group the Deny Logon Through Terminal Services user right in the local security policy or in a security template imported into a Group Policy object applied to the CA computer account in Active Directory.



**Tip** A good starting point for securing Windows Server 2003 Certificate Services is to use the Hisecws.inf security template available in the Security Templates MMC console. Microsoft has performed extensive testing with this security template.

## Designing Physical Security Measures

In addition to CA configuration security measures, you should implement several physical security measures to protect your CA computers.



- **Store the offline CA computers in a physically secured room.** Rather than keeping offline CA computers in the standard server room, consider storing the offline CAs in a limited-access server room or in a safe. Allow only those with CA Administration roles to enter the server room or open the safe, and record all attempts to access the server room. Alternatively, you can enforce physical access logs, where any access to the CA computers is logged.
- **Store the CA computers in a secured cage.** Server cages are available that require PIN codes to open. Some models even track all attempts to access the server cage and allow retrieval of the access logs via serial connections.
- **Store hardware related to offline CAs in a separate, secured location.** Some companies remove the hard drives from the CA computers and store them in a remote safe, requiring an attacker to gain access to both the server hardware and the server drives before gaining access to an offline CA.



**Note** This methodology allows companies to use the offline server computer for alternative purposes when the CA is removed from the network by loading a separate set of hard drives into the CA computer chassis.

- **Disable hardware in the CA computer BIOS.** If you wish to prevent the attachment of the CA computer to the network, you can disable the network cards in the server's basic input/output system (BIOS) and protect the BIOS with a password. In addition, you can consider disabling universal serial bus (USB) ports and other devices to prevent copying data from the CA computer hard disk.
- **Implement BIOS startup passwords for offline computers.** You can further restrict access to the computer by implementing BIOS startup passwords. To start an offline CA computer, you must enter a BIOS startup password. This prevents a user that does not know the startup password from booting the offline CA.



**Warning** On some systems, a BIOS startup password can be reset to a blank password by shorting out the battery on the motherboard of the computer. If you physically store the computer in a safe or limited-access server room, you protect against an unauthorized user physically accessing the server to reset the BIOS password.

- **Implement SYSKEY level two or level 3.** Another method of restricting the booting of an offline CA is to implement system key (SYSKEY) level 2 or level 3 security. SYSKEY level 2 requires that a password be entered before the local accounts database is accessed, allowing the offline CA computer to start. A SYSKEY level 3 setting increases the security, by requiring that a floppy disk containing the SYSKEY password be inserted in the floppy drive to boot the computer.



**Warning** If you implement SYSKEY level 2 or level 3 and forget the password or lose access to the password on the SYSKEY disk, you lose all access to the offline CA computer. Ensure that the password is recorded in a secure location or that a copy of the SYSKEY disk is maintained to protect against this type of failure.

## Securing the CA's Private Key

Your security measures must protect a CA's private key. If an individual is able to obtain the CA's private key, it is possible to build another CA computer with the same key pair, allowing impersonation of the CA and the ability to issue fraudulent certificates that are trusted by all users of your public key infrastructure (PKI). In a worst-case scenario, if the root CA private key is obtained, an attacker can build additional CAs that are trusted by the users and computers within your organization.

The measures you should take to protect your CA's private key depend on how the private key is stored. For a Windows Server 2003 CA, there are three possibilities:

- Store the private key in the Local Machine store of the CA computer.
- Store the private key on a two-factor device, such as a smart card.
- Store the private key on a hardware security module (HSM).

### Private Key Stored in the Local Machine Store

If the CA's private key is stored in the Local Machine store of the CA computer, by default it is possible for *any* member of the local Administrators group to export the CA's private key to a PKCS #12 file. If the CA is a domain member, as is typical for online CAs, the local Administrators group of the CA computer will also include the Domain Admins group from the domain where the CA's computer account exists and could also contain the forest root domain's Enterprise Admins group and other custom groups defined by the organization.

The only way to protect the private key in this scenario is to attempt to limit membership in the local Administrators group. In addition, if your organization uses

image for server installations, changing the default Administrator account and password from the default stored in the server image is recommended. This protects against access to the private key by anyone who gains knowledge of the default Administrator account and password.

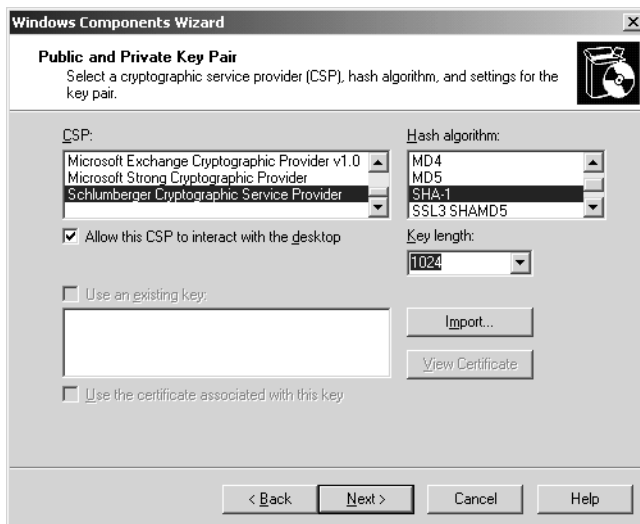


**Warning** Even if you implement Restricted Groups to limit membership in the local Administrators group, a member of Enterprise Admins or the domain's Domain Admins group can add his account to the local Administrators group. Limiting the membership of the local Administrators group ensures that the membership is initially restricted. Only by auditing membership and configuration changes can you detect whether a rogue member of the Enterprise Admins or Domain Admins group is attempting to modify the security settings.

## Private Keys Stored on Smart Cards

To increase the security of the private key, you can store the key on a two-factor device, such as a smart card. Moving the CA's private key to a smart card requires a CA Administrator to have access to the smart card and know the smart card's PIN.

If you implement a smart card cryptographic service provider (CSP), you must enable the Allow CSP to Interact with the Desktop option during the Certificate Services Installation Wizard. (See Figure 7-3.) The Allow CSP to Interact with the Desktop option enables the display of the PIN entry dialog box for the smart card in the user's session when a machine-related private key is accessed.



**Figure 7-3** Allowing a smart card CSP to interact with the Windows desktop

You can further secure the implementation of a smart card for protecting the CA's private key by storing the CA's smart card in a secure location, such as a safe. By splitting the responsibilities of retrieving the smart card from the safe and knowing the smart card's PIN, you can ensure that at least two people are involved in starting Certificate Services at an online CA.



**Note** If you implement a smart card for the CSP of an online CA, the smart card must remain in the smart card reader of the CA computer at all times. Removing the smart card from the reader causes the computer to lose access to the private key material. This prevents Certificate Services from starting, new certificates cannot be issued, and updated certificate revocation lists (CRLs) cannot be published.

## Private Keys Stored on Hardware Security Modules

A hardware security module protects a CA's private key by removing the key from the CA computer to a cryptographic device. The CA performs all cryptographic functions on Hardware Security Module (HSM), including key generation, certificate signing, and CRL signing.

Moving the key material from the CA to the HSM protects the key material against any attacks against the CA operating system. In addition, an HSM increases the protection of the private key by allowing an organization to require the involvement of several administrative personnel to access the key. For example, you can configure the HSM to require that four of nine administrators be present for an offline CA to publish an updated CRL or issue a new subordinate CA certificate. This requirement of a quorum of administrators being present is known as an "M of N" scheme.



**Note** As with a smart card CSP, you must allow an HSM's CSP to interact with the desktop so that the operators of the HSM are prompted to authorize all private key usage by the HSM (during an interactive logon session).

## Hardware Security Modules

Hardware security modules allow you to increase the protection of the CA's private key to meet Federal Information Processing Standards (FIPS) 140-2 level 2 and level 3 security. A FIPS 140-2 level 3 device protects the CA's private key by providing two functions:

- The cryptographic device is tamper evident. The cryptographic store on an HSM is typically coated with an epoxy layer, so that any attempts to access the cryptographic store is indicated in the epoxy layer.
- If an attempt to compromise the cryptographic store on the HSM takes place, the data stored on the cryptographic store—namely the private key—is destroyed, which protects the private key against compromise.



**More Info** The FIPS 140-2 document that defines the security requirements for cryptographic modules can be found at <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>.



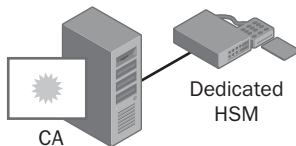
**Note** FIPS 140-2 level 4 devices now exist. A FIPS 140-2 level 4 device adds physical security to the HSM by providing a physical envelope of protection around the cryptographic module.

## Categories of HSMs

In general, you can separate HSMs into two categories: dedicated HSMs and network-attached HSMs.

### Dedicated HSMs

A dedicated HSM is directly attached to a CA through either a SCSI card or a proprietary PCI card inserted into the CA computer. (See Figure 7-4.)

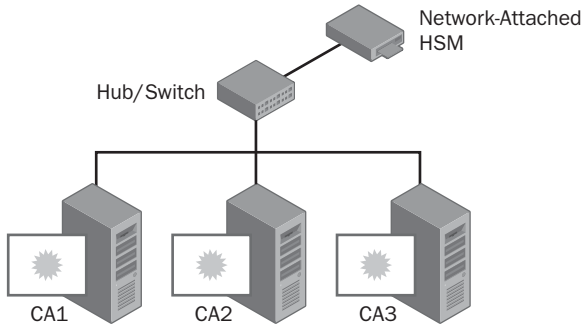


**Figure 7-4** A dedicated HSM

All communications with the CA computer are performed through the PCI or SCSI connection and the private key material never leaves the protective space of the dedicated HSM. To allow communications with the HSM, a proprietary CSP must be installed on the CA computer. If required, device drivers for both the HSM and the HSM interface card also must be installed on the CA computer to allow communications between the CA computer and the HSM.

## Network-attached HSMs

Network-attached HSMs are another alternative for cryptographic security. Rather than implementing a dedicated HSM at each CA in the hierarchy, two or more CAs can share the same HSM. (See Figure 7-5.)



**Figure 7-5** A network-attached HSM

As with a dedicated HSM, all cryptographic operations occur within the HSM and the results are transmitted to the CA from the HSM. To protect communications between the CA and the HSM, the network channel is protected through both encryption and authorization. In other words, all communications are encrypted between the CA and the HSM. In addition, CAs authorize the HSM through unique hashes, certificates, or serial numbers and authorize the clients through certificates, IP addresses, or hashes.

You cannot implement an unlimited number of clients with a single network-attached HSM. The maximum number of client CAs is determined by the model of the network-attached HSM and the license agreement purchased by your organization.



**Note** The HSM and the CA computer do not have to be on the same network segment. The HSM and CA computer can be separated by routers and even firewalls as long as the required ports for communications are opened between the HSM and the CA computers.

## HSM Vendors

nCipher and Rainbow Chrysalis-ITS are the two most commonly selected HSM manufacturers when an organization wants to implement HSMs to protect the private keys for Windows Server 2003 CAs.

### nCipher

nCipher provides the following dedicated and network-attached solutions for HSMs:

- **nShield.** A dedicated HSM that attaches to the CA computer with either a PCI or a SCSI interface, depending on the model of HSM. nShield is available in both a FIPS 140-2 level 2 and level 3 format. This provides flexibility for an organization by allowing deployment of different levels of FIPS 140-2 protection for offline and online CAs if required by an organization's security policy.
- **netHSM.** A network-attached HSM that requires all clients to use either the Impath or Inter-module path protocol. Developed by nCipher, the Impath protocol is a protocol that is similar to Secure Sockets Layer (SSL) security in its operation. This protocol accepts connections to Transmission Control Protocol (TCP) port 9004. To interact with the netHSM, the CA computer must be configured with an IP address, the serial number, and the hash of the netHSM's encryption key. In addition, the netHSM must have the CA computer's IP address added as a valid client IP address.



**Note** If you change the IP address of either a CA computer or the netHSM, you must reconfigure the relationship between the netHSM and the CA computer.

nCipher's HSM management roles are defined in an nCipher security world. A security world consists of the following components:

- **One or more HSMs.** A CA can be configured to connect to a single HSM or to a series of daisy-chained HSMs.
- **Management software.** nCipher provides software for installing the CSP, management tools for the HSM, device drivers for direct-attached nShield devices, and software for connectivity to a netHSM.
- **Host server that stores nCipher-specific management information.** This is the CA computer when using an nShield HSM or any online computer that can connect to the netHSM and act as the remote file system (RFS). The RFS contains information about all administrative and operator card sets implemented at the netHSM:
  - An administrative card set (ACS) is used to restore a security world; recover keys if key recovery is enabled; replace an existing ACS; recover pass phrases if enabled for the security world; delegate FIPS 140-2 level 3 authorization activities; and manage key counting.
  - An operator card set (OCS) is used to authorize use of the CA's private key and FIPS 140-2 level 3 management tasks.
- **Smart cards.** Smart cards provide credential storage for both administrative and operational roles in managing the netHSM.

The use of two card sets in a security world allows you to implement role separation in the management of the CA. Typically, the ACS is managed by an organization's security officer. The security officer determines who will be key holders in the ACS. The OCS is more closely related to the operational staff of the PKI, as the card set is required for accessing the private key of the CA.

Each ACS and OCS card from a card set is managed by a unique individual and, if desired, assigned a unique PIN. In both cases, you can implement a split-key solution where the key material for authorizing an ACS or OCS transaction requires presentation of multiple smart cards.

For example, you can define that all ACS operations require three of a possible seven cards to be presented. The key generated for the ACS is split between the seven smart cards so that any combination of three will authorize an ACS transaction. The same is true for an OCS. nCipher refers to this type of configuration as “k of n” key fragmentation.



**Note** You can define different k of n values for each ACS management function. For example, you could require three of seven ACS cards to restore a security world but require five of the same seven cards to replace the existing ACS.

Each nCipher installation therefore forms a completely separate nCipher security world and is independent of the number of actual physical HSM devices deployed. Each nCipher security world, on the other hand, can be securely extended for central management by the same security officer, and can share keys belonging to the same trust chain. Keys and card sets are tied to their originating module keys and will cease to be valid if the nCipher security world is reinitialized. The ACS and OCS card sets are not interchangeable; access to one provides no access to the other.



**More Info** More details on nCipher devices and configuration can be found at [www.ncipher.com](http://www.ncipher.com).

## Rainbow Chrysalis-ITS

Rainbow Chrysalis-ITS provides the following dedicated and network-attached HSM solutions:

- **Luna CA3.** A dedicated HSM that connects to the CA computer by a proprietary PCI card. The Luna CA3 provides fault tolerance by daisy chaining multiple Luna CA3 devices to a single CA.



- **Luna SA.** A network-attached HSM that implements SSL encryption between the CA computer and the Luna SA device. To enable SSL encryption, the CA computer and the Luna SA generate self-signed certificates. The Luna SA certificate provides encryption services for the connection between the CA computer and the Luna SA, as well as authentication of the Luna SA. The client certificate validates the identity of the CA client computer to the Luna SA.

The Luna CA3 and the Luna SA each have five different roles for the management of the HSM. Each role-holder is given a plastic key, with different colors representing different PKI management roles. Each key contains an electronic chip that might or might not be protected by a PIN that identifies the role holder. PKI management roles and their keys are:

- **HSM initializer (gray).** The gray key is used to initialize the token or HSM during setup. The gray key must be protected to ensure that an attacker cannot reinitialize the HSM, resulting in the loss of all key material stored on the HSM.
- **Security officer (blue).** The blue key is PIN protected. The security officer is able to create users, define HSM partition owners, and change passwords. You can create backup copies of the blue key, but each copy of the blue key for a specific set of keys will have the same PIN. The blue keys can be defined separately for each CA or be shared between multiple CAs in the CA hierarchy.
- **HSM partition owner (black).** The black key allows creation of encryption keys and encrypted objects in an HSM partition. As with the blue key, a black key is PIN protected; the PIN is the same across all black keys in a related set. Black keys can be used across multiple CAs in a CA hierarchy.
- **Key cloning vector (red).** The red key stores the domain identifier for any defined group of HSMs. The domain identifier is an identifier that indicates whether the Luna tokens share the same red key for management of the Luna token or whether separate red keys are used for each Luna token. A partition can be backed up only to a backup token that shares the same domain identifier. In addition to being stored on the red key, the domain identifier is also stored on the current HSM partition. Multiple red keys can be created for backup purposes; no PIN is associated with a red key.
- **M of N key holders (green).** Green key holders can validate the functions of blue and black key holders. If M of N protection is enabled, any operations performed by the security officer or partition manager must be verified by a quorum of green key holders. The M of N parameter is defined when you initialize the HSM. For example, you can configure the HSM so that every security officer or partition manager task requires five of the nine green key holders to validate the task. If any number less than five is present, the task is blocked.



**Note** Although this sounds similar to the k of n solution implemented by nCipher, there are differences between the two. With the Luna CSP, a PIN is only required by the security officer (blue key) or partition manager (black key) holder. The green key holders do not require a PIN when they validate the actions of the blue or black key holders. For the nCipher CSP, a PIN is required for all OCS and ACS cards in the card set. For this reason, you must ensure that the green keys are distributed to each key holder individually, and are not stored in a common location such as a safe. This ensures that the keys are not misused when “M of N” or “k of n” validation is taking place.

All Luna HSMs includes a personal entry device (PED) with a socket for key insertion. Each key is activated by putting the key in the socket and turning the key a quarter turn. If the key is blue or black, the associated PIN must be input using the numeric keypad on the Luna PED.



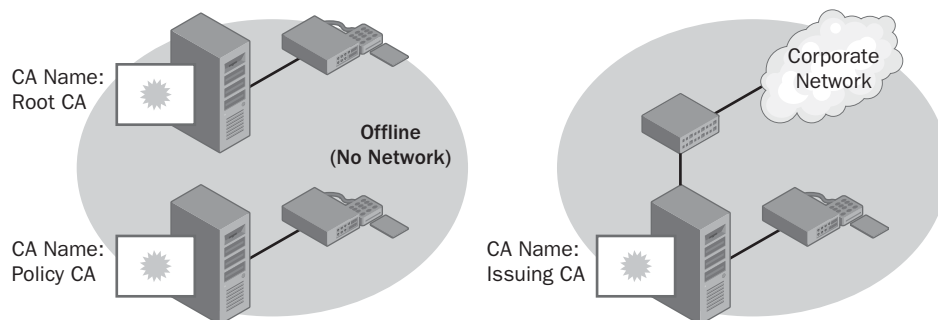
**More Info** More details on Luna devices and configuration can be found at [www.chrysalist-its.com](http://www.chrysalist-its.com).

## HSM Deployment Methods

Several options exist for deploying HSMs in a CA hierarchy. This section reviews some of the more common designs, and discusses the advantages and disadvantages of each.

### Dedicated HSMs on Each CA

The most common deployment method for HSMs is to implement a dedicated HSM on each CA in the CA hierarchy. (See Figure 7-6.)



**Figure 7-6** Implementing dedicated HSMs at each CA in the CA hierarchy



**Note** This is the most common deployment method only because network-attached HSMs are a recent innovation introduced toward the end of the calendar year 2003.

Implementing dedicated HSMs at each CA in the CA hierarchy allows for deployment of different FIPS 140-2 security levels at each CA in the CA hierarchy. For example, if an organization's security policy requires FIPS 140-2 level 3 security for offline CAs and FIPS 140-2 level 2 security for online CAs, the required HSMs can be purchased on a CA-by-CA basis depending on the CA's role in the hierarchy.

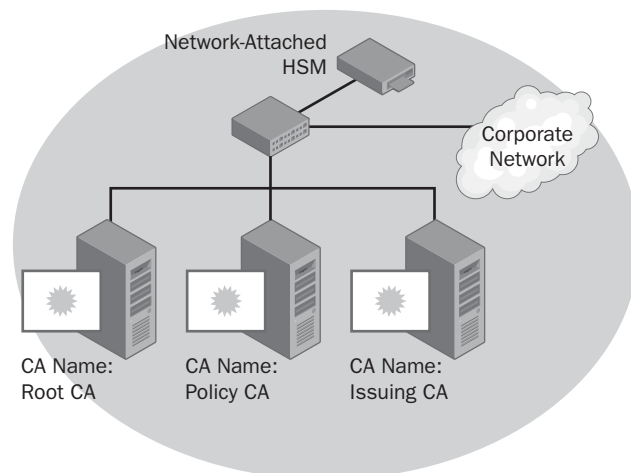
The advantage of implementing dedicated HSMs at each CA in the CA hierarchy configuration is that each CA has its own HSM. The failure of a single HSM will only affect a single CA, not multiple CAs. The disadvantage is cost. If your hierarchy has five CAs, you are looking at purchasing at least five HSMs, one for each CA.



**Note** You might require additional HSMs for redundancy. Alternatively, you could choose to share security worlds or domains among offline CAs and utilize the same HSM on each offline CA to reduce costs.

## Network-Attached HSMs on Each CA

With the introduction of network-attached HSMs, it is now possible for an organization to deploy a single HSM for the entire network or at each location that hosts CA computers, sharing the HSM among multiple CAs. One possible deployment scenario is to connect the HSM to a corporate network. (See Figure 7-7.)



**Figure 7-7** Implementing a network-attached HSM for all CAs in the hierarchy

When you implement a network-attached HSM for all CAs in the CA hierarchy, the HSM and all of the CAs in the hierarchy are connected to the corporate network.

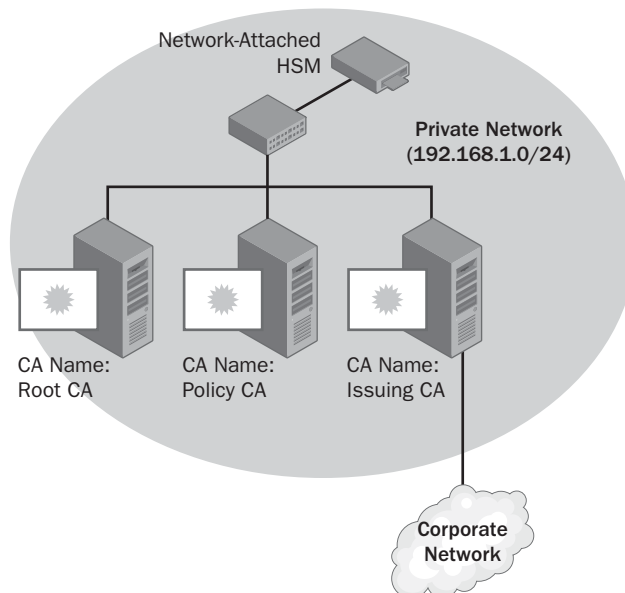


**Note** The CAs do not have to be on the same subnet as the HSM. As long as packets are able to pass freely between the CAs and the HSM and through any routers or firewalls in between, connectivity can take place between multiple network segments.

The obvious advantage of implementing a single network-attached HSM is that you reduce the hardware costs associated with HSMs. You are able to deploy a single HSM for all CAs in the hierarchy, subject to the licensing requirements of the HSM vendor. The disadvantage is that you must connect the offline CA computers to the corporate network when they have to connect to the HSM.

Some companies choose to temporarily disconnect the HSM from the corporate network and connect the offline CA computer directly to the HSM with a cross-over cable. While temporarily connecting the HSM to the offline CA secures communications with the HSM, it also prevents the online CA computers from communicating with the HSM, blocking access to the online CA's private key.

To prevent loss of communications to an online CA when accessing the HSM from an offline CA, you can deploy the network-attached HSM on a private network rather than the corporate network. (See Figure 7-8.)



**Figure 7-8** Implementing the network-attached HSM on a private network

When you implement a network-attached HSM on a private network, the network-attached HSM, offline CAs, and online CAs have connectivity on a dedicated private network. To allow communications with the corporate network, the issuing CA is dual-homed with network connectivity to both the private network and the corporate network.

The advantage of this configuration is that communication with the HSM is only possible by computers on the private network. When access to an offline CA computer is required, the offline CA computer can be connected to the private network without fear of network-based attacks from the corporate network.



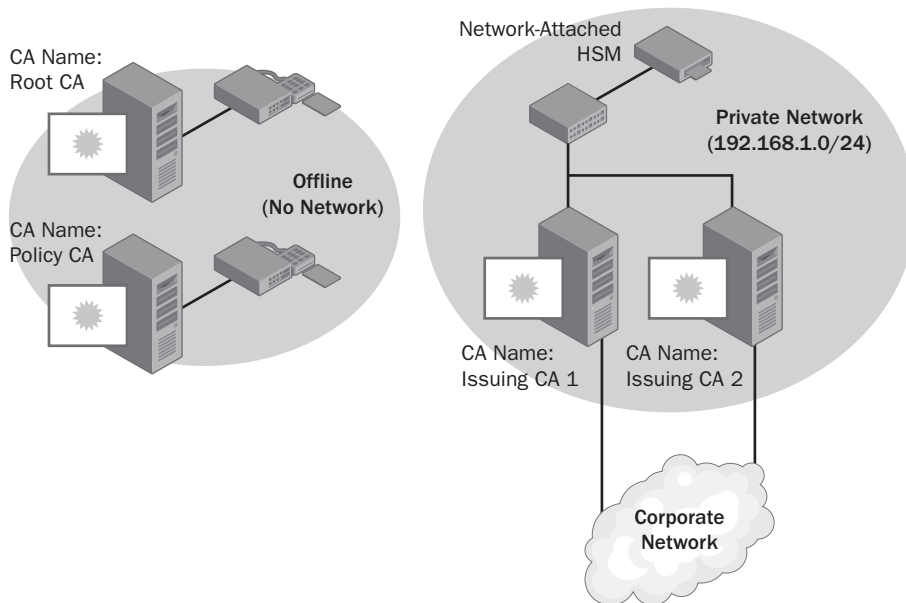
**Note** Additional security measures are required at the issuing CA to prevent attacks from the corporate network. The online CAs must prevent IP routing to stop attackers from routing packets to the private network through the online CAs. In addition, your organization can choose to prevent remote desktop connectivity to the offline CAs from the online CA computer. This can be accomplished through either Group Policy configuration or Internet Protocol Security (IPSec) filters that prevent connectivity on all ports from the online CAs to the offline CAs.

Another advantage of implementing a private network for the network-attached HSM is that all traffic between the CAs and the network-attached HSM is relegated to the private network, which allows the offline CAs to be attached to the network. Implementing a private network also allows changing the corporate network IP addressing scheme with limited configuration changes to the CAs and the HSM. This is because the IP addressing used to connect the CAs to the HSM is on the private network addressing where the IP addresses are not changed. The only drawback is that an organization's security policy must be modified to allow network connectivity of offline CAs.

### **Dedicated HSMs on Offline CAs and Network-Attached on Online CAs**

If an organization's security policy will not allow offline CAs to be connected to either the corporate network or a private network, you can deploy a combination of dedicated and network-attached HSMs. (See Figure 7-9.)

When you combine dedicated and network-attached HSMs, the offline CAs implement dedicated HSMs and are never attached to any form of network. The online CAs are connected to a network-attached HSM on a private network and are dual-homed, which allows connectivity to the corporate network.



**Figure 7-9** Combining dedicated and network-attached HSMs in a CA hierarchy

The advantage of this configuration is that physical access is required to use the offline CAs. Likewise, if an online CA is compromised, it does not allow an attacker to compromise an offline CA. By deploying the network-attached HSM on a private network, you ease the configuration changes at the online CAs and the network-attached HSM if IP addressing is modified on the corporate network.



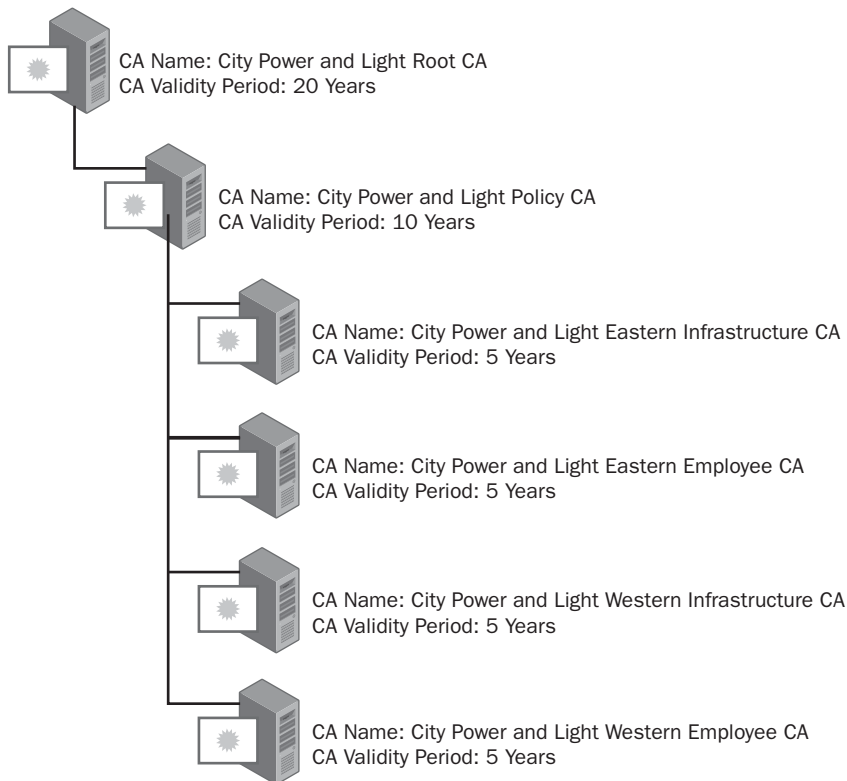
**Note** If you are deploying HSMs at multiple network locations, you will require a network-attached HSM at each network location. You can implement a single network-attached HSM only if you modify this configuration to deploy the HSM on the corporate network, rather than on a private network. This will allow CAs on remote networks to protect their key material on the HSM. The only risk is that if network connectivity is down, a remote CA will be unable to access its private key.

## Case Study: Planning HSM Deployment

In this case study, you will plan the physical and CA configuration security for your organization's CA hierarchy.

## Scenario

You are the security services manager for City Power and Light. Your organization has planned a three-tier CA hierarchy, shown in Figure 7-10.



**Figure 7-10** The City Power and Light CA hierarchy

The CA hierarchy implements both an offline root and an offline policy CA, to allow flexibility in the future if City Power and Light starts to issue certificates to its customers.

To provide high availability of Certificate Services, issuing CAs are deployed at Atlanta, Georgia, for the east coast, and at Anaheim, California, for the west coast. The network management model defines separate managers for the certificates issued to infrastructure components, such as computers and network devices and the certificates issued to City Power and Light employees.

The security policies of City Power and Light include:

- All CA computers in the CA hierarchy must implement FIPS 140-2 level 3 protection for the CA key material.
- The root and policy CAs are maintained at the City Power and Light head office in Chicago.

- Offline CA computers must *never* be attached to the network. All interaction with the issuing CAs in the CA hierarchy must be performed using USB tokens.
- Any operations of the offline CAs must involve the approval of three of the five network managers and City Power and Light. This includes the installation of the CA hierarchy and the issuance of subordinate CA certificates and CRLs.
- The IP addressing scheme used on the City Power and Light network has changed three times in the past five years. The CA security design must minimize the impact of these IP addressing scheme changes on the operations of the CAs.
- Online CAs must audit all security events at the CA except the starting and stopping of Certificate Services. For offline CAs, all security events must be audited at the CA.

## Case Study Questions

1. If you were to script the configuration of auditing settings for the offline CAs, what command would you include in the script to meet the auditing requirements?
2. What command is required to meet the audit setting requirements for the online CAs?
3. Can you meet the security requirements for the CA hierarchy by implementing either a software-based CSP or a smart card CSP? Why or why not?
4. Can you use dedicated HSMs at each CA in the hierarchy and meet the design requirements? What are the drawbacks to this approach if it is possible?
5. Can you use network-attached HSMs at each CA in the CA hierarchy and meet the design requirements? What are the drawbacks to this approach if it is possible?
6. If you want to implement network-attached HSMs for the issuing CAs in the CA hierarchy, how many network-attached HSMs would you recommend to City Power and Light?
7. If you were to implement Luna HSMs for the solution, how would you implement the management requirements for operations of the offline CAs?
8. If you were to implement nCipher HSMs for the solution, how would you implement the management requirements for operations of the offline CAs?



## Additional Information

- Microsoft Official Curriculum, Course 2821: “Designing and Managing a Windows Public Key Infrastructure” ([www.microsoft.com/traincert/syllabi/2821afinal.asp](http://www.microsoft.com/traincert/syllabi/2821afinal.asp))
- Microsoft Windows Security Resource Kit ([www.microsoft.com/mspress/books/6418.asp](http://www.microsoft.com/mspress/books/6418.asp))
- “Windows 2000 Server and PKI: Using the nCipher Hardware Security Module” ([www.microsoft.com/technet/security/prodtech/win2000/ncipher.mspx](http://www.microsoft.com/technet/security/prodtech/win2000/ncipher.mspx))
- “Deploying Certificate Services on Windows 2000 and Windows Server 2003 with the Chrysalis-ITS Luna CA3 Hardware Security Module” ([www.microsoft.com/windows2000/techinfo/planning/chrysalis.asp](http://www.microsoft.com/windows2000/techinfo/planning/chrysalis.asp))
- “Microsoft Windows Server 2003 PKI and Deploying the nCipher nShield Hardware Security Module” ([www.ncipher.com/resources/downloads/files/white\\_papers/win2003\\_nshield\\_wp.pdf](http://www.ncipher.com/resources/downloads/files/white_papers/win2003_nshield_wp.pdf))
- nCipher nShield HSM ([www.ncipher.com/nshield/index.html](http://www.ncipher.com/nshield/index.html))
- nCipher netHSM ([www.ncipher.com/nethsm/index.html](http://www.ncipher.com/nethsm/index.html))
- Luna CA3 ([www.rainbow.com/products/luna/luna\\_ca3.asp](http://www.rainbow.com/products/luna/luna_ca3.asp))
- Luna SA ([www.rainbow.com/products/luna/luna\\_sa.asp](http://www.rainbow.com/products/luna/luna_sa.asp))
- “Windows Server 2003 PKI Operations Guide” ([www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03pkog.mspx](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03pkog.mspx))



## Chapter 8

# Designing Certificate Templates

Certificate templates are used by Microsoft Windows Server 2003 public key infrastructure (PKI) to define the contents of certificates issued by enterprise certificate authorities (CAs). The Certificate Templates Microsoft Management Console (MMC) provides an easy-to-use interface for defining and customizing certificate templates.



**More Info** For more detailed information on modifying and creating certificate templates, see the “Implementing and Administering Certificate Templates in Windows Server 2003” white paper referenced in the “Additional Information” section at the end of this chapter.

## Certificate Template Versions

Windows Server 2003 supports two versions of certificate templates: version 1 and version 2. All certificate templates are stored as objects in Microsoft Active Directory and are stored in the configuration naming context in the following location: CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,*ForestRootDomain* (where *ForestRootDomain* is the Lightweight Directory Access Protocol [LDAP] distinguished name of the forest root domain).

Certificate templates have a forest-wide definition and can be modified by a user with the necessary permissions at any computer where the Certificate Templates console is installed. By storing certificate templates in the configuration naming context, definition availability is ensured because the certificate templates are replicated to every domain controller in the forest.

### Version 1 Certificate Templates

Version 1 certificate templates were introduced with Windows 2000 Certificate Services and are available for Windows Server 2003 enterprise CAs. Attributes of version 1 certificate templates cannot be modified, except for the permissions assignments.

When you install an enterprise CA or launch the Certificate Templates console, the following version 1 certificate templates are automatically installed in Active Directory:

- **Administrator.** Allows a holder to perform trust list signing, send secure e-mail, encrypt and decrypt files protected by the Encrypting File System (EFS), and perform user authentication.
- **Authenticated Session.** Enables a holder to use a certificate for user authentication.
- **Basic EFS.** Allows a user to use a certificate for encrypting and decrypting files.



**Note** If this certificate template is not available, and version 2 certificate templates are not distributed to users automatically, a user will generate a self-signed Basic EFS certificate template. See Chapter 16, “Encrypting File System” for more details on EFS.

- **CEP Encryption.** Permits a holder to act as a registration authority (RA) for Simple Certificate Enrollment Protocol (SCEP) requests from Cisco network equipment.



**Note** The CEP Encryption certificate template requires that the MSCEP add-on be installed at the CA. The MSCEP add-on is included in the Windows Server 2003 Resource Kit tools referenced in the Additional Information section at the end of this chapter.

- **Code Signing.** Permits a holder to digitally sign software.
- **Computer.** Allows a computer to authenticate to other computers and users on the network.
- **Domain Controller.** Allows a domain controller to authenticate to other computers and users on the network.
- **EFS Recovery Agent.** Allows a holder to decrypt files previously encrypted with EFS if the holder is designated as a data recovery agent for the file.
- **Enrollment Agent.** Allows a holder to request certificates, such as smart card certificates, on behalf of other users.
- **Enrollment Agent (Computer).** Allows a computer account to request certificates on behalf of another subject.



**Note** The Enrollment Agent (Computer) certificate is required if you deploy the Microsoft Exchange 5.5 or Exchange 2000 Key Management Service (KMS) to allow the server to request Email certificates on behalf of any user.

- **Exchange Enrollment Agent (Offline request).** Allows a computer host in the KMS to request certificates on behalf of Exchange e-mail encryption users.
- **Exchange Signature Only.** Allows a holder to send digitally signed Secure/Multipurpose Internet Mail Extensions (S/MIME) e-mail messages.
- **Exchange User.** Allows a holder to receive and decrypt encrypted S/MIME e-mail messages.
- **IPSec.** Allows computers to digitally sign, encrypt, and decrypt network communications that use Internet Protocol Security (IPSec).
- **IPSec (Offline request).** Allows computers that are not members of the forest to participate in IPSec communications.
- **Root Certification Authority.** Allows a computer to function as the root CA of a CA hierarchy.
- **Router (Offline request).** Allows a router to request certificates from a CA that holds a Certificate Enrollment Protocol (CEP) encryption certificate by using SCEP.
- **Smartcard Logon.** Allows a holder to authenticate with the network using a smart card.
- **Smartcard User.** Allows a holder to authenticate with the network and send and receive digitally signed and encrypted e-mail messages using a smart card.
- **Subordinate Certification Authority.** Permits a computer to function as a subordinate CA in a CA hierarchy.
- **Trust List Signing.** Allows a holder to digitally sign a certificate trust list.
- **User.** Permits a holder to send digitally signed or encrypted e-mail and authenticate with the network using certificate-based authentication.
- **User Signature Only.** Allows a holder to authenticate with the network using certificate-based authentication.
- **Web Server.** Allows a Web server to implement Secure Sockets Layer (SSL) security. The certificate proves the identity of the Web server and is used to encrypt communications between a Web client and the Web server.

## Version 2 Certificate Templates

Version 2 certificate templates extend the abilities of version 1 certificate templates and are fully customizable. You can define any attribute within version 2 certificate templates, whereas version 1 certificate templates only allow permission modification. Windows Server 2003 ships with several version 2 certificate templates and allows new templates to be defined by duplicating existing version 1 or version 2 templates.



**Note** Certificates based on version 2 templates can be issued only by enterprise CAs running on Windows Server 2003, Enterprise Edition, or Windows Server 2003, Datacenter Edition.

The following version 2 certificate templates are automatically installed in Active Directory when you open the Certificate Templates MMC for the first time or install a Windows Server 2003 enterprise CA.

- **CA Exchange.** Allows a computer to encrypt private key material sent to the CA for key archival. The certificate is only issued to a CA that enables archival of private keys.
- **Cross Certification Authority.** Permits your organization to define qualified subordination constraints when issuing certificates to CAs outside of your organization's CA hierarchy.
- **Directory Email Replication.** Allows domain controllers to use secure Simple Mail Transfer Protocol (SMTP) for replication.
- **Domain Controller Authentication.** Allows domain controllers to authenticate with users and computers in the forest using certificates.
- **Key Recovery Agent.** Allows a CA to implement key archival and recovery. The Key Recovery Agent certificate is used to encrypt and decrypt the certificate and private key in the CA database.
- **RAS and IAS Server.** Allows Remote Access Service (RAS) and Internet Authentication Service (IAS) servers to mutually authenticate with remote clients.
- **Workstation Authentication.** Allows computers to mutually authenticate with other computers and users on the network.



**Note** Users with Windows 2000 computers can request version 2 certificate templates through the Certificate Services Web Enrollment pages or through custom scripts using the Certificate Enrollment control. Users with Windows XP and Windows Server 2003 computers can also use autoenrollment or the Certificate Enrollment Wizard.

## Enrolling Certificates Based on Certificate Templates

For both version 1 and version 2 certificate templates, the ability to enroll a certificate based on a certificate template is defined in the discretionary access control list (DACL) associated with a specific certificate template. If users have both Read and Enroll permissions assigned to their user accounts or to groups in which their user accounts have membership, they can request certificates based on the certificate template. Likewise, if a user is assigned the Read, Enroll, and Autoenroll permissions for a version 2 certificate template, the certificate can be deployed automatically through Group Policy.

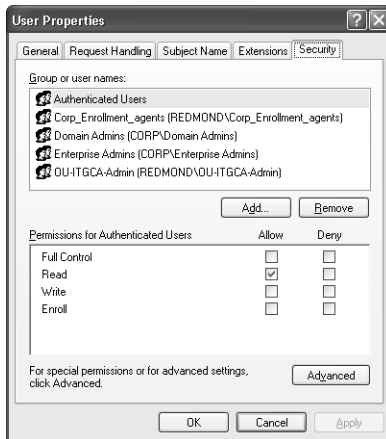
## Modifying Certificate Templates

Creation and modification of certificate templates is an important step when deploying PKI-enabled applications. For each application, you must identify the required certificate templates and then customize them according to your PKI design document.

To modify a version 2 certificate template, you must log on as a user that has Read and Write permissions for the certificate template. Once logged on, a user can use the Certificate Templates console (`certtmpl.msc`) to modify existing certificate templates or create new version 2 certificate templates.

## Modifying Version 1 Certificate Template Permissions

Version 1 certificate templates allow the permission settings for the certificate template to be modified. You cannot modify the contents of a version 1 certificate template, however. Figure 8-1 shows the Security tab for a version 1 certificate template.



**Figure 8-1** Modifying the Security tab for a version 1 certificate template

In the security template, you can add global or universal groups from Active Directory and assign a combination of the following permissions:

- **Full Control.** Allows a permission holder to modify the permissions of the version 1 certificate template and to change the ownership of the certificate template.
- **Read.** Allows a permission holder to see the certificate template when enrolling for certificates. Read permission is required to enroll a certificate based on a version 1 certificate template and for a certificate server to find the certificate templates in Active Directory.
- **Write.** Allows a permission holder to modify permissions of a version 1 certificate template.
- **Enroll.** Allows a permission holder to enroll for a certificate based on the certificate template. To enroll for a certificate, the security principal also must have Read permissions.

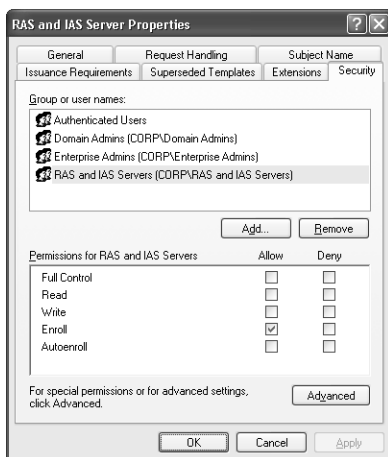
## Modifying Version 2 Certificate Templates

Version 2 certificate templates allow users with Write permission to change any attribute. The following sections detail modifications that can be made to version 2 certificate templates on a tab-by-tab basis.

### The Security Tab

As with version 1 certificate templates, the Security tab defines the permissions for version 2 certificate templates. (See Figure 8-2.)





**Figure 8-2** Modifying the Security tab for a version 2 certificate template

For a version 2 certificate template, the definition of the Write permission includes the ability to change *any* attribute of the certificate template, not just the permission of the certificate template.

The only additional permission for a version 2 certificate template is the Autoenroll permission. When a user or computer is assigned Read, Enroll, and Autoenroll permissions, it is possible to automatically distribute the certificate to the user or computer.



**Note** Autoenrollment is only supported for Windows XP or later.

## The General Tab

On the General tab (see Figure 8-3), you can configure the following attributes of the certificate template:

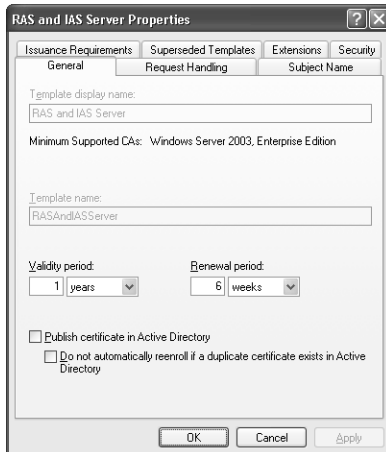
- **Template Display Name.** The display name of the version 2 certificate template shown in the MMC, the Certificate Services Web Enrollment pages, and the Certificate Services Enrollment Wizard.
- **Template Name.** The name of the *PKI-Certificate-Template* object created in the CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration, *ForestRootDomain* container.
- **Validity Period.** Defines the certificate template's validity period.

- **Renewal Period.** Defines the time before the validity period expires, which is when autoenrollment attempts to re-enroll a certificate based on the certificate template.



**Note** Default values defined for the renewal period prevent you from setting too short of a renewal period. For more details, see the “Implementing and Administering Certificate Templates in Windows Server 2003” white paper referenced in the “Additional Information” section at the end of this chapter.

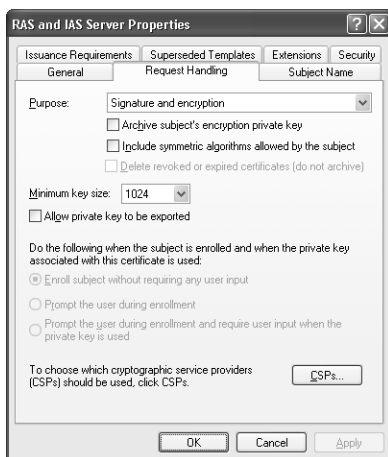
- **Publish Certificate in Active Directory.** Allows you to publish the certificate into the *userCertificate* attribute of a user account object. This option is typically enabled to allow other users to access the associated public key of their encryption certificate.
- **Do Not Automatically Re-Enroll If a Duplicate Certificate Exists in Active Directory.** Prevents a user from enrolling multiple copies of a certificate based on the certificate template. If a version is already published in Active Directory, re-enrollment is prevented during autoenrollment processes.



**Figure 8-3** Modifying the General tab for a version 2 certificate template

## The Request Handling Tab

On the Request Handling tab (see Figure 8-4), you can configure the following attributes of the certificate template:



**Figure 8-4** Modifying the Request Handling tab for a version 2 certificate template

- **Purpose.** Describes the overall purpose of the certificate template. Available options are:
  - **Encryption.** The certificate's key pair can be used to encrypt data.
  - **Signature.** The certificate's key pair can be used to sign data or verify the signature applied to data.
  - **Signature and Encryption.** The certificate's key pair can be used for encryption and digital signature applications.
  - **Signature and Smart Card Logon.** The certificate's key pair can be used to sign data, verify the signature applied to data, or encrypt and decrypt data for Kerberos authentication. In addition, the key pair must be stored on a two-factor hardware device, such as a smart card.



**Note** The Purpose setting determines what other settings are enabled or disabled on the Request Handling tab. For example, the Archive Subject's Encryption Private Key check box is only enabled if the certificate purpose is set to Encryption or Signature And Encryption.

- **Archive Subject's Encryption Private Key.** Enables archival of the certificate's private key in the CA database. To use this option, key archival must be enabled at the CA.

- **Include Symmetric Algorithms Allowed By the Subject.** Ensures that supported symmetric encryption algorithms are included in the certificate for applications such as Microsoft Outlook.
- **Delete Revoked or Expired Certificates (Do Not Archive).** Deletes the subject's previous signing certificate from the local store if the previous certificate is expired or revoked when a newer version is obtained from the CA.
- **Minimum Key Size.** Defines the private or public key's minimum size in bits as allowed by the CSP. You cannot set a minimum key size above or below the value allowed by the CSP.
- **Allow Private Key to be Exported.** Enables or disables the user's ability to export the certificate's private key.
- **Do the Following When the Subject Is Enrolled and When the Private Key Associated with this Certificate Is Used.** Defines what level of user interaction is required during the certificate enrollment process if autoenrollment is used to deploy the certificate. The options are:
  - **Enroll Subject Without Requiring Any User Input.** The certificate enrollment occurs silently, without any notification to the user.



**Note** You must set the Enroll Subject Without Requiring Any User Input option if you want to silently distribute certificates to users. If you want to distribute computer certificates with autoenrollment, you must enable the option to not require any user input.

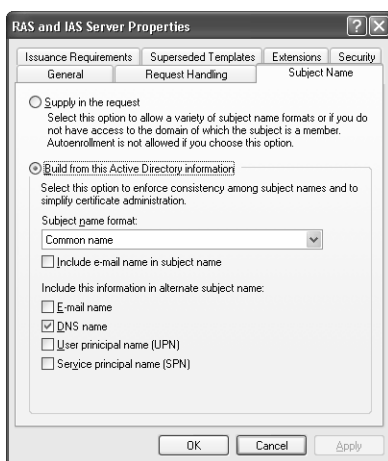
- **Prompt the User During Enrollment.** The user is notified that a certificate is available for autoenrollment. This option is typically enabled if a user action is required, such as selecting a certificate to sign the enrollment request or inserting a smart card in the smart card reader.
- **Prompt the User During Enrollment and Require User Input When the Private Key is Used.** Enables strong private key protection requiring that a user provide a password to access the private key material every time the private key is used.
- **CSPs.** Allows you to define what cryptographic service providers (CSPs) can be used when requesting a certificate based on the certificate template. You can choose to allow requests to use any CSP on the subject's computer or designate a specific CSP for the certificate template.



**Note** If you use a third-party CSP, you must install the CSP at the computer where you define the certificate template and at the computer(s) where enrollment occurs.

## The Subject Name Tab

The Subject Name tab defines what information is provided in the certificate request to build the issued certificate's subject name. (See Figure 8-5.) You must allow the subject information to be supplied in the certificate request or use information stored in the subject's Active Directory object when building the certificate request.



**Figure 8-5** Modifying the Subject Name tab for a version 2 certificate template

- Supply in Request.** This option is commonly used when a certificate template is intended for users or computers that are not part of the forest—meaning that a user or computer account does not exist in Active Directory. It is also used if the certificate request is generated programmatically by using the XEnroll.dll Microsoft ActiveX control or if the certificate template allows a requesting user to provide a name other than his or her own for the subject of the certificate. For example, a user requesting a Code Signing certificate might want to put the organization's name as the subject of the certificate rather than his or her personal name.



**Note** You cannot enable the option to supply the subject name in the request if you are using the Certificate Services Enrollment Wizard in the Certificate MMC console or autoenrollment. These enrollment methods require that the subject name be built from Active Directory information.

- **Build from this Active Directory Information.** If you choose to build the subject name from Active Directory information, you can choose which name formats from the requestor's Active Directory object are used in the subject name formation. Available options are:

- **Subject Name Format.** The subject name can contain either the object's common name or the object's fully distinguished name (the LDAP distinguished name) in Active Directory. You can also choose to implement no value in the subject name.



**Note** If you choose to implement no value in the subject name, you *must* include at least one alternate subject name format.

- **Include E-Mail Name in Subject Name.** Includes the e-mail name in the subject name. The e-mail name is added to the front of the subject name, with a qualifier of *E=e-mail name*.
- **E-mail Name.** Includes the user's e-mail name in the certificate's subject alternative name extension.



**Warning** If the user object does not have an e-mail name defined, and the certificate template requires one, the certificate request will fail. You must ensure that all required name formats are included in the requestor's Active Directory object attributes.

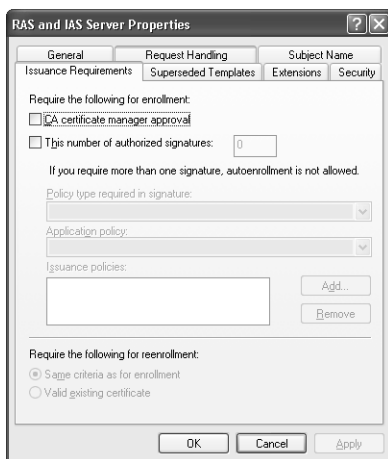
- **DNS Name.** Includes the computer's fully qualified Domain Name System (DNS) name in the certificate's subject alternative name extension.
- **User Principal Name (UPN).** Includes the user's UPN in the certificate's subject alternative name extension.
- **Service Principal Name (SPN).** Includes the computer's SPN in the certificate's subject alternative name extension.



**Note** If you enable any of the alternative subject name options, you must ensure that all users or computers that request the certificate have those fields populated in Active Directory. For example, if a user requests a certificate that places the user's e-mail name in the subject alternative name extension, and the user does not have a defined e-mail name, the certificate request will fail.

## The Issuance Requirement Tab

The Issuance Requirements tab allows you to define additional requirements to ensure the measures for validating a certificate requestor's identity. The tab also allows you to designate the measures required for re-enrollment. (See Figure 8-6.)



**Figure 8-6** Modifying the Issuance Requirements tab for a version 2 certificate template

The following options are available on the Issuance Requirements tab:

- **CA Certificate Manager Approval.** Places a certificate request in a pending state until a certificate manager issues or denies the request. This option allows the certificate manager to perform any (manual) identification validation (that is defined by an organization's certificate policy) to determine whether the certificate should be issued.
- **This Number of Authorized Signatures.** Defines how many digital signatures must be applied to the certificate request for approval. Once you define how many signatures are required, you also must define which application policy or issuance policy object identifiers (OIDs) are required in the signing certificate.
  - **Policy Type Required in Signature.** Defines whether a specific application policy OID, a specific issuance policy OID, or both are required.



**Note** Issuance policies are also known as certificate policies.

- **Application Policy.** Defines the specific application policy OID required in the signing certificate if an application policy is designated in the required signing certificate.

- **Issuance Policy.** Defines one or more issuance policy OIDs accepted in the signing certificate if an issuance policy is designated in the required signing certificate.

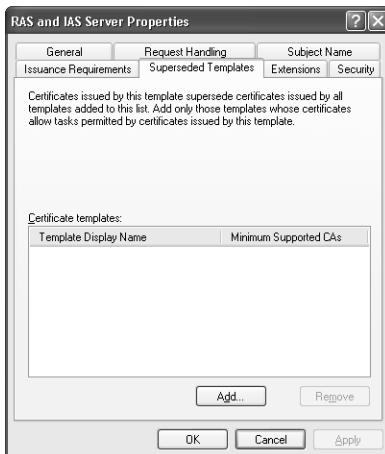


**Important** If you define complex signature requirements, such as requiring two or more signatures on a certificate request, you will have to create a custom workflow process, such as a custom Web enrollment page, that will implement and enforce the required workflow to allow multiple signatures to be applied to the certificate request.

- **Require the Following for Reenrollment.** Allows you to designate whether the same identity validation procedures must be used for re-enrollment. You can choose to implement the same validation procedures or simply allow re-enrollment if the user holds a valid existing certificate. For example, when your organization initially distributes smart cards to employees, it might require face-to-face interviews. Rather than have the employees participate in another face-to-face interview when the smart card certificate comes up for renewal, employees can renew their certificate by proving that they have an existing certificate. This reduces the procedural overhead for certificate renewal.

## The Superseded Templates Tab

The Superseded Templates tab allows you to define updated certificate templates for previously defined version 1 or version 2 certificate templates. (See Figure 8-7.)



**Figure 8-7** Modifying the Superseded Templates tab for a version 2 certificate template



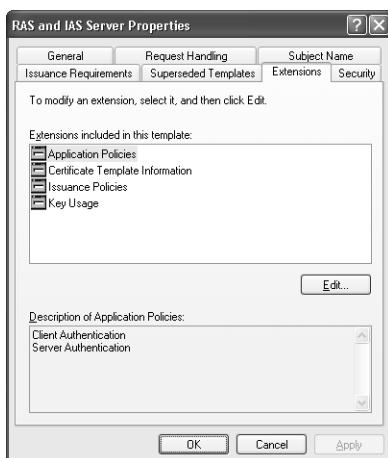
By adding one or more certificate templates to the Superseded Templates tab, you can replace the existing certificate template(s) with an updated version 2 template. The updated template is automatically deployed by using certificate autoenrollment.



**Note** When a certificate template is superseded, the original certificate is not removed from the user's certificate store. Instead, the certificate is marked as archived, and suppressed from view in the Certificates console.

## The Extensions Tab

The Extensions tab allows you to define specific X.509 version 3 certificate extension settings. (See Figure 8-8.)



**Figure 8-8** Modifying the Extensions tab for a version 2 certificate template

The following certificate extensions can be defined:

- Application Policies.** Define the specific applications for which a certificate can be used. Application policies are represented in a certificate by an OID that is defined for a given application. When the certificate is required, an application filters the available certificates to only include those with the necessary application policy OID.



**Note** The OIDs in the application policies extension are also duplicated in the enhanced key usage (EKU) extension for older applications that do not recognize the application policies extension. The only difference is that you can enable the criticality flag for the application policy extension but not for the EKU.

- **Certificate Template Information.** Defines the display name of the certificate template, the automatically assigned OID for the certificate template, and the subject type. The available subject types are:
  - Key recovery agent
  - Directory e-mail replication
  - Cross-certified certification authority
  - Certification authority (CA)
  - Computer
  - User



**Note** You cannot edit certificate template information. You must ensure that the certificate template you duplicate has the required subject type.

- **Issuance Policies.** Also known as certificate policies, issuance policies define the measures taken to validate a certificate's subject. An OID is placed in the issuance policy extension, representing the implemented certificate policy, as is a URL that provides more information regarding the certificate policy.
- **Key Usage.** A certificate attribute that can further restrict how a certificate can be used. This allows the administrator to define a certificate's specific signing or encryption purposes:
  - For signing certificates, you can further restrict certificates for digital signatures, signature is a proof of origin (non-repudiation), certificate signing, or CRL signing.
  - For encryption certificates, you can restrict certificates for key exchange without key encryption or key exchange with key encryption only.

## Best Practices for Certificate Template Design

When designing certificate templates, the following best practices should be employed:

- Determine whether a default version 1 or version 2 certificate template meets your business goals. A default template does not require any modifications other than permission assignments.
- If you need to change settings in a certificate template other than permissions, duplicate a template that is closest to the required template. This minimizes the number of changes required.

- If you replace an existing certificate template with an updated template, ensure that you add the previous template to the Superseded Templates tab.
- To enroll a certificate, a user or computer must be assigned Read and Enroll permissions, either directly or through group membership.
- To enroll a certificate with autoenrollment, a user or computer must be assigned Read, Enroll, and Autoenroll permissions.
- To modify a certificate template, a user must be assigned Write permissions.
- Determine whether you should deploy fewer certificates with multiple purposes or many certificates with specific purposes. The decision is based on the purposes you require and whether you foresee removing a purpose from a certificate holder.

## Case Study: Certificate Template Design

You are responsible for designing certificate templates for your organization. The software development department has created several custom applications that require digital signing prior to network deployment. Digital signatures are required to meet the company's security policy regarding custom application security.

### Requirements

To meet the security policy, the manager of the security department has provided you with the following requirements:

- The code signing certificate must be stored on a Gemplus GemSAFE 8KB smart card.
- Only members of the Code Signing group can request a code signing certificate.
- All initial code signing certificate requests are subject to the approval of the company's notary public.
- If you already have a code signing certificate, you can re-enroll without having to meet with the notary public again.
- The code signing certificate must be valid for four years.
- The code signing certificate must have a key length of 1,024 bits.

### Case Study Questions

1. What MMC console do you use to perform certificate template management?
2. Does the default Code Signing certificate template meet the design requirements?

3. Can you modify the default Code Signing certificate template? If not, what would you do?
4. In the table that follows, define the settings on the General tab to meet the design requirements for your custom code signing certificate template:

Attribute	Your recommended design
Template Display Name	
Template Name	
Validity Period	
Publish Certificate in Active Directory	
Do Not Automatically Re-Enroll if a Duplicate Certificate Exists in Active Directory	

5. In the table that follows, define the settings on the Request Handling tab to meet the design requirements for the custom code signing certificate template:

Attribute	Your recommended design
Purpose	
Allow Private Key to be Exported	
Minimum Key Size	
Do the Following When the Subject Is Enrolled and When the Private Key Associated with this Certificate Is Used	
CSPs	

6. In the table that follows, define the settings on the Issuance Requirements tab to meet the design requirements for the custom code signing certificate template:

Attribute	Your recommended design
CA Certificate Manager Approval	
This Number of Authorized Signatures	
Require the Following for Re-Enrollment	

7. How should you configure the settings on the Superseded Templates tab to ensure that all certificates a CA issues for code signing use the version 2 certificate template?
8. What permission assignment modifications are required for the custom code signing certificate?

## Additional Information

- Microsoft Official Curriculum, Course 2821: “Designing and Managing a Windows Public Key Infrastructure” ([www.microsoft.com/traincert/syllabi/2821afinal.asp](http://www.microsoft.com/traincert/syllabi/2821afinal.asp)).
- “Implementing and Administering Certificate Templates in Windows Server 2003” ([www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03crtm.mspix](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03crtm.mspix)).
- “PKI Enhancements in Windows XP Professional and Windows Server 2003” ([www.microsoft.com/technet/prodtechnol/winxp/pro/plan/pkienb.mspix](http://www.microsoft.com/technet/prodtechnol/winxp/pro/plan/pkienb.mspix)).
- Windows Server 2003 Resource Kit tools (<http://www.microsoft.com/downloads/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cffd&displaylang=en>).
- Knowledge Base Article 264589: “Duplicate Certificate Templates Appear in Active Directory”
- Knowledge Base Article 278257: “Requests for Certificates from an Enterprise Certificate Authority Are Unsuccessful”
- Knowledge Base Article 281260: “A Certificate Request That Uses a New Template Is Unsuccessful”
- Knowledge Base Article 330238: “Users Cannot Enroll for a Certificate When the Include E-mail Name in Subject Name Option Is Selected on the Template”



**Note** Microsoft Knowledge Base articles can be found at <http://support.microsoft.com>. Enter the article number in the Search the Knowledge Base text box.



## Chapter 9

# Certificate Validation

Certificate validation ensures that the certificate's information is authentic, that the certificate can be used only for its intended purposes, and that the certificate is trusted.

If certificate revocation list (CRL) checking is enabled in an application, the Microsoft Windows operating system automatically performs certificate validation and repeats the validation for each certificate in a certificate chain until it reaches the root certification authority (CA). The certificate chaining engine within the Windows operating system performs the validation testing.



**More Info** For more information on CRL checking and certificate validation, see the “Troubleshooting Certificate Status and Revocation” white paper listed in the “Additional Information” section of this chapter.

## Certificate Validation Process

When a certificate is presented to an application, the application must use the certificate chaining engine to determine the certificate's validity. The certificate chain must be successfully validated before the application can trust the certificate and the identity represented by the certificate to encrypt data or verify a digital signature. Three distinct but interrelated processes are used to determine a certificate's validity.

- **Certificate discovery.** To build certificate chains, the certificate chaining engine must collect the issuing CA certificate and all CA certificates up to the root CA certificate. CA certificates are collected from the CryptoAPI cache, Group Policy, or Enterprise Policy, or, as a last resort, downloaded from Authority Information Access (AIA) URLs in issued certificates. Once a certificate is downloaded from a location other than the CryptoAPI cache, it is added to the user's CryptoAPI cache for faster retrieval.
- **Path validation.** When the certificate chaining engine validates a certificate, it does not stop at the presented certificate. Each certificate in the certificate chain must be validated until a self-signed root certificate is reached. Validation tests can include verifying Authenticode signatures, determining whether the

issuing CA certificate is included in the NTAAuth store, or checking for specific application or certificate policy object identifiers (OIDs). If one certificate fails a validity test, it is possible that the entire chain will be deemed invalid and not used by the calling application.

- **Revocation checking.** Once the certificate chain is built, the certificate chaining engine checks the revocation status of each certificate in the chain. When running Windows XP or Windows Server 2003, the chaining engine checks revocation as the chain is built. By contrast, Windows 2000 and earlier operating systems do not perform revocation checking until the chain is assembled.

## Certificate Validity Checks

When a certificate is presented to an application, the certificate chaining engine tests the following components:

- **Certificate contents.** A certificate must have information in all required X.509 standard fields. If a required field is missing or populated incorrectly, the certificate is considered invalid.



**Note** The certificate chaining engine excludes all invalid certificates found during the certificate discovery process. Invalid certificates are used by the certificate chaining engine when building certificate chains.

- **Certificate format.** A certificate must conform to a valid X.509 standard for digital certificates. The certificate chaining engine rejects a certificate that does not follow X.509 version 1, version 2, or version 3 formats.
- **Critical extensions.** If the certificate contains any X.09 version 3 certificate extensions that are marked as critical, the chaining engine will identify the critical extensions to the calling application. If the calling application does not understand the critical extension, the application will consider the certificate to be invalid.
- **Policy validation.** If the application that calls the certificate chaining engine expects a specific application policy or certificate OIDs in the certificate, and the required policy or OIDs are not contained within the certificates in the CA chain, the certificate chaining engine considers the certificate to be invalid.
- **Revocation check.** The certificate chaining engine calls any installed revocation providers to ensure that the certificate's serial number is not in the issuing CA's CRL. If the certificate is in the CRL listing, the certificate is considered to be invalid. This revocation check is performed for each certificate in the certificate chain below the root CA certificate.



- **Root check.** The certificate chain assembled by the certificate chaining engine must chain to a trusted root CA or be included in a certificate trust list (CTL) manually configured by the organization or downloaded from Windows Update. If the chain terminates at a nontrusted root CA or does not chain to a self-signed root CA certificate, the presented certificate is considered to be invalid.
- **Signature check.** When a CA issues a certificate, the CA's private key digitally signs the issued certificate's contents. If the contents are modified or corrupted, the digital signature validation fails, resulting in an invalid certificate.
- **Time validity.** The current date and time must fall within the presented certificate's validity period. If it doesn't, the certificate chaining engine considers the certificate to be invalid.

## Certificate Revocation

Certificate revocation is necessary when you must terminate a certificate's usage before the validity period expires. When a certificate is revoked, a certificate manager must select the certificate to revoke in the Certification Authority console and provide a reason for revocation. The serial number of the certificate is then stored in the CA's database with a reason code specifying why the certificate was revoked; it can then be used to publish a CRL, etc.

### Types of CRLs

The Windows Server 2003 public key infrastructure (PKI) supports two different but related types of CRLs: base CRLs and delta CRLs.

A *base CRL* contains the serial numbers of certificates revoked by the CA that are signed with the CA's private key. If you renew a CA's certificate with a new key pair, the Windows Server 2003 CA maintains two separate CRLs—one for each key pair maintained by the CA. Base CRLs are recognized by all versions of the Windows operating system.

A *delta CRL* contains only the serial numbers of certificates revoked by the CA since the last base CRL publication. Again, if the CA's certificate is renewed with a new key pair, separate delta CRLs are maintained for each CA key pair. Delta CRLs allow you to publish revocation information more quickly and allow smaller updates to be downloaded by client computers.



**Caution** Delta CRLs are only supported by Windows XP and Windows Server 2003 operating systems. Older operating systems will ignore the delta CRL and determine revocation information by inspecting the base CRL. Support for delta CRLs is expected in the Windows 2000 Service Pack 5.

## CRL Retrieval Process

When a client computer checks the revocation status of a certificate, it first checks for the desired base CRL or delta CRL in the CryptoAPI cache. If the base CRL or delta CRL is found, the CRL is checked to determine whether the CRL is time-valid. Like certificates, a CRL has a validity period defined by the CRL publication interval. If a time-valid CRL is found in the CryptoAPI cache, that version of the CRL is used for revocation checking, even if an updated version has been published manually. The cached CRL is used to prevent excess network traffic. Use of a cached CRL also follows the recommendations in RFC 3280 to acquire an updated CRL only when the previous CRL expires.



**Warning** Microsoft does not support designs that manually delete the cached version of a CRL from the CryptoAPI cache.



**More Info** The process described here follows the definition of CRL usage in RFC 3280, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” listed in the “Additional Information” section of this chapter.

## Revocation Reasons

The following revocation reasons are available for CRLs:

- **AffiliationChanged.** An individual is terminated, resigns, or dies. This revocation reason also can be used if a person changes roles within an organization and no longer requires use of the certificate associated with the previous role.
- **CACompromise.** You suspect that a CA’s private key is compromised and in the possession of an unauthorized individual. If a CA’s private key is revoked, all certificates below that CA in the CA hierarchy are considered revoked.
- **CertificateHold.** A temporary revocation that indicates a CA will not validate a certificate at that specific time.



**Tip** Although CertificateHold allows a certificate to be unrevoked, use of the CertificateHold reason code is not recommended, as it becomes difficult to determine whether a certificate was valid at a specific time.

- **CessationOfOperation.** A CA is decommissioned and all certificates issued by the CA are no longer in use.



**Tip** You cannot decommission a CA if any of the certificates issued by the CA are in use. Even if you do not plan to issue any additional certificates, the CA must still publish CRL information at regular intervals for revocation checking purposes.

- **KeyCompromise.** You suspect that the private key associated with a certificate is compromised. For example, if a laptop belonging to a user in your organization is stolen, it is possible that any private keys stored on the laptop are compromised.
- **RemoveFromCRL.** Unrevokes a certificate revoked using `CertificateHold`. The unrevoking process still lists the certificate in the CRL, but the certificate also appears in a delta CRL with the revocation code set to `RemoveFromCRL`. When the next base CRL is published, the CA removes the certificate from all forms of the CRL.
- **Superseded.** A new certificate must be issued if a user's certificate is replaced for any reason with a new updated certificate. For example, if you update a certificate template and reissue certificates, you can revoke the previous certificate with this reason code.
- **Unspecified.** You can revoke a certificate without providing a specific revocation code. Using `Unspecified` is not recommended, however, as it does not provide an audit trail identifying why a certificate was revoked.

## Revoking a Certificate

To revoke a certificate, a user must be designated as a certificate manager by assigning the user or a group the user is a member of the Issue and Manage Certificates permission at the issuing CA. The permission assignment is performed by a CA Administrator or a user assigned the Manage CA permissions. You can use the following process to verify the permission assignment:

1. Log on to the CA computer.
2. From Administrative Tools, open the Certification Authority console.
3. In the console tree, right-click *CAName* (where *CAName* is the logical name of the CA) and click Properties.
4. In the *CAName* Properties dialog box, select the Security tab to ensure that the user account or a group that the user is a member of is assigned the Issue and Manage Certificates permission.



**Note** If you want to assign a new user or security group the certificate manager role to allow them to revoke certificates, assign the user or security group the Issue and Manage Certificates permission.

Once you assign the necessary permissions, the following procedure revokes a certificate:

1. From Administrative Tools, open the Certification Authority console.
2. In the console tree, expand *CAName* and click Issued Certificates.
3. In the details pane, find the certificate that you need to revoke, right-click the certificate, point to All Tasks, and click Revoke Certificate.
4. In the Certificate Revocation dialog box, in the Reason Code drop-down list, select the appropriate reason code and click Yes.

## Building Certificate Chains

The certificate chaining engine builds chains by inspecting specific extensions in a presented certificate. There are different processes the certificate chaining engine uses to determine the issuing CA's correct certificate. The actual selection is based on the current certificate's attributes. Specifically, the certificate chaining engine examines a combination of the following certificate fields and X.509 version 3 certificate extensions:

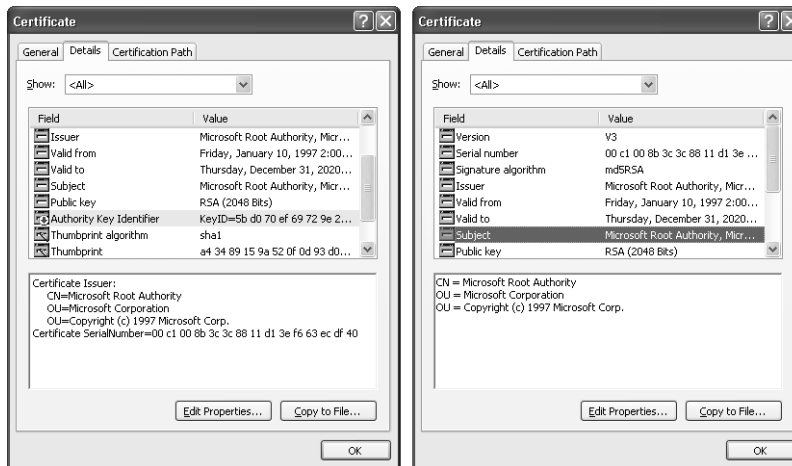
- **Authority Key Identifier (AKI) extension.** The matching method the certificate chaining engine performs is based on the contents of the AKI extension. When using the Windows Server 2003 PKI, the AKI extension can contain:
  - The subject and serial number of the issuing CA's certificate.
  - The hash of the issuing CA's public key.
  - Nothing, or is not present in the evaluated certificate.
- **The Issuer field.** If an AKI extension is not present, the certificate chaining engine determines the issuing CA's name from the evaluated certificate's Issuer field.

- **The Subject of the issuing CA certificate.** The subject is used to identify the issuing CA certificate. If the AKI contains the subject and the serial number of the issuing CA certificate, the CA certificate with the same serial number and subject is selected.
- **The Serial Number field of the issuing CA certificate.** If the AKI contains the subject and the serial number of the issuing CA certificate, the CA certificate with the same serial number and subject is selected.
- **The Subject Key Identifier (SKI) extension of the issuing CA certificate.** If the AKI contains the hash of the issuing CA's public key, the CA certificate's SKI contains a matching hash value.

These fields and extensions are used by the certificate chaining engine to build certificate chains. Based on the contents of the evaluated certificate's AIA extension, the chaining engine builds the certificate chain using an exact match, key match, or name match.

## Exact Match

In the event that an evaluated certificate contains the issuing CA's subject name and serial number, the certificate chaining engine uses an exact match (also known as a key and name match), to find the issuing CA's certificate. The chaining engine searches for a CA certificate with the subject name and the serial number defined in the evaluated certificate's AKI extension. (See Figure 9-1.)



**Figure 9-1** An exact match

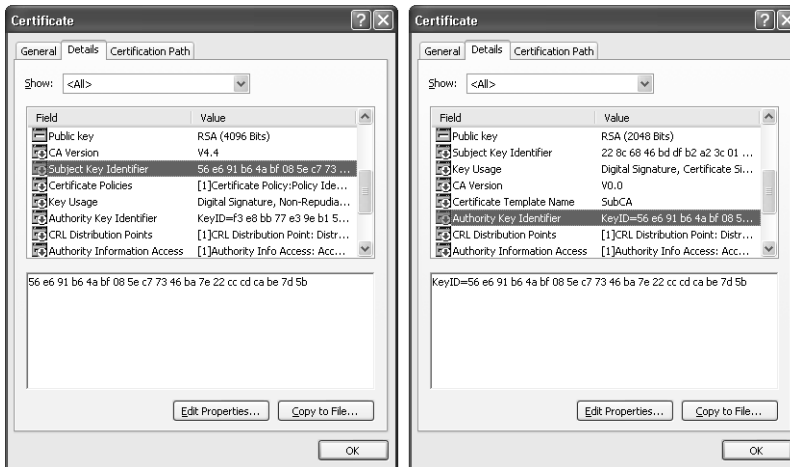
The left certificate's AKI extension contains the subject and serial number of the issuing CA's certificate. Note that the certificate on the right has a matching serial number and subject name.



**Note** A single match can happen only in the case of an exact match. Anytime you renew a CA's certificate, the new certificate has a different serial number.

## Key Match

If an evaluated certificate's AKI extension contains only the hash of the issuing CA's public key, the certificate chaining engine searches for CA certificates that have a matching value in each CA certificate's SKI extension. (See Figure 9-2.)



**Figure 9-2** A key match

In the certificate on the right, the AKI extension contains the hash of the issuing CA's public key. In the issuing CA certificate on the left, the same public key hash exists in the SKI extension. For the match to be successful, the two hashes must be calculated using the same hash algorithm. Even if the issuing CA certificate does not have an SKI extension, a key match is still possible if the hash algorithm used to calculate the hash of the public key is SHA-1, the default hash algorithm used by the Microsoft CA and CryptoAPI. If other hash algorithms are used, the resulting hash of the public key must exist in both the evaluated certificate's AKI extension and the CA certificate's SKI extension.



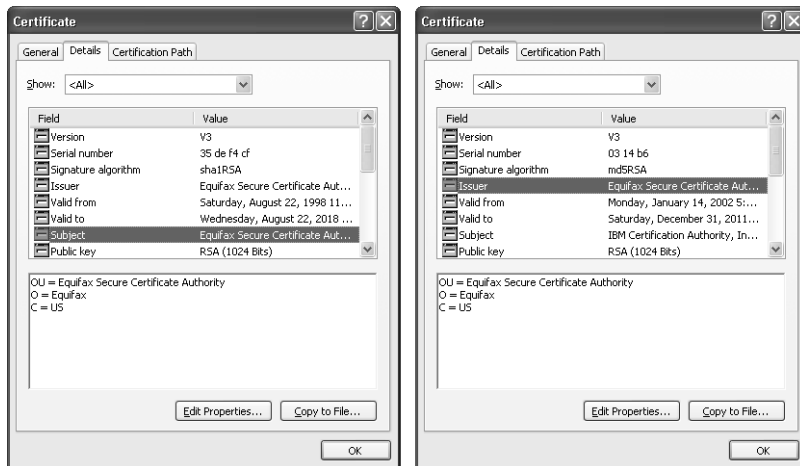
**Note** There can be multiple matches when key matching is used to build a certificate chain. This scenario, known as ambiguous chaining, occurs when the CA certificate is renewed with the same key pair. Both versions of the CA certificate contain the same value in the SKI extension.

## Name Match

If no information exists in the AKI, or if the AKI does not exist in the evaluated certificate, the certificate chaining engine uses a name match to find the issuing CA's certificate. To perform name matching, the certificate chaining engine matches the contents of the evaluated certificate's Issuer field to the Subject field of the issuing CA's certificate. (See Figure 9-3.)



**Note** The name matching process is case sensitive.



**Figure 9-3** A name match

The right certificate's Issuer field contains the same subject name as the left certificate's Subject field.



**Note** Multiple matches are possible when name matching is used to build a certificate chain. This scenario occurs when the CA certificate is renewed with either the same key pair or a new key pair. When the CA certificate is renewed, the Subject of the CA certificate does not change.

## Designing PKI Object Publication

To enable certificate validation, you must ensure that a CA's certificate and CRL are available for download by the certificate chaining engine. This is done by confirming that the certificate and CRL are available by using the desired protocols from the desired locations and are published at the required intervals.

### Choosing Publication Protocols

Determining the protocols used for CA certificate and CRL retrieval is the first step in choosing publication points. The following protocols are available with Windows Server 2003 PKI:

- **HTTP.** The Hypertext Transfer Protocol (HTTP) provides the most flexibility. Almost all client computers have a Web browser installed that allows access to HTTP URLs. The HTTP protocol is also useful when computers that are not members of the forest require access to the CA certificate or CRL. The CA certificate and CRL also can be published to a Web cluster to provide redundancy and high availability.



**Note** There should be no need to implement Secure Sockets Layer (SSL) protection for the Web server hosting the CA certificate or CRL publication points. The CA certificates and CRLs are digitally signed objects that do not require transport level security to provide data integrity. In addition, the use of SSL can cause recursion of revocation checks. To download the updated version of the CRL, you must check the CRL to ensure that the certificate that signed the CRL is valid.

- **LDAP.** The Lightweight Directory Access Protocol (LDAP) provides high availability by publishing the CA certificate and CRL to the Microsoft Active Directory Configuration naming context. LDAP URLs can be accessed by any forest members that can resolve them. This includes Windows 2000 and later and Windows 98, Windows Me, and Windows NT 4.0 computers with the Directory Services Client installed.





**Note** If an explicit X.500 distinguished name is used in the LDAP URL, Active Directory must contain an explicit referral to the object.



**Note** LDAP URLs can be accessed by operating systems other than Windows if the LDAP URL is modified to include the DNS name of the LDAP server in the LDAP URL. For example, rather than publishing the CDP URL as LDAP:///CN=CAName,CN=CAComputer,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,ForestRootDomain, you would publish the CDP URL as LDAP://Webserver/CN=CAName,CN=CAComputer,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,ForestRootDomain. In addition, if published in Active Directory, the permissions of the CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,ForestRootDomain container must be modified to allow anonymous access.

- **FTP.** The File Transfer Protocol (FTP) provides access to FTP clients for the download of CA certificates and CRLs. Although not typically used, FTP URLs are supported by Microsoft clients with the TCP/IP protocol stack.
- **File.** The file protocol provides access to file shares using the Common Internet File System (CIFS) or Server Message Blocks (SMBs). Although not commonly used for CA certificate and CRL retrieval, the file protocol is sometimes used to publish CA certificates and CRLs to remote file locations.

You can implement more than one publication protocol. When you define the publication points, the order in which they appear on the CA's Extensions tab is the order in which the client computers search the URLs.

## Choosing Publication Points

Once you choose the publication protocols, you must choose *where* to publish the CA certificates and CRLs. The location decision includes the physical servers where you publish the files and the servers on the corporate network: intranet or extranet.

Choose publication points according to the following rules:

- If most computers are running Windows 2000 or later and are members of the forest, you should include an LDAP URL that references the Active Directory Configuration naming context. This location is published to all domain controllers in the forest and ensures availability and fault tolerance.

- If you have several nonforest computers or third-party operating systems, such as UNIX, you should include Web server publication points for HTTP URLs.
- If certificates are to be evaluated from the external network, the CA certificate and CDP must be published to an externally accessible location, such as a Web server or LDAP server in the demilitarized zone (DMZ) of the network.
- File publication points typically are not used for CA certificate and CRL retrieval. File publication points are more common for publishing CA certificate and CRL information to remote servers.
- The URL order is determined by the type of network clients. The order should be set so that the majority of clients can retrieve the CA certificate or CRL from the first URL in the listing. If a client cannot retrieve the CA certificate or CRL from the first URL, the client times out in an attempt to connect, and then proceeds through the next URLs in the listing.



**Note** The URL order is not important to all operating systems. Some UNIX systems use their own methods to determine what order URLs are fetched when multiple URLs exist in the CDP extension.

- Delta CRLs are published more frequently than base CRLs. You can consider not publishing delta CRLs to LDAP locations because of Active Directory replication latency. Instead, publish delta CRLs to HTTP locations. The Active Directory replication interval must be more frequent than the delta CRL validity period.

## URL Ordering Issues

---

When you implement multiple URLs in a CDP extension, the order of the URLs is important. If you do not choose the correct order, a client will spend a specific amount of time attempting to connect to each URL in the listing before attempting to use the next URL in the listing. The default behavior for a Windows client is:

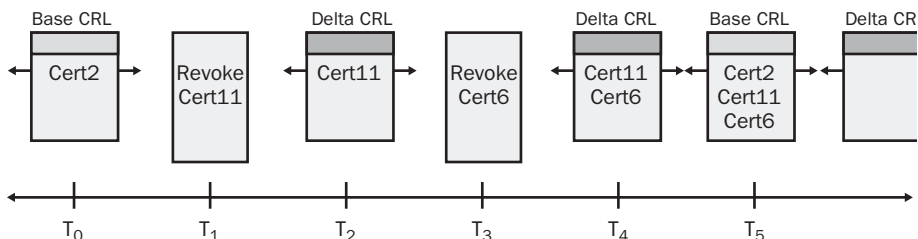
- The maximum timeout for all CRL retrievals is 20 seconds. If a download did start, it will continue after the 20-second interval, perhaps resulting in a success the next time a connection is attempted.

- The first CDP location is given a maximum of 10 seconds to succeed. If the CRL cannot be downloaded in the 10-second interval, the certificate chaining engine will proceed to the next URL in the listing. You should ensure that the first URL listed can be accessed by the greatest number of computers. For example, if several computers are not members of the forest, or use another operating system, such as UNIX, consider moving the default first entry of `LDAP:///CN=CAName,CN=CAComputer,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=ForestRootDomain` to a lower placement in the URL listing.
- Subsequent CDP locations will each use a maximum of one-half of the remaining time to retrieve a specific CRL object before continuing to the next location.
- Each location download is attempted in sequential order. If CryptoAPI is unable to retrieve a CRL for any reason during the allotted maximum timeout interval, such as invalid path, access denied, etc., an error of “revocation offline” will be returned to the application.

Careful planning of the publication locations will prevent timeout errors from affecting certificate revocation status checking.

## Choosing Publication Intervals

When you configure a CA, one of the design decisions is how frequently to publish the base CRL and the delta CRL. Before discussing these decision points, it is useful to review the interaction of base and delta CRLs. (See Figure 9-4.)



**Figure 9-4** Base and delta CRL publication

1. In Figure 9-4, the initial base CRL is published at time  $T_0$  and includes one revoked certificate, Cert2.
2. At time  $T_1$ , Cert11 is revoked with a revocation reason of AffiliationChanged.

3. At time T2, when the delta CRL is published, the delta CRL contains only one entry, Cert11.
4. At time T3, Cert6 is revoked with a revocation reason of Superseded.
5. At time T4, when the next version of the delta CRL is published, the delta CRL contains both Cert6 and Cert11.
6. At time T5, when the next version of the base CRL is published, the base CRL contains three certificates: Cert2, Cert6, and Cert11. In addition, an empty delta CRL is published with no entries in the delta CRL.

Publication intervals should be based on the answers to the following questions:

- **What is the maximum period your organization is willing to accept a revoked certificate as valid?** If you use the default publication intervals, the base CRL is published weekly and the delta CRL is published daily. You must redefine these publication intervals to meet your organization's acceptable risk level.
- **What operating systems run on your organization's network?** If your client computers run Windows 2000 or earlier versions, you must define shorter CRL publication intervals so that computers have up-to-date information. Only Windows XP and Windows Server 2003 operating systems support delta CRLs. If you run another operating system, such as UNIX, you must verify whether this operating system supports delta CRLs.



**Note** Windows 2000 Service Pack 5 is expected to add delta CRL recognition to all Windows 2000 client computers.

- **What is the network traffic associated with CRL retrieval?** The more frequently you publish the base CRL, the more often clients download the base CRL, which increases the network traffic associated with CRL retrieval.
- **How large is the delta CRL?** Publishing several delta CRLs between each base CRL publication can result in a larger delta CRL. The goal of a delta CRL is to reduce the size of downloaded CRLs, in addition to making more frequent updates. In the case of a larger delta CRL, consider reducing the publication interval for base CRLs or publishing delta CRLs less frequently.
- **How often are certificates revoked?** The number of certificates revoked within a period greatly influences the publication interval for both base and delta CRLs. You must define publication intervals so that revoked certificates are recognized as soon as possible. You must balance the interval against the network load resulting from CRL-download traffic.

- **What is the Active Directory replication latency on your network?** The delta CRL and base CRL publication intervals are limited by the replication latency of Active Directory. Because the replication latency can be eight hours or longer in some cases, defining CRL publication to an interval of less than eight hours can result in the CRL being unavailable until Active Directory replication is completed. Replication latency results in the failure of the path-validation process due to the inability to download an updated CRL.
- **What is the expected time to recover from a disaster?** If Certificate Services fails, you must rebuild the CA and restore the CA database and registry settings before the previous CRL expires. If the CRL publication interval is shorter than the amount of time required to recover a failed CA, certificates issued by the CA will fail revocation checking due to the inability to download an updated CRL.

## Troubleshooting Publication Points

The misconfiguration of CA certificate and CRL publication points is the most common error in a PKI. If the publication points are referenced incorrectly, certificate validation errors, CA failures, issuance failures, logon failures, and so on can result.



**Note** If the certificate chaining engine cannot find an updated CRL as referenced in the CDP extension of a certificate, the chaining engine invalidates the certificate with a revocation status: “Cannot determine the revocation status of the certificate.” Most applications consider this revocation status (also known as the revocation unknown status code) to be the equivalent of a revoked certificate when strong CRL checking is enabled because it is safer to reject the certificate than to accept a revoked certificate.

To prevent publication errors from occurring on your network, you should use tools to ensure that the publication points are configured correctly. The following tools are available for validating the AIA and CDP URLs:

- Certutil
- PKI Health Tool
- CryptoAPI Monitor (CAPIMON)

## Certutil

Certutil.exe, a utility in the Windows Server 2003 Administration Pack (adminpak.msi), allows a PKI administrator to manage a PKI from the command line. One of the abilities of certutil.exe is to verify certificate chaining and CRL retrieval. By using the command `certutil -verify -urlfetch CertificateFileName`, you can verify the ability to retrieve CA certificates and CRLs for the entire certificate chain of the *CertificateFileName* file.

For example, if you were to verify the certificate `brian.cer` by typing **certutil -verify -urlfetch brian.cer**, the output would fetch each CDP and AIA URL in the certificate and report on the status of the URL. A validated LDAP URL for a base CRL appears like this:

```
Verified "Base CRL (36)" Time: 0
[1.0] ldap:///CN=Fabrikam%20Issuing%20CA,CN=IssuingCA,
CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,
DC=fabrikam,DC=com?certificateRevocationList?base?objectClass=
cRLDistributionPoint
```

Likewise, a validated HTTP URL for a base CRL appears like this:

```
Verified "Base CRL (36)" Time: 0
[0.0] http://www.fabrikam.com/CertData/Fabrikam%20Issuing%20CA.crl
```

The output reports on every URL in every certificate in the certificate chain, from the examined certificate to the certificate chain's root CA. If certutil is unable to connect to one of the referenced URLs, the output indicates the following:

```
Failed "CDP" Time: 0
Error retrieving URL: Error 0x800701f6 (WIN32: 502)
http://www.fabrikam.com/CertEnroll/Fabrikam%20Issuing%20CA.crl
```

If any errors are encountered by certutil, the final lines of the output reports that revocation checking failed, as shown here:

```
ERROR: Verifying leaf certificate revocation status returned. The revocation
function was unable to check revocation because the revocation server was offline.
0x80092013 (-2146885613)
CertUtil: The revocation function was unable to check revocation because the
revocation server was offline.
```

## PKI Health Tool

The Windows Server 2003 Resource Kit includes the PKI Health Tool (pkiview.msc), a retrieval tool for URLs in both the CDP and AIA extensions of all certificates in the certificate chain. The PKI Health Tool reports on the status of each URL configured in the CA hierarchy using status codes of OK, Expired, and Unable to download.

To use the PKI Health Tool, you must initialize the associated dynamic link library (DLL) with the following procedure:

1. Open a command prompt.
2. In the command prompt, type **regsvr32 pkiview.dll** and press ENTER.
3. In the Regsvr32 dialog box, click OK.



**Note** If you install the Windows Server 2003 Resource Kit Tools, the PKI Health Tool and associated pkiview.dll files are automatically installed and registered. Use this procedure if you only want to install the PKI Health Tool, not the entire resource kit.

Once the DLL is registered, you can open the PKI Health Tool by running `pkiview.msc`. (See Figure 9-5.)



**Figure 9-5** The PKI Health Tool console

Within the PKI Health Tool console, you can view the status for each AIA and CDP URL. The status codes will include:

- **OK.** The CA certificate or CRL at the referenced URL is valid.
- **Expiring.** The CA certificate or CRL at the referenced URL is near expiration.



**Note** You can define the expiration interval for CA certificates, CRLs, and delta CRLs within the PKI Health Tool to match the publication intervals used by your organization. For example, if you publish base CRLs every day, you could define the expiration warning interval to be eight hours before expiration rather than the default of two days.

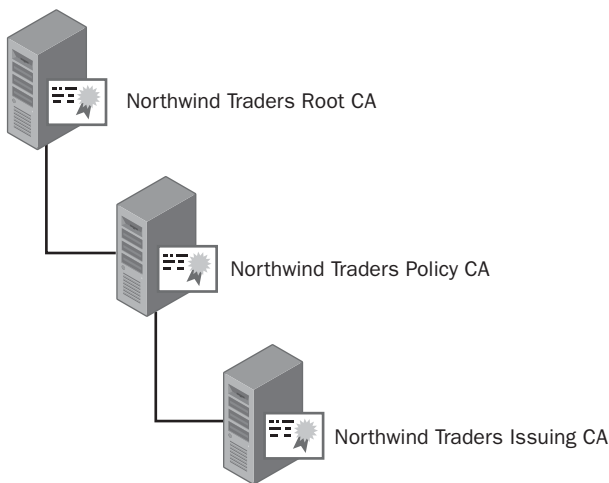
- **Expired.** The CA certificate or CRL at the referenced URL is expired.
- **Unable to download.** The CA certificate or CRL could not be downloaded from the referenced URL.

## Case Study: Choosing Publication Points

This case study will test your knowledge of choosing CRL and CA certificate publication points.

### Design Requirements

You are responsible for defining the CA certificate and CRL publication points for your CA hierarchy. Your organization, Northwind Traders, is implementing a three-tier CA hierarchy, as shown in Figure 9-6.



**Figure 9-6** The Northwind Traders CA hierarchy

The following requirements for your network should influence your decision on where to publish the CA certificate and CRLs for your CA hierarchy:

- Northwind Traders implements an Active Directory forest with a single domain named corp.nwtraders.com on the production network.
- Externally accessible Windows 2000 Web servers are located in a DMZ and are not members of the corp.nwtraders.com domain.
- The client computers run Windows 2000 Professional and Windows XP Professional.
- Some Web servers run BSD UNIX with Apache Web servers.
- All access to Web servers is authenticated by using certificate-based authentication.
- The Northwind Traders security policy requires that all applications implement strong CRL checking.



## Case Study Questions

1. What URLs do you include in the Northwind Traders root CA certificate for the AIA and CDP extensions?
2. Are there any network design issues that prevent you from implementing an LDAP URL as the first URL in the list of available URLs for CA certificates and CRLs?
3. What form of URL should you implement as the first URL in CDP and AIA URL listings?
4. What protocol by default provides redundancy and high availability in an Active Directory environment?
5. How do you provide redundancy and high availability for HTTP URLs?

## Additional Information

- “Troubleshooting Certificate Status and Revocation” (*[www.microsoft.com/technet/security/topics/crypto/tshtcrl.aspx](http://www.microsoft.com/technet/security/topics/crypto/tshtcrl.aspx)*)
- RFC 3280, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” (*[www.ietf.org/rfc/rfc3280.txt](http://www.ietf.org/rfc/rfc3280.txt)*)
- CAPIMON tool (*[www.microsoft.com/downloads/details.aspx?FamilyID=0bfe87a8-4e79-4441-9d4c-0cab35d49a01&DisplayLang=en](http://www.microsoft.com/downloads/details.aspx?FamilyID=0bfe87a8-4e79-4441-9d4c-0cab35d49a01&DisplayLang=en)*)
- Knowledge Base Article 320528, “How to Configure Active Directory to Allow Anonymous Queries” (Windows 2000)
- Knowledge Base Article 326690, “Anonymous LDAP Operations to Active Directory Are Disabled on Windows Server 2003 Domain Controllers”



**Note** Microsoft Knowledge Base articles can be found at <http://support.microsoft.com>. Enter the article number in the Search the Knowledge Base text box.



# Chapter 10

## Role Separation

A step in designing and implementing a public key infrastructure (PKI) is determining the groups or users who will manage it. To facilitate secure administration of Certificate Services, the Microsoft Windows Server 2003 PKI supports Common Criteria role separation. Common Criteria defines that PKI management be configured so that no single person has full control and thereby protects an organization against a “malicious PKI administrator.”

Other roles also must be considered when designing and implementing your organization’s PKI in addition to the roles defined in the Common Criteria protection profile. This chapter will discuss how to plan PKI membership and implement role separation.

### Common Criteria Roles

According to Common Criteria guidelines, no user can hold more than one PKI management role—any user who does hold two or more PKI management roles must be blocked from all management functions.



**Note** You can assign multiple users the same role when defining role holders. Enforcing Common Criteria role separation on a Windows Server 2003 certification authority (CA) ensures that *a single user cannot hold multiple roles, but multiple users can hold the same role.*

### Common Criteria Levels

“Certificate Issuing and Management Components Family of Protection Profiles” is a standards document that defines requirements for the issuance, revocation, and management of X.509 certificates. Taking into consideration that different security levels are required for different organizations, the standards document describes four protection profiles. Each profile provides additional safety through increased security and assurance requirements for X.509 certificate distribution.



**More Info** Windows Server 2003 Certificate Services is designed to meet the role definitions defined in version 1.0 of “Certificate Issuing and Management Components Family of Protection Profiles,” which can be found at [http://csrc.nist.gov/pki/documents/CIMC\\_PP\\_20011031.pdf](http://csrc.nist.gov/pki/documents/CIMC_PP_20011031.pdf).

## Security Level 1

CIMC Security level 1 defines the minimum level of certificate management security for environments in which threats against the PKI are considered to be low. It defines two PKI management roles:

- **CA administrator.** Responsible for account administration, key generation of the certification authority (CA) certificate’s key pair, and auditing configuration.
- **Certificate manager.** Responsible for certificate management. Management functions include issuing and revoking certificates.

In addition, the PKI must restrict access to authorized PKI users and only implement cryptographic algorithms that are validated against FIPS 140-1, “Security Requirements for Cryptographic Modules.”

## Security Level 2

CIMC Security level 2 increases the level of certificate management security for environments in which the risks and consequences of data disclosure are not considered a significant issue. It also increases security by rejecting certificate requests by unauthorized users. All users must authenticate with the PKI before certificate issuance.

Security level 2 uses the same two management roles as Security level 1. The difference is that level 2 requires increased auditing and cryptographic protection of audit logs and system backups. In addition, FIPS 140-1 level 2 cryptographic modules are required for the protection of a CA’s key pair.

## Security Level 3

CIMC Security level 3 raises the security level further and is intended for environments in which it is considered a moderate risk if data is disclosed or there is a loss of data integrity. As compared to Security level 2, CIMC Security level 3 implements additional integrity controls to ensure that an unauthorized person cannot modify data. This includes protection against an unauthorized person who gains physical access to a CA.

Security level 3 defines three PKI management roles:

- **CA administrator.** Responsible for account administration, key generation of the CA certificate's key pair, and auditing configuration.

## Choosing Auditing Behavior

Windows Server 2003 Service Pack 1 allows you to choose which Common Criteria role can define audit settings. The default behavior in Windows Server 2003 is to allow the Auditor role to both define audit settings at the CA and to view and maintain the audit logs.

With Windows Server 2003 Service Pack 1 installed, you can instead choose to have the CA administrator role define the audit settings at a specific CA. This is accomplished by having a local administrator run the following certutil command:

```
certutil -setreg CA\InterfaceFlags +IF_ENABLEADMINASAUDITOR
```

Once the command executes and Certificate Services is restarted, the task of defining the CA audit settings is allocated to the CA administrator role rather than the CA auditor role.

- **Certificate manager.** Responsible for certificate management. Management functions include issuing and revoking certificates.
- **Auditor.** Responsible for maintaining the CA audit logs.

Additional security measures include having at least two persons involved in the control and management of private keys, implementing FIPS 140-1 level 3 protection of CA keys, and requiring digital signatures for all data transferred between the CA and the HSM.

## Security Level 4

CIMC Security level 4 provides the highest PKI security protection. It is intended for environments in which threats to and consequences of data disclosure and loss of data integrity by either authorized or unauthorized users are significant to the organization.

Security level 4 defines four PKI management roles:

- **CA administrator.** Responsible for account administration and key generation of the CA certificate's key pair.
- **Certificate manager.** Responsible for certificate management including functions such as issuing and revoking certificates.

- **Auditor.** Responsible for maintaining and viewing the CA audit log entries in the Windows Security log.
- **Backup operator.** Responsible for performing backups of PKI information.

Security level 4 requires signed third-party timestamping of audit logs to increase integrity. In addition, cryptographic modules at each CA must be validated to FIPS 140-1 level 4.



**Note** The only cryptographic module rated at FIPS 140-1 level 4 at the time of publication is the AEP SureWare Keyper Enterprise ([www.aepsystems.com/prod\\_keyper\\_ent.htm](http://www.aepsystems.com/prod_keyper_ent.htm)). More FIPS 140-1 level 4 devices are expected to be available in the near future.

## The Windows Server 2003 Implementation of Common Criteria

Windows Server 2003 allows you to define PKI management roles in compliance with the four roles defined in CIMC Security level 4. The Windows Server 2003 PKI management roles are:

- CA administrator
- Certificate manager
- Auditor
- Backup operator

The sections that follow provide information on Windows Server 2003 Common Criteria roles and how to implement each role.



**Note** Windows Server 2003 PKI does not require the user to have administrative rights on the CA computer for day-to-day PKI management. The user must be assigned only the CA permissions or the user rights associated with one of the four Common Criteria roles.



**Important** The only cases where administrative rights are required at a CA are the installation of a new CA or the renewal of a CA certificate. You must be a member of the local administrators to install Certificate Services and generate key material in the Local Machine store. In addition, you must be a member of Enterprise Admins to install or renew an enterprise CA.

## CA Administrator

A CA administrator configures and maintains the CA. A user assigned the CA administrator role can designate other CA administrators, assign certificate managers, and perform the following CA management tasks:

- **Configure extensions.** Define URLs for both CRL Distribution Points (CDPs) and Authority Information Access (AIA).
- **Configure policy and exit modules.** Policy and exit modules determine the actions a CA takes during certificate issuance. For example, the default policy module allows a CA administrator to configure whether all certificate requests are pending or issued based on the user's credentials. An exit module allows you to define whether the certificate information is published to pre-configured file sharing locations.

### Using Exit Modules

---

Exit modules can be used in many ways to enhance the functionality of a Windows Server 2003 CA. For example, Microsoft has deployed a custom exit module that performs a real-time, centralized logging function that tracks all issued certificates into a Microsoft SQL Server database. This functionality is discussed in the article "Deploying PKI Inside Microsoft" at [www.microsoft.com/technet/itsolutions/msit/security/deppkiin.aspx](http://www.microsoft.com/technet/itsolutions/msit/security/deppkiin.aspx).

In the default exit module for Certificate Services, you can enable additional functionality by enabling simple mail transfer protocol (SMTP) within the exit module. SMTP allows the CA to send e-mail messages to designated e-mail recipients when specific CA activities take place, such as the publication of a CRL, revocation of a certificate, or stopping and starting of Certificate Services. The SMTP exit module is discussed in the Windows Server 2003 PKI Operations Guide available at <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03pkog.aspx>.

- **Define certificate manager restrictions.** Restrict each defined certificate manager to management of members of designated global groups.
- **Define certificate managers.** Designate certificate managers to issue and deny certificate requests and to extract encrypted private keys from the CA database for key recovery.
- **Define key recovery agents.** Designate key recovery agent certificates at a CA for the archival and recovery of private keys at the CA database.

- **Define other CA administrators.** Designate CA administrators to perform CA management tasks.
- **Delete a single record in the CA database.** By using the `certutil -deleterow` command to delete the record associated with the certificate, you can remove specific certificate information from the CA database.
- **Enable, publish, or configure CRL schedule.** Manage all aspects of publishing CRLs and delta CRLs at a CA.
- **Read the CA configuration information.** View the CA's current configuration and modify only those areas enabled for modification by CA administrators.
- **Stop and start Certificate Services.** Stop and start Certificate Services to apply registry changes.



**Warning** This does not prevent a local Administrator from stopping and starting Certificate Services. This only allows a CA administrator to stop and start Certificate Services.

- **Configure audit parameters.** As mentioned, by running `certutil -setreg CA\InterfaceFlags +IF_ENABLEADMINASAUDITOR` you can allow a CA administrator to define audit settings at a CA rather than allow a CA auditor to define these settings.

## Certificate Manager

This role approves or denies certificate enrollment requests and revokes issued certificates. Specifically, a user assigned the certificate manager role can:

- **Issue or deny pending certificate requests.** At a standalone CA all certificate requests are pending by default until a certificate manager approves the certificate requests. Likewise, a certificate template can be defined so that a certificate manager must approve a certificate request before the CA issues the certificate.
- **Revoke issued certificates.** A certificate manager can revoke a certificate if the organization's revocation policy requires certificate revocation. For example, a certificate can be revoked if the private key is compromised. Certificate revocation terminates the certificate's validity prior to expiration.



- **Determine key recovery agents.** A certificate manager determines which defined key recovery agent can decrypt an archived private key from the CA database.
- **Extract archived private keys from the CA database.** A certificate manager can extract the archived private key from the CA database. The private key is extracted in a binary large object (BLOB) format, which is an encrypted PKCS #7 file that only the designated key recovery agent can decrypt.



**Note** A binary large object (BLOB) is a data type that can store any format of data in a binary format.

## Auditor

An auditor is able to define the audit settings for Certificate Services. This includes defining the specific events to audit and viewing the Security event log to review auditing events related to Certificate Services. An auditor can enable the following auditing settings for the CA in the Certificate Authority console:

- **Backup and restore the CA database.** Logs any attempt to back up or restore the CA database to the Windows Security log.
- **Change CA configurations.** Logs any attempt to modify CA configuration. This can include defining AIA and CDP URLs or defining a key recovery agent.
- **Change CA security settings.** Logs any attempt to modify CA permissions. This can include adding CA administrators or certificate managers.
- **Issue and manage certificate requests.** Logs any attempt by a certificate manager to approve or deny certificate requests that are pending subject approval.
- **Revoke certificates and publish CRLs.** Logs any attempt by a certificate manager to revoke an issued certificate or by a CA administrator to publish an updated CRL.
- **Store and retrieve archived keys.** Logs any attempt during the enrollment process to archive private keys in the CA database or by certificate managers to extract archived private keys from the CA database.
- **Start and stop Certificate Services.** Logs any attempt by the CA administrator to start or stop Certificate Services.



**Note** To ensure that all events related to Certificate Services auditing are logged to the security log, ensure that both success and failure events are enabled for Object Access at the CA. The settings can be applied directly in the Local Security Settings or by applying a Group Policy object (GPO) with the required auditing settings.



**Important** With the installation of Windows Server 2003 Service Pack 1 you can change the default behavior and prevent auditors from defining the audit settings at the Windows Server 2003 CA. Instead, the task is assigned to the CA administrator role.

## Backup Operator

Performs backups of the CA database, the CA configuration, and the CA's private and public key pair (also known as a key pair).



**Note** If the CA's private and public key pair is stored on a hardware security module (HSM), backup operators can only back up the CA key pair if the HSM's security context allows this ability.

You can use one of the following methods to perform the backup of CA information:

- **Windows Server 2003 backup utility.** By including the System State in the backup set, you ensure that Certificate Services is fully backed up. The System State includes the CA database, CA log files, and registry configuration of Certificate Services.
- **Certification Authority console.** From the Certification Authority console, a backup operator can include the private key and CA certificate, as well as the certificate database and certificate database log, in the backup set. In addition, the backup operator can choose whether to perform a full or an incremental backup.

- **Certutil.exe.** Certutil provides three command lines for backing up Certificate Services:
  - **Certutil –backup.** The backup set includes the certificate database, the CA certificate, and the CA key pair.
  - **Certutil –backupDB.** The backup set only includes the certificate database.
  - **Certutil –backupkey.** The backup set only includes the CA certificate and the CA key pair.

## Assigning Common Criteria Roles

Once you determine which users should hold which Common Criteria role, you must define the role holders. The definition is CA-specific, meaning that you can assign different role holders at each CA in the hierarchy.



**Tip** Assign the permissions for Common Criteria role separation to either domain local groups (for domain member computers) or local groups within the local Security Account Management (SAM) database of each CA.

### CA Administrator

You can use the following procedure to define a CA administrator at a CA:

1. Open the Certification Authority console.
2. In the console tree, right-click *CAName* and click Properties.
3. On the Security tab, click Add, and type the names of any users or domain local groups that will be CA administrators.
4. Assign the users or groups Manage CA permission and click OK.

### Certificate Manager

You can use the following procedure to define a certificate manager at a CA:

1. Open the Certification Authority console.
2. In the console tree, right-click *CAName* and click Properties.

3. On the Security tab, click Add and type the names of any domain local groups that will be certificate managers.
4. Assign the users or groups Issue and Manage Certificates permission and click OK.

## Auditor

You can use the following procedure to assign a user the role of auditor:

1. From Administrative Tools, open Local Security Policy.
2. In the console tree, expand Local Policies and click User Rights Assignment.
3. In the details pane, double-click Manage Auditing and Security Log.
4. Add the user accounts or groups that will perform auditing at the CA and click OK.
5. Close Local Security Policy.



**Warning** A CA auditor is assigned the auditor role systemwide. The user cannot be limited to only viewing Security event log entries related to Certificate Services. The user can view *all* entries in the Security event log.

## Backup Operator

You can use the following procedure to assign a user or group the role of backup operator:

1. From Administrative Tools, open Local Security Policy.
2. In the console tree, expand Local Policies and click User Rights Assignment.
3. In the details pane, double-click Backup Files and Directories.
4. Add the user accounts or groups that will perform auditing at the CA and click OK.
5. In the details pane, double-click Restore Files and Directories.
6. Add the user accounts or groups that will perform auditing at the CA and click OK.
7. Close Local Security Policy.



**Note** Alternatively, you can choose to simply add the user account to the local Backup Operators group. The advantage of assigning the user rights directly is that it allows you to split the roles of backup and restoration.

## Implementing Certificate Manager Restrictions

Some organizations require further restrictions on certificate manager activities. Rather than allow a certificate manager to issue or revoke *any* certificate issued by a CA, the organization might want a certificate manager to only manage a subset of all certificates.

Windows Server 2000 Certificate Services allows a CA administrator to define restrictions for certificate managers. A certificate manager restriction limits a certificate manager to only issuing or revoking a certificate whose subject has membership in a specified security group.

For example, assume that the following groups are assigned the Issue and Manage Certificates permission:

- APACCertManagers
- EMEACertManagers



**Important** To define a certificate manager restriction for a specific user or group, the user or group must be explicitly defined the Issue and Manage Certificates permission in the CA's security tab. You cannot define certificate manager restrictions for users or groups nested within a group assigned the Issue and Manage Certificates permission.

A CA administrator could then restrict which groups, computers, or users the APACCertManagers and EMEACertManagers can manage. The APACCertManagers group can be limited to only issuing or revoking certificates issued to the members of the APACUsers and APACComputers groups. Likewise, the EMEACertManagers group can be limited to issuing and revoking certificates issued to the EMEAUsers and EMEAComputers groups.



**Important** If a user account has membership in both the APACUsers and EMEAUsers groups, the certificate issued to that user can be managed by certificate managers in either the APACCertManagers or EMEACertManagers groups.

To implement certificate manager restrictions, the CA computer account must be included in the Pre-Windows 2000 Compatible Access group. Membership in this group allows the CA to determine the group memberships defined for the subject of a certificate.

## Enforcing Common Criteria Role Separation

Windows Server 2003, Enterprise Edition, and Windows Server 2003, Datacenter Edition, allow you to enforce Common Criteria role separation. By enforcing role separation, Certificate Services blocks any user account assigned two or more Common Criteria roles from all Certificate Services management activities.

For example, if a user is assigned both the CA administrator and certificate manager roles, the user cannot perform the tasks defined for either role. If a user is assigned multiple roles, the user is blocked from backing up the CA database, key pair, and logs when using any of the backup tools.

To enforce Common Criteria role separation, a local administrator of the computer must configure the RoleSeparationEnabled registry entry. This is done with the following procedure:

1. Type the following command at a Command Prompt:

```
certutil -setreg CA\RoleSeparationEnabled 1
```

2. Restart Certificate Services.

If any users are assigned two or more roles, their administrative activities are blocked immediately.



**Tip** If you accidentally assign yourself two or more Common Criteria roles—thereby blocking yourself from PKI management tasks—a local operating system administrator must disable Common Criteria role separation by typing **certutil -delreg CA\RoleSeparationEnabled** and restart Certificate Services. With role separation disabled, a CA administrator or local administrator must fix the role assignments and re-enable Common Criteria role separation.

### **Role Separation and CA Certificate Renewal**

The one scenario where role separation hinders PKI management activities is the case of CA certificate renewal. When a CA certificate is renewed, a user might have to hold different roles. The user:

- Must be a CA administrator to publish an updated CRL.
- Must be a local administrator to renew the CA certificate.
- Must be a member of the local Administrators group to access the Local Machine store of a software-based cryptographic service provider (CSP), such as the Microsoft Strong Cryptographic Service Provider v1.0. Only members of the local Administrators group have the necessary permissions to add or remove certificates from the Local Machine store.
- Must be a member of the *ForestRootDomain*\Domain Admins or Enterprise Admins group to allow creation of the CDP and CA certificate objects within the Configuration Naming context.
  - A new CDP object is created in the CN=CAName,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,*ForestRootDomain* (where *CAName* is the NetBIOS name of the CA computer and *ForestRootDomain* is the LDAP distinguished name of the forest) container.
  - A new CA certificate object is created in the AIA container (CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,*ForestRootDomain*).
  - A new CA certificate object is added to the NTAUTH store (CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,*ForestRootDomain*).
  - If the CA is an enterprise CA, a new CA certificate object is created in the Enrollment Services container (CN=Enrollment Services,CN=Public Key Services,CN=Services,CN=Configuration,*ForestRootDomain*).
  - If the CA is an enterprise root CA, a new CA certificate object is created in the Certification Authorities container (CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration,*ForestRootDomain*).

To accomplish the task of CA certificate renewal, temporarily disabling role separation during the CA certificate renewal process is recommended. Ensure that the account that performs the CA certificate renewal is a member of the Enterprise Admins group, a member of the local Administrators group, and assigned the Manage CA permissions. Once the CA certificate renewal process is completed, role separation should be enforced.

## Other PKI Management Roles

In addition to the Common Criteria roles, Windows Server 2003 can implement other roles in the PKI management structure.

### Local Administrator

The CA's local Administrator is any member of the local Administrators group in the local accounts database of the CA computer. This typically includes the local Administrator account and the Domain Admins global group from the CA computer's domain. The membership can also contain the Enterprise Admins group from the forest root domain.

### Local Administrator Tasks

A local Administrator can perform the following tasks at a Windows Server 2003 CA:

- **All CA administrator tasks.** By default, the local Administrator account is assigned the Manage CA permission.
- **All certificate manager tasks.** By default, the local Administrator account is assigned the Issue and Manage Certificates permission.
- **Enable or disable Common Criteria role separation.** Members of the local Administrators group have the required permissions to make the necessary registry modifications to enable or disable Common Criteria role separation.
- **Install Certificate Services.** To install Certificate Services, the installer must be a member of the local Administrators group.
- **Renew a CA certificate.** To renew a CA certificate, the user must have access to the local machine's certificate store. By default, only members of the local Administrators group have the necessary access.

### Assigning the Local Administrator Role

Assuming that the CA computer is either a member of a workgroup or a member server in the domain (not a domain controller), you can use the following procedure to assign the local administrator role:

1. From Administrative Tools, open Computer Management.
2. In the console tree, expand Local Users and Groups and click Groups.
3. In the details pane, double-click Administrators.
4. In the Administrators Properties dialog box, click Add.



5. In the Select Users or Groups dialog box, type the name of the user account or group you want to make a local Administrator and click OK.
6. In the Administrators Properties dialog box, click OK.
7. Close the Computer Management console.

## Enterprise Admins

By default, Enterprise Admins are able to create and modify objects stored in Microsoft Active Directory's Configuration naming context. When you install an enterprise CA in your forest, a member of the Enterprise Admins group must perform the installation to ensure that the required objects are created in the Configuration naming context.



**Note** The user performing the installation must be a member of the local Administrators group to install Certificate Services.

## Enterprise Admins Tasks

A member of the Enterprise Admins group is able to perform the following PKI administration tasks:

- **Install an enterprise CA.** Only members of the Enterprise Admins group can create the required objects in the Configuration naming context when an enterprise CA is installed.
- **Modify and create certificate templates.** A member of the Enterprise Admins group can modify permissions of a version 1 certificate template and all properties of a version 2 certificate template. In addition, members of the Enterprise Admins group can create new version 2 certificate templates based on existing version 1 or version 2 certificate templates.
- **Publish CA certificates to Active Directory.** A member of the Enterprise Admins group can publish the CA certificate for an offline CA, NTAAuth certificates, and Cross Certification Authority certificates to the Configuration naming context.
- **Publish offline CA CRLs to Active Directory.** A member of the Enterprise Admins group can publish the CRL for an offline CA to the Configuration naming context.

## Assigning the Enterprise Admins Role

You can use the following procedure to assign membership to the Enterprise Admins group:

1. Log on as a member of the Enterprise Admins group or the forest root domain's Domain Admins group.
2. From Administrative Tools, open Active Directory Users and Computers.
3. In the console tree, ensure that the focus of the Active Directory Users and Computers console is on the forest root domain.
4. In the console tree, expand *ForestRootDomain* and click the Users container.
5. In the details pane, double-click Enterprise Admins.
6. In the Enterprise Admins Properties dialog box, on the Members tab, click Add.
7. In the Select User, Contact, Computers, or Groups dialog box, type the names of the users or groups you want to add to the Enterprise Admins group and click OK.
8. In the Enterprise Admins Properties dialog box, click OK.
9. Close the Active Directory Users and Computers console.

## Certificate Template Manager

In some organizations, the task of managing certificate templates can be delegated to a custom group rather than left to the Enterprise Admins group.

### Certificate Template Manager Tasks

A certificate template manager is able to manage the properties of existing certificate templates. In addition, a certificate template manager is able to create, modify, or delete version 2 certificate templates.

### Assigning the Certificate Template Manager Role

Three separate tasks must be performed to assign the Certificate Template Manager role:

- Delegate permissions to the Certificate Templates container in the Configuration naming context to create new certificate templates.
- Delegate permissions to the OID container in the Configuration naming context to create new object identifiers (OIDs).
- Delegate permissions to every existing certificate template in the Certificate Templates container in the Configuration naming context.

**Delegate Permissions for Creation of New Templates**

You can delegate the permission to create new templates by assigning permissions to a custom universal group for the CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=*ForestRootDomain* container, as follows:

1. Log on as a member of the Enterprise Admins group or the forest root domain Domain Admins group.
2. Open the Active Directory Sites and Services console.
3. From the View menu, ensure that the Show Services Node option is enabled.
4. In the console tree, expand Services, expand Public Key Services, and click Certificate Templates.
5. In the console tree, right-click Certificate Templates and click Delegate Control.
6. In the Delegation of Control Wizard, click Next.
7. On the Users or Groups page, click Add.
8. In the Select Users, Computers, or Groups dialog box, type a user or group name and click OK.
9. On the Users or Groups page, click Next.
10. On the Tasks to Delegate page, click Create a Custom Task to Delegate and click Next.
11. On the Active Directory Object Type page, click This Folder, Existing Objects in this Folder, and Creation of New Objects in This Folder, and click Next.
12. On the Permissions page, in the Permissions list, enable Full Control and click Next.
13. On the Completing the Delegation of Control Wizard page, click Finish.

**Delegate Permissions for Creation of New OIDs**

When a certificate template is created, an OID is generated to identify the certificate template. To create a new certificate template, a user must be delegated the permission to create new OIDs in the CN=OID,CN=Public Key Services,CN=Services,CN=Configuration,DC=*ForestRootDomain* container.

1. Log on as a member of the Enterprise Admins group or the forest root domain Domain Admins group.
2. Open the Active Directory Sites and Services console.
3. On the View menu, ensure that the Show Services Node option is enabled.
4. In the console tree, expand Services, expand Public Key Services, right-click OID, and click Properties.

5. In the OID Properties dialog box, on the Security tab, click Add.
6. In the Select Users, Computers, or Groups dialog box, type the names of the users or groups you want to delegate certificate management permissions, and click OK.
7. In the OID Properties dialog box, select the users or groups that you want to add, enable the Allow check box for Full Control for each entry, and click OK.

### Delegate Permissions to Every Existing Certificate Template in the Certificate

Once you delegate permissions for creating and modifying new certificate templates, you must modify the permissions of the existing certificate templates.

You can run the script file that follows to delegate permissions to a custom universal group. The script file assumes that only the 31 default certificate templates exist. If you create any other certificate templates, you must modify the script to include the additional certificate templates created before executing the script file.



**On the Resource Kit CD** A copy of this script is included on the accompanying CD-ROM. The script, `DelegateTemplateModification.cmd`, must be modified to replace the `example\TemplateAdministrators` group with the name of the custom universal group deployed in your forest.



**Note** This script requests that Windows Support Tools are installed to allow the use of the `dscls.exe` command.

```
@echo off
```

```
echo Add custom ACEs for the TemplateAdministrators group
```

```
dscls "CN=Administrator,CN=Certificate Templates,CN=Public Key Services,CN=Services,
CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWPRPCCDCWSLO
dscls "CN=CA,CN=Certificate Templates,CN=Public Key Services,CN=Services,
CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWPRPCCDCWSLO
dscls "CN=CAExchange,CN=Certificate Templates,CN=Public Key Services,CN=Services,
CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWPRPCCDCWSLO
dscls
"CN=CEPEncryption,CN=Certificate Templates,CN=Public Key Services,CN=Services,
CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWPRPCCDCWSLO
dscls "CN=ClientAuth,CN=Certificate Templates,CN=Public Key Services,CN=Services,
```

```

CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWP RPCCDCWSLO
dsacIs "CN=CodeSigning,CN=Certificate Templates,CN=Public Key Services,CN=Services,
CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWP RPCCDCWSLO
dsacIs "CN=CrossCA,CN=Certificate Templates,CN=Public Key Services,CN=Services,
CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWP RPCCDCWSLO
dsacIs "CN=CTLSigning,CN=Certificate Templates,CN=Public Key Services,CN=Services,
CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWP RPCCDCWSLO
dsacIs "CN=DirectoryEmailReplication,CN=Certificate Templates,CN=Public Key Services,
CN=Services,CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWP RPCCDCWSLO
dsacIs "CN=DomainController,CN=Certificate Templates,CN=Public Key Services,
CN=Services,CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWP RPCCDCWSLO
dsacIs "CN=DomainControllerAuthentication,CN=Certificate Templates,CN=Public Key Services,
CN=Services,CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWP RPCCDCWSLO
dsacIs "CN=EFS,CN=Certificate Templates,CN=Public Key Services,CN=Services,
CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWP RPCCDCWSLO
dsacIs "CN=EFSRecovery,CN=Certificate Templates,CN=Public Key Services,CN=Services,
CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWP RPCCDCWSLO
dsacIs "CN=EnrollmentAgent,CN=Certificate Templates,CN=Public Key Services,CN=Services,
CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWP RPCCDCWSLO
dsacIs "CN=EnrollmentAgentOffline,CN=Certificate Templates,CN=Public Key Services,
CN=Services,CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWP RPCCDCWSLO
dsacIs "CN=ExchangeUser,CN=Certificate Templates,CN=Public Key Services,CN=Services,
CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWP RPCCDCWSLO
dsacIs "CN=ExchangeUserSignature,CN=Certificate Templates,CN=Public Key Services,
CN=Services,CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWP RPCCDCWSLO
dsacIs "CN=IPSecIntermediateOffline,CN=Certificate Templates,CN=Public Key Services,
CN=Services,CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWP RPCCDCWSLO
dsacIs "CN=IPSecIntermediateOnline,CN=Certificate Templates,CN=Public Key Services,
CN=Services,CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWP RPCCDCWSLO
dsacIs "CN=KeyRecoveryAgent,CN=Certificate Templates,CN=Public Key Services,
CN=Services,CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWP RPCCDCWSLO
dsacIs "CN=Machine,CN=Certificate Templates,CN=Public Key Services,CN=Services,
CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWP RPCCDCWSLO
dsacIs "CN=MachineEnrollmentAgent,CN=Certificate Templates,CN=Public Key Services,
CN=Services,CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWP RPCCDCWSLO

```

```

dsacIs "CN=OfflineRouter,CN=Certificate Templates,CN=Public Key Services,CN=Services,
CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWPRPCCDCWSLO
dsacIs "CN=RASAndIASServer,CN=Certificate Templates,CN=Public Key Services,CN=Services,
CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWPRPCCDCWSLO
dsacIs "CN=SmartCardLogon,CN=Certificate Templates,CN=Public Key Services,CN=Services,
CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWPRPCCDCWSLO
dsacIs "CN=SmartCardUser,CN=Certificate Templates,CN=Public Key Services,CN=Services,
CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWPRPCCDCWSLO
dsacIs "CN=SubCA,CN=Certificate Templates,CN=Public Key Services,CN=Services,
CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWPRPCCDCWSLO
dsacIs "CN=User,CN=Certificate Templates,CN=Public Key Services,CN=Services,
CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWPRPCCDCWSLO
dsacIs "CN=UserSignature,CN=Certificate Templates,CN=Public Key Services,CN=Services,
CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWPRPCCDCWSLO
dsacIs "CN=WebServer,CN=Certificate Templates,CN=Public Key Services,CN=Services,
CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWPRPCCDCWSLO
dsacIs "CN=Workstation,CN=Certificate Templates,CN=Public Key Services,CN=Services,
CN=Configuration,DC=example,DC=com" /G example\TemplateAdministrators:
SDDTRCWDWOLCWPRPCCDCWSLO

```

## Enrollment Agent

An enrollment agent is able to request certificates on behalf of other users.

### Enrollment Agent Tasks

The enrollment agent role is typically used to request smart card certificates on behalf of other users. An enrollment agent validates the smart card requestor's identity and then submits a smart card request on behalf of the requestor. The enrollment request differs from a normal enrollment request in that the enrollment agent signs the request with a certificate that has the Certificate Request Agent OID (1.3.6.1.4.1.311.20.2.1) in the certificate's Application Policy extension. The CA enforces that the certificate request must be signed by a certificate with the Certificate Request Agent OID if the subject provided in the certificate request does not match the identity in the submitted of the certificate request.

### Assigning the Enrollment Agent Role

To assign the enrollment agent role, a user must request a certificate with the Certificate Request Agent OID in the Application Policy or in the Enhanced Key Usage (EKU) extension.

By default, the Enrollment Agent version 1 certificate template includes the necessary OID. A user becomes an enrollment agent by requesting and receiving a certificate based on the Enrollment Agent certificate template.



**Note** The design decisions for deploying enrollment agent and smart card certificates are discussed in Chapter 15, “Smart Card Deployment.”

## Key Recovery Agent

The key recovery agent role is responsible for recovering private keys archived in the CA database. Only the holders of the private key associated with the Key Recovery Agent certificate can recover the private keys once a certificate manager extracts the PKCS #7 blob file from the CA database.

### Key Recovery Agent Tasks

A key recovery agent is responsible for decrypting a PKCS #7 blob file that contains an encrypted copy of the user’s certificate and private key. The resulting decryption provides a PKCS #12 object (file) that can be imported by the user into his or her profile.

A key recovery agent is dependent on the certificate manager role to extract the encrypted PKCS #7 blob file from the CA database. To ensure that at least two people are involved in the key recovery process, the key recovery agent should not be assigned the certificate manager role.



**Warning** You should never assign a user both the certificate manager and key recovery agent roles. Even though Common Criteria role separation does not address key archival, allowing one user to hold both the certificate manager and key recovery agent roles gives that user the ability to both extract and decrypt an archived private key from the CA database.

### Assigning the Key Recovery Agent Role

To assign the key recovery agent role, a user must have a certificate with the Key Recovery Agent application policy OID. The default Key Recovery Agent version 2 certificate template includes this application policy OID and can be further secured by limiting the users and groups with enrollment permissions.

In addition, a CA must be configured to enable key recovery. This is done by designating one or more Key Recovery Agent certificates to act as the CA's key recovery agent. Only the holders of the private keys associated with the selected Key Recovery Agent certificates are able to decrypt the extracted PKCS #7 blobs.



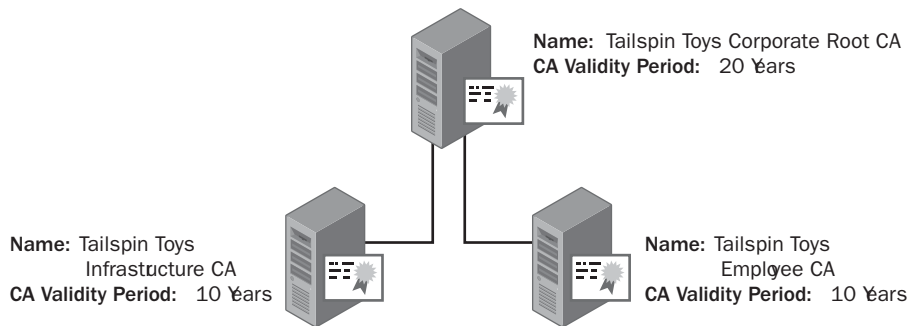
**Note** The design decisions for deploying key recovery agents and enabling key archival and recovery are discussed in Chapter 14, “Archiving Encryption Keys.”

## Case Study: Planning PKI Management Roles

In this case study, you will look at the definition of PKI Management roles.

### Scenario

You are the security services manager for Tailspin Toys. Your organization implements a two-tier CA hierarchy, as shown in Figure 10-1.



**Figure 10-1** The Tailspin Toys CA hierarchy

The CA hierarchy implements two issuing CAs:

- **Tailspin Toys Infrastructure CA.** This CA issues certificates to domain controllers, servers, computers, and network devices.
- **Tailspin Toys Employee CA.** This CA issues certificates to employees (users) of Tailspin Toys.



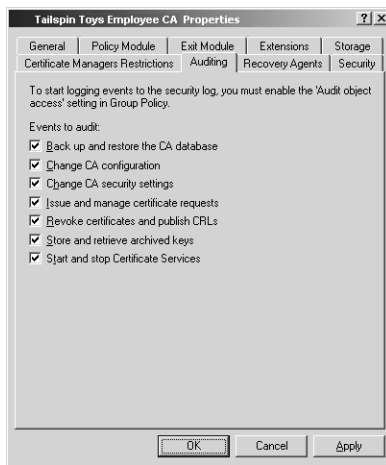
The issuing CAs are managed by two different teams: the network services team manages the Tailspin Toys Infrastructure CA and the directory services team manages the Tailspin Toys Employee CA. Your team, security services, has the ability to manage both CAs.

Within each department, different users are assigned the PKI Common Criteria roles of CA administrator and certificate manager. Backups are performed by a centralized backup services account. Auditing is performed by members of both the Security Services team and the Internal Audit department. The security policy of Tailspin Toys requires strong enforcement of Common Criteria role separation for PKI management.

## Case Study Questions

1. The backup software implemented by Tailspin Toys uses a centralized backup services account. When reviewing the event logs, the backup operator notices that the backup fails every night on the two issuing CAs. On inspecting the event logs further, the backup software reports that the failed backup item is the System State backup. What is the likely cause of the error?
2. When inspecting the security permission assignments at the Tailspin Toys Infrastructure CA, you accidentally assign the CA Administrator group the Issue and Manage Certificates permission. When you try and fix the permissions assignment error, you find that access is denied. What must be done to fix the issue?
3. The certificate for the Tailspin Toys Employee CA is reaching the halfway point of its validity period and must be renewed. You are logged on to the CA as a CA Administrator but all attempts to renew the CA certificate fail. Who must perform the renewal of the CA certificate?
4. The Tailspin Toys Employee CA implements key archival for both EFS certificates and e-mail encryption certificates. The security policy of your organization requires that all key recovery operations be performed by at least two employees. If you are assigned the key recovery agent role, what Common Criteria role can you not hold, as this would break the security policy for key recovery?

5. Tailspin Toys implements several version 1 certificate templates at the Tailspin Toys Infrastructure CA. You have delegated the task of managing Certificate Templates to Andy, a member of the IT security team. Andy is able to create new version 2 certificates but is unable to modify the permissions for any of the version 1 certificate templates deployed at the Tailspin Toys Infrastructure CA. Why is Andy unable to modify the version 1 certificate templates?
6. Tailspin Toys wishes to deploy a new enterprise subordinate CA named Tailspin Toys Contractor CA to issue certificates to contractors and vendors working on-site. When you attempt to install the enterprise CA, the options for both enterprise root CA and enterprise subordinate CA are unavailable. What group memberships are required to install an enterprise CA?
7. You have enabled auditing at all issuing CAs in the CA hierarchy. Today, you received a call from the audit department indicating that no events related to Certificate Services exist in the Windows Security log. You view the properties of each CA and find that the auditing is configured at each CA, as shown in Figure 10-2.



**Figure 10-2** Auditing settings defined at the Tailspin Toys Employee CA

Why are there no audit entries related to Certificate Services?

## Additional Information

- Microsoft Official Course 2821: “Designing and Managing a Windows Public Key Infrastructure” ([www.microsoft.com/traincert/syllabi/2821afinal.asp](http://www.microsoft.com/traincert/syllabi/2821afinal.asp))

- “PKCS #7: Cryptographic Message Syntax Standard” (<ftp://ftp.rsasecurity.com/pub/pkcs/doc/pkcs-7.doc>)
- “Windows Server 2003 PKI Operations Guide” ([www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03pkog.mspix](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03pkog.mspix))
- “Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure” ([www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws3pkibp.mspix](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws3pkibp.mspix))
- “PKI Enhancements in Windows XP Professional and Windows Server 2003” ([www.microsoft.com/technet/prodtechnol/winxp/Plan/PKIEnb.asp](http://www.microsoft.com/technet/prodtechnol/winxp/Plan/PKIEnb.asp))
- “Deploying PKI Inside Microsoft” ([www.microsoft.com/technet/itsolutions/msit/security/deppkiin.mspix](http://www.microsoft.com/technet/itsolutions/msit/security/deppkiin.mspix))
- “Certificate Issuing and Management Components Family of Protection Profiles” ([http://csrc.nist.gov/pki/documents/CIMC\\_PP\\_20011031.pdf](http://csrc.nist.gov/pki/documents/CIMC_PP_20011031.pdf))
- FIPS 140-2, Security Requirements for Cryptographic Modules (<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>)



## Chapter 11

# Planning and Implementing Disaster Recovery

When designing a public key infrastructure (PKI) for your organization, you must develop an effective disaster recovery plan to ensure that, in the event of failure of the computer hosting Certificate Services, you can recover in a timely manner with little effect on your organization.

Common reasons that make a disaster recovery plan necessary include:

- **Failed services.** If Certificate Services fails to start on the certification authority (CA) computer, no certificate can be issued and certificate revocation lists (CRLs) cannot be published. Your disaster plan for recovery should include performing and testing either System State or manual CA backups on a regular basis.
- **Hardware failure.** Disaster plan options for recovering after hardware failure include:
  - Maintaining duplicate hardware (such as spare motherboards or spare computers);
  - Performing binary backups with software (such as Symantec Ghost) to rebuild the CA in a timely manner on similar hardware; or
  - Implementing fault-tolerant RAID 1 or RAID 5 volumes to prevent CA failure due to a single disk failure.
- **Network infrastructure failure.** Disaster recovery plans must account for network infrastructure failures. If an application implements CRL checking and network infrastructure failure prevents the application from accessing the most recent version of the CRL, the application will not validate the certificates presented to the application. Your disaster recovery should include methods of diagnosing network infrastructure failures and developing methods of publishing CRL information that are redundant to protect against network failure.

## Developing Required Documentation

One of the most important tasks during the design and deployment of a PKI is to ensure that your network and configuration documentation is updated continually. When you undergo disaster recovery, this documentation is the most important source of information regarding the previous Certificate Services configuration.

You should maintain the following documentation to ensure that you can apply all required configuration of Certificate Services successfully:

- **All certificate template definitions.** In the worst case, you might have to rebuild Active Directory, which requires the redefinition of all certificate templates. By documenting the individual settings for each certificate template on a tab-by-tab basis, you can easily re-create each certificate template.
- **All certificate templates published at the CA.** You can create a custom script file that implements the `certutil -SetCATemplates +<TemplateName>` to publish certificate templates and `certutil -SetCATemplates -<TemplateName>` to remove certificate templates from the CA.
- **All permissions and user rights assignments.** CA permissions define which users or groups hold the CA administrator and certificate manager Common Criteria roles, which groups or users can read the CA configuration, and which groups or users can request certificates from the CA. In addition, the Local Security Policy or domain-based Group Policy objects (GPOs) applied to the CA's computer account define the user rights assigned to the computer account, including the Common Criteria backup operators and auditor role holders.
- **All names used for the CA.** Includes the CA's logical name, the NetBIOS name of the computer hosting Certificate Services, and the domain or workgroup membership. The certificate information is based on the CA's specific names and must be restored exactly.
- **All specific settings in the properties of the CA in the Certification Authority console.** Be sure to identify which certificates are designated for key recovery, if implemented, as well as certificate manager restrictions.
- **Any post- or preinstallation script files used to configure the CA.** For example, if you run a batch file consisting of `certutil` commands that define the CA's registry settings, you should store a copy of the batch file for documentation and recovery purposes. Likewise, you should keep a copy of a batch file that publishes the CA's CRL on an externally accessible Web server.
- **The CA data paths.** When you restore the CA, the previous file locations for the CA database, CA log files, and CA configuration information must be maintained to match the restored registry values.
- **The CRL and Authority Information Access (AIA) publication points.** Once the CA is restored, you must publish an updated CRL and, possi-

bly, an updated CA certificate to the designated publication points. Ensure that no previous publication points are omitted.

- **The cryptographic service provider (CSP) used to protect the CA's private key.** The same CSP must be used to restore the previous key pair for the CA. The CSP might require additional software.
- **The key length of the CA's certificate.** If you are reinstalling the CA or renewing the CA certificate, you should maintain the same key length as originally deployed.
- **The logical disk-partitioning scheme for the CA computer.** When you restore Certificate Services configuration, the disk volumes must implement the same drive letters. Disk volumes can be different sizes or implement different RAID levels, but the drive letters and locations must remain the same for the CA database, CA logs, CA configuration folder (if implemented), and operating system.
- **A copy of the CAPolicy.inf file deployed in the %windir% of the CA computer.** The CAPolicy.inf must be in place when renewing the CA's certificate.

## Choosing a Backup Method

In addition to ensuring that your documentation is up-to-date, make certain that your organization performs regular CA computer backups. Certificate Services offers two backup methods: System State backups and manual backups.

### Who Can Perform Backups of Certificate Services

---

If you implement Common Criteria role separation, choose carefully who can perform a Certificate Services backup. By definition, Common Criteria role separation prevents a user from performing the actions of two or more Common Criteria roles, which are CA administrator, certificate manager, auditor, and backup operator. If a user holds two or more roles, the Certificate Services backup fails.

If the user holds two or more roles, an error message appears stating: "CertUtil: The operation is denied. The user has multiple roles assigned and the CA is configured to enforce role separation." This indicates that Common Criteria role separation is preventing backup. You can overcome this error by disabling Common Criteria role separation, fixing the multiple role assignments and re-enabling Common Criteria role separation as discussed in Chapter 10, "Role Separation."

## System State Backups

System State backup is the preferred method for backing up Certificate Services. A System State backup includes the following settings related to Certificate Services:

- **The CA database.** Includes details on every certificate issued and revoked by the CA.
- **The CA key pair.** The CA either has a self-signed certificate (in the case of a root CA) or a certificate issued by another CA in the hierarchy. The CA key pair must be backed up to ensure that you can rebuild the CA using the same key pair. This also ensures that any certificates currently issued by the CA remain valid after the CA is restored. If the CA's certificate is renewed with a new key pair, the backup must include all versions of the CA key pair.



**Note** If the CA implements a hardware security module (HSM), the backup of the CA's key pair can require third-party backup software. When an HSM is implemented, the CA's private key is removed from the CA computer and protected by the HSM device. This protection causes the System State to not include the CA's key pair in the backup set. The backup of the CA's key pair might require the use of HSM software or backup utilities.

- **The Internet Information Services (IIS) metabase.** If you make any changes to the Certificate Services Web enrollment pages, modifications are made to the IIS metabase. A System State backup ensures that these modifications are included in the backup set.
- **All registry settings related to Certificate Services.** The installation and configuration of a CA includes changing several registry values. Inclusion of the registry in the backup set ensures that the registry settings are restorable.

The main advantage of System State backups is an all-in-one backup, which eliminates the need to restore multiple services, data sets, and registry settings.

## Manual Backups

A manual backup of Certificate Services, a backup performed from the CA or by using the Certutil command, only includes the CA database and the CA's key pair(s). A manual backup does not include the IIS metabase or any Certificate Services registry settings. These items must be restored separately to ensure the full recovery of Certificate Services.





**Note** As with a System State backup, in a manual backup the CA's key pair cannot be backed up if the key pair is protected by an HSM. Details on how to exclude the key pair from the backup set when performing a manual backup is discussed later in this chapter in the section "Performing Manual Backups."

## Performing System State Backups

To perform a System State backup, users can use the Backup program that ships with Microsoft Windows Server 2003, or they can use third-party software that allows inclusion of System State in the backup set.

Use the following procedure to perform a System State backup:

1. From the Start menu, point to Administrative Tools and click Certification Authority.
2. In the console tree, ensure that Certificate Services is running.



**Note** A System State or manual backup of Certificate Services requires Certificate Services to be running. If Certificate Services is stopped, the backup will fail.

3. Close the Certification Authority console.
4. From the Start menu, point to Programs, point to Accessories, point to System Tools, and click Backup.
5. On the Welcome to the Backup or Restore Wizard page, click Next.
6. On the Backup or Restore page, click Back Up Files and Settings and click Next.
7. On the What to Back Up page, click Let Me Choose What To Back Up and click Next.
8. On the Items to Back Up page, in the console tree, expand My Computer and enable the System State check box.
9. On the Items to Back Up page, click Next.
10. On the Backup Type, Destination, and Name page, provide a file location or tape backup system to use and click Next.

11. On the Completing the Backup or Restore Wizard, click Advanced.
12. On the Type of Backup page, choose a Normal backup and click Next.



**Note** Although it is possible to perform a differential backup of Certificate Services, it is recommended to perform full backups of the Certificate Services database. The size of the System State backup is small enough that it should not affect your decision to use full backups.

13. On the How to Back Up page, enable the Verify Data and Backup check box and click Next.
14. On the Backup Options page, click either Append this Backup to the Existing Backups or Replace the Existing Backups, enable the Allow only the owner and the Administrator access to the backup data and to any backups appended to this medium check box, and then click Next.
15. On the When to Backup page, click Now and click Next.
16. On the Completing the Backup or Restore Wizard, click Finish.

## Performing Manual Backups

Manual backups can be performed from either the Certification Authority console or the command line by using the `certutil.exe` command. There is no technical difference between the results of the two backup methods; the only difference is in how you perform each backup.



**Note** Manual backups are recommended for organizations testing Certificate Services in a lab environment, to allow quick rollback if testing does not go as expected.

## Using the Certification Authority Console

To perform a backup from the Certification Authority console, the user must be assigned the backup files and directories user right—and not hold any other Common Criteria roles.

Use the following procedure to perform the backup:

1. From the Start menu, point to Administrative Tools and click Certification Authority.

2. In the console tree, ensure that Certificate Services is running.
3. In the console tree, right-click *CAName*, point to All Tasks and click Backup CA.
4. On the Welcome to the Certification Authority Backup Wizard page, click Next.
5. On the Items to Backup page, input the following options:
  - **Private key and CA certificate.** Includes the CA's certificate and private key(s) in the backup set. Select this option only if you are using a software CSP. If using a hardware CSP, leave this check box cleared.
  - **Certificate database and certificate database log.** Always select this option to ensure that you include the CA database and log files in the backup set.
  - **Perform incremental backup.** This check box is not usually selected. Full backups of the CA database and log files are recommended instead.
  - **Backup to this location.** Select a folder on the local file system that does not contain any existing data.
6. If the Certification Authority Backup Wizard dialog box appears, click OK to create the location designated on the Items to Backup page.
7. If you choose to back up the private key and CA certificate, open the Select a Password page, type and confirm a password to protect the PKCS #12 file generated by the backup procedure, and click Next.
8. On the Completing the Certification Authority Backup Wizard page, click Finish.

Once the backup is complete, open the folder designated in step 5. In the folder, there is a \*.p12 file (the PKCS #12 backup of the CA's certificate and private key) and a subfolder named Database that contains the backup of the CA database and log files.

## Using Certutil

The certutil command allows you to automate the backup of the CA in a batch file. The batch file can be scheduled by using the Task Scheduler services.

If you are using a software CSP, ensure that the backup set includes both the CA database and the CA's key pair. To do this, use the following procedure:

1. Open a command prompt.
2. At the command prompt, type **net start certsvc** to ensure that Certificate Services is running.
3. Create a folder that will contain the results of the manual backup of the CA database—for example, C:\CABackup.

4. At the command prompt, type **certutil -backup C:\CABackup** and press ENTER.
5. At the command prompt, at the Enter New Password prompt, type a complex password and press ENTER.
6. At the command prompt, at the Confirm New Password Prompt, type the same password again and press ENTER.
7. When the backup is complete, ensure there are no error messages and close the command prompt.

You are providing a password to protect the PKCS #12 file containing the CA's key pair. To create a successful backup of the private key, you must be a local administrator of the computer; to create the backup of the CA database, you can only hold the Common Criteria role of backup operator. In other words, you can only run this command successfully if Common Criteria role separation is not enforced.

If Common Criteria role separation is enforced, you can separate the two backups by running two `certutil` commands.

To backup only the CA database, a backup operator can use the `-backupdb` option, as shown here:

1. Open a command prompt.
2. At the command prompt, type **net start certsvc** to ensure that Certificate Services is running.
3. Create a folder that will contain the results of the manual backup of the CA database—for example, `C:\CABackup`.
4. At the command prompt, type **certutil -backupdb C:\CABackup** and press ENTER.
5. When the backup is complete, ensure there are no error messages and close the command prompt.

Likewise, if you are a local administrator and only want to backup the CA's key pair, you can use the `-backupkey` option to backup the CA's private key and public key to a PKCS #12 file.

1. Open a command prompt.
2. At the command prompt, type **net start certsvc** to ensure that Certificate Services is running.
3. Create a folder that will contain the results of the manual backup of the CA database—for example, `C:\CABackup`.
4. At the command prompt, type **certutil -backupkey C:\CABackup** and press ENTER.

5. At the command prompt, at the Enter New Password prompt, type a complex password and press ENTER.
6. At the command prompt, at the Confirm New Password prompt, type the same password and press ENTER.
7. When the backup is complete, ensure there are no error messages and close the command prompt.

## Other Backup Methods

Rather than performing System State or manual backups, some organizations use alternative methods for disaster recovery. These methods—binary backups and HSM backups—often depend on the role a CA plays in the CA hierarchy and the methods used to protect the CA’s key pair.

### Binary Backups

For offline CAs, some organizations choose to create binary images of the computers. This is done by using disk-imaging software such as Norton Ghost or Symantec Partition Magic. These software packages make a binary-level backup of the computer’s hard disk, allowing for quick CA restoration.



**Note** A binary backup can also require a manual or System State backup. The binary image only includes the CA database state at the time of the backup. A System State or manual restoration still might be required to restore the CA to its last working state.

The advantage of a binary backup is the speed of restoration. Both software packages mentioned earlier allow you to boot from a CD that immediately starts restoration. The disadvantage is the additional security that must be implemented to protect the backup media. If attackers gain access to the backup media, they can create an exact copy of a valid CA to issue invalid certificates.

### HSM Backups

One method that protects a CA’s private key material from being extracted from the Local Machine store by a member of the local Administrators group is to move the CA’s key pair to an HSM. An HSM moves the key pair or a portion of the key material and all cryptographic operations off the CA computer to a secure “black box.” Because the key material is removed from the CA, proprietary methods must be used to back up and restore the CA key material.

For example, if you implement a Rainbow Chrysalis CA3 or Luna SA HSM, the key material is backed up to Luna tokens. The backup process requires the participation of three “key holders,” where each key holder holds a separate PKI management role. The backup ensures that, in the event of HSM failure, the key material can be loaded onto a replacement HSM and, in the event of CA hardware failure, the replacement CA can be connected to the existing key material stored on the HSM.

Likewise, if you implement an nCipher HSM, the key material is protected by a combination of smart card tokens and encrypted files stored on the CA or a remote file system server. The key pair is re-assembled through the combination of a key pair split between a predefined number of operator cards and the encrypted data stored within the CA’s `\nfast\kmdata\local` folder.

## Restoration Procedures

If a CA fails, restore the CA’s System State or manual backup. Before you restore the backup, you must reinstall Certificate Services, using the previous CA certificate and key pair to ensure that Certificate Services is using the same key pair for all signing operations. Once you reinstall Certificate Services, the restoration procedure depends on the CA’s backup method.

### Reinstalling Certificate Services

The first step in restoring the CA computer is to ensure that Certificate Services is installed correctly and can be started and stopped. If you have a good backup of Certificate Services, whether the backup is a System State backup or a manual backup, you must first reinstall Certificate Services using the same certificate and key pair.

To reinstall Certificate Services, ensure that the CA certificate and private key are available to the CA.

- For a software-based CSP, a local administrator of the computer can import a PKCS #12 into the local machine store. You can verify that the certificate is imported successfully by loading the Certificates MMC console focused on the local computer.
- For a hardware-based CSP, such as an HSM, you must install the third-party CSP and utilities before you restore connectivity to the hardware device. Once you restore connectivity, the CA computer can communicate with the HSM and access the CA certificate and key pair.

Once the CA certificate and private key are loaded or accessible to the CA, use the following procedure to install Certificate Services, using the previous CA certificate and private key:

1. From the Start menu, click Control Panel and click Add or Remove Programs.
2. In the Add or Remove Programs window, click Add/Remove Windows Components.
3. In the Windows Components Wizard, in the Windows Components list, select the Certificate Services check box.
4. In the Microsoft Certificate Services dialog box, click Yes.
5. On the Windows Components page, click Next.
6. On the CA Type page, select the previous role of the CA, enable the Use Custom Settings To Generate the Key Pair and CA Certificate check box, and click Next.
7. On the Public and Private Key Pair page, set the following options:
  - CSP: The same CSP as used previously
  - Use an existing key: Enabled
  - Select the certificate with the same CA name as the subject
  - Use the certificate associated with this key: Enabled



**Note** The hash algorithm and key length will automatically populate based on the previous CA certificate.

8. On the Public and Private Key Pair page, click Next.
9. On the CA Identifying Information page, verify that the CA's common name and distinguished name are correct and click Next.
10. On the Certificate Database Settings page, verify that the database, database log, and, if used, shared folder paths are the same as the original CA. Enable the Preserve Existing Certificate Database check box and click Next.



**Note** If you cannot start Certificate Services after reinstalling it with the same certificate and key pair, try reinstalling without enabling the option to preserve the existing certificate database. The problem could be a corrupt CA database or log file. Once you reinstall, you can restore a working version of the CA database and log files from a System State or manual backup.

11. If the Microsoft Certificate Services dialog box appears, click Yes to temporarily stop IIS.
12. If prompted, insert the Windows Server 2003, Enterprise Edition, CD in the CD-ROM drive or point to the media installation point on the network and choose the \i386 folder.
13. On the Completing the Windows Components Wizard page, click Finish.
14. Close the Add or Remove Programs dialog box.
15. From Administrative Tools, open the Certification Authority console.
16. Attempt to start Certificate Services.

If Certificate Services starts, you can proceed to restoring the last System State or manual backup.

## Restoring System State Backups

To restore a System State backup, a user with the operating system restore files and directories user right must restore the System State backup from the backup media. Use the following procedure to restore a System State backup:

1. From the Start menu, point to Programs, point to Accessories, point to System Tools, and click Backup.
2. On the Welcome to the Backup or Restore Wizard page, click Next.
3. On the Backup or Restore page, click Restore Files and Settings and click Next.
4. On the What to Restore page, expand File, expand *FolderName* (where *FolderName* is the folder containing the System State backup), click System State, and click Next.
5. On the Completing the Backup or Restore Wizard, click Advanced.
6. On the Where to Restore page, choose Original Location and click Next.
7. In the Warning dialog box, click OK.
8. On the How to Restore page, click Replace Existing Files and click Next.
9. On the Advanced Restore Options page, enable all active check boxes and click Next.
10. On the Completing the Backup or Restore Wizard, click Finish.
11. When the restoration completes, in the Restore Progress dialog box, click Close.
12. In the Backup Utility dialog box, click Yes to reboot the CA.





**Warning** If you are restoring a System State backup to a domain controller, start the computer in Active Directory Restore Mode. This allows the restoration of the Active Directory database, which is also included in the System State backup for a domain controller. Deploying a domain controller as a CA is not recommended.

## Restoring Manual Backups

A manual backup, whether it was created with certutil or the CA console, can be restored by using the CA console, as follows:

1. From the Start menu, point to Administrative Tools and click Certification Authority.
2. In the console tree, click *CAName*.
3. In the console tree, right-click *CAName*, point to All Tasks and click Restore CA.
4. In the Certification Authority Restore Wizard, click OK to stop Certificate Services during the restore procedure.
5. On the Welcome to the Certification Authority Restore Wizard page, click Next.
6. On the Items to Restore page, enable the Certificate Database and Certificate Database Log check box. If required, enable the Private key and CA certificate check box, and click Browse.
7. In the Browse for Folder dialog box, select the folder that contains the manual backup files and click OK.
8. On the Items to Restore page, click Next.
9. On the Completing the Certification Authority Restore Wizard, click Finish.
10. In the Certification Authority Restore Wizard dialog box, click Yes.
11. Verify that Certificate Services starts successfully.

## Evaluating Backup Methods

Although it is generally recommended to implement System State backups when planning for CA disaster recovery, there are circumstances where it is preferable to perform a manual backup or a combination of a System State and a manual backup.

No matter which method you ultimately choose for protecting your CA, ensure that you perform regular CA backups.

- For online CAs, perform full backups of the CA database nightly. This ensures that, in the event of failure, the worst-case scenario is that you restore to the state at the time of the last full backup.
- For offline CAs, perform full backups each time you access the offline CA. This occurs whenever you publish a new CRL, renew a CA's certificate, or issue new subordinate CA certificates.



**Note** If you restore the previous night's full backup, the CA is not aware of any certificates issued between recovery time and backup time if the log file directory is unavailable. The certificates issued in this time frame *are* valid. The caveat is that you cannot revoke these certificates, as they do not appear in the Certification Authority console. Microsoft has implemented a custom exit module in Certificate Services to allow real-time, centralized logging of all CA transactions to a Microsoft SQL Server database. The information stored in this database allows certificates not included in the CA database due to restoration of the CA database to be identified, allowing the certificate to be revoked. The exit module is discussed in the article "Deploying PKI Inside Microsoft" referenced in the "Additional Information" section of this chapter.

The following sections describe some scenarios for disaster recovery of a CA, as well as recommendations on how to perform CA backup.

## Hardware Failure

If your CA suffers from hardware failure, the action you take depends on the nature of the hardware failure. If you can replace the failed hardware without affecting the operating system or disk files, you can simply replace the hardware and start the CA. If the hardware stores the CA database, the CA logs, or the CA key pair, you can reduce the risk of failure by storing the data on hardware RAID volumes. These hardware configurations prevent the CA from functioning due to the failure of a single disk. Likewise, if your private key is stored on an HSM, maintaining proprietary backups of the HSM and providing redundant hardware can minimize CA downtime.

## Certificate Services Failure

If Certificate Services fails, back up the folders containing the CA database and logs and the CA key pair. On first attempt, try removing and reinstalling Certificate Services by using the existing key pair. The CA reinstallation attempts to use the existing files in the CA database and logs folders. If this attempt fails, reinstall and restore from the latest backup set.



**Note** Ensure that you have included the registry in the backup by including the System State in the backup set or by manually backing up the HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\CANAME registry key.

## Server Replacement

If the server hosting Certificate Services fails due to one or more hardware failures, or if the server hardware does not meet the current processing requirements, an organization might choose to replace the server hosting Certificate Services.



**Note** Some organizations lease their server hardware. Much like the case of server hardware replacement, the replacement of a server due to a lease-hold switch will use the same process described here.

Use the following process to move Certificate Services from one server to another server:

1. Create a manual backup of the CA database, or gain access to the last manual backup of the CA database.
2. Create or gain access to a backup of the CA key pair. If using a software CSP, you can include the key pair in the manual backup. If using an HSM, use the HSM's proprietary method to back up the key pair.
3. In the Registry Editor, export the following registry key: HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\CANAME.
4. Uninstall Certificate Services and remove the CA computer account from the domain.
5. Turn off the existing computer, and remove the computer from the network. Do not reinstall or wipe the computer's hard drive until the restoration to the new computer is verified.
6. Build the replacement computer with the same disk partitioning as the original CA.
7. Ensure that the new computer is assigned the same NetBIOS name as the computer being replaced.
8. If the DNS entries are static entries, ensure that the IP address information for the new computer is the same as used on the computer being replaced.

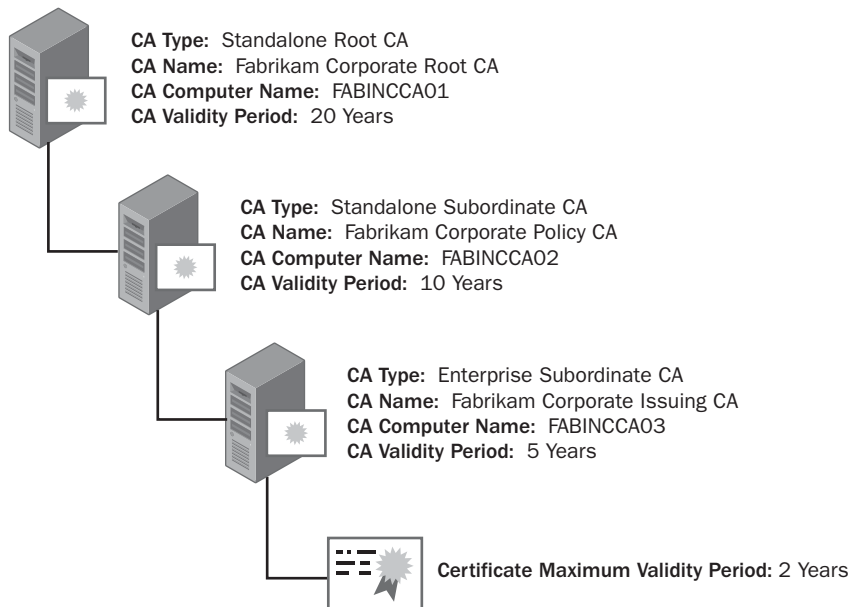
9. If the computer is replacing an enterprise CA, join the new computer to the same domain as the computer being replaced.
10. Ensure that you copy all configuration files for the replaced CA to the local disk of the replacement CA.
11. Copy the original CAPolicy.inf file to the %windir% folder.
12. Reinstall Certificate Services using the existing key pair saved in step 2 of this procedure.
13. Restore the registry file saved in step 3 of this procedure.
14. Restore the manual backup of the CA database.
15. Verify that Certificate Services starts successfully.



**Note** This same process, with minor modifications, also can be used if the computer hosting Certificate Services fails and must be replaced.

## Case Study: Replacing Server Hardware

You manage the team responsible for the day-to-day operations of the CAs in the Fabrikam Inc. network. Fabrikam has a three-tier CA hierarchy, as shown in Figure 11-1.



**Figure 11-1** The Fabrikam Inc. CA hierarchy

## Scenario

The server hosting the Fabrikam Corporate Root CA is five years old and must be replaced due to server hardware errors detected when you attempted to start the server this morning. You must replace the old server hardware with the new server hardware in the next week because the CRL for the Fabrikam Corporate Root CA expires in seven days time.

Before starting the hardware replacement, you gather the following details about the current root CA:

- The root CA computer has two drive partitions:
  - Drive C contains the Windows Server 2003, Standard Edition, operating system in a folder named C:\winnt.
  - Drive D contains the Windows Server 2003 Certificate Services database (D:\CertDB), the database logs (D:\CertLogs), and the shared folder (D:\CAConfig).
- The NetBIOS name of the computer is FABINCCA01.
- The last full backup of the offline root CA was a System State backup performed at the last CRL update 25 weeks ago.
- The root CA uses an HSM. You have the original media for the support software for the HSM.

You must replace the hardware for the root CA without interrupting Certificate Services on the network.

## Case Study Questions

1. When you perform the installation of the replacement root CA computer, can you use the default installation folder for Windows Server 2003?
2. Can you assign the replacement CA computer the NetBIOS name FABINCCA01A to designate that this as the second instance of the root CA computer? Why or why not?
3. Which registry key should you back up on the original CA computer to reduce the replacement CA computer configuration?
4. What type of backup should you perform on the original root CA computer before you start the installation of the replacement CA computer—a System State backup or a manual backup?
5. What software must be installed on the replacement CA computer before you start the installation of Certificate Services? Why?
6. How does the installation of Certificate Services differ from the original installation of Certificate Services?

7. Once the installation of Certificate Services is complete, what must be done to allow the CA to recognize the certificates issued by the CA on the previous computer?
8. What should be done to the original hardware before it is returned to the leasing company?
9. Do you have to republish the root CA certificate in Active Directory once the hardware replacement is complete?

## Additional Information

- Microsoft Official Curriculum, Course 2821: “Designing and Managing a Windows Public Key Infrastructure” ([www.microsoft.com/traincert/syllabi/2821afinal.asp](http://www.microsoft.com/traincert/syllabi/2821afinal.asp))
- “Deploying PKI Inside Microsoft” (<http://www.microsoft.com/technet/itsolutions/msit/security/deppkiin.mspix>)
- “Windows Server 2003 PKI Operations Guide” (<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03pkog.mspix>)
- Knowledge Base Article 231182: “Certificate Authority Servers Cannot Be Renamed or Removed from Network”
- Knowledge Base Article 298138: “HOW TO: Move a Certification Authority to Another Server”
- Knowledge Base Article 313272: “HOW TO: Back Up and Restore a Certificate Authority in Windows 2000”
- Knowledge Base Article 811944: “Computer Does Not Start After You Use Windows Backup to Restore the System State”



**Note** Microsoft Knowledge Base articles can be found at <http://support.microsoft.com>. Enter the article number in the Search the Knowledge Base text box.

## Chapter 12

# Deploying Certificates

Having created certificate templates for your application enabled by a public key infrastructure (PKI), the next step is to determine how to get the certificates to the desired computers, users, or network devices.

A certificate request involves actions performed at the computer where the certificate request is generated and at the certification authority (CA) that issues the certificate to the requestor.

When a certificate request is initiated, the following process (shown in Figure 12-1) takes place:

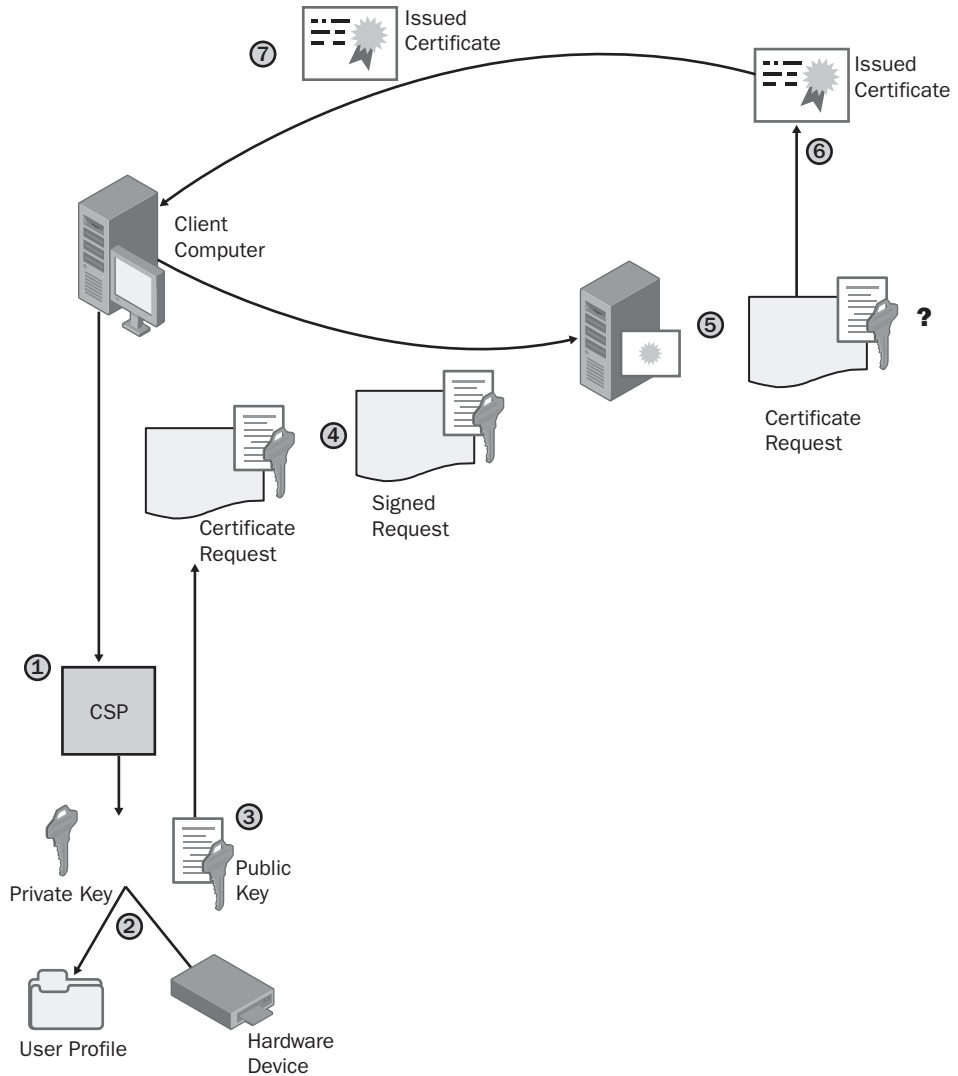
1. The client computer asks the cryptographic service provider (CSP) designated by the certificate template or selected by the user to generate a key pair.
2. The CSP generates a key pair based on the key length designated in the certificate template or selected by the user. If the CSP is software-based, the key pair is generated in the user's profile. If the CSP is for hardware, such as a smart card, the key pair is generated on the hardware device.



**Note** The private key generated by a software CSP is protected by the Data Protection Application Programming Interface (DPAPI). The private key is protected by the user's password in the user's profile.

3. The public key of the key pair is added to the certificate request, along with any other information required by the certificate template or configured by the user.
4. The certificate request is signed by the private key of the key pair and is sent to the CA.
5. The CA issues the requested certificate, denies the request, or causes it to be pending until a certificate manager manually approves or denies it.

6. The certificate is generated at the CA. It includes the subject information either provided in the certificate request or built from information in Active Directory, as well as the public key of the key pair. The certificate is then signed with the CA's signing certificate, and the resulting hash is placed in the certificate's thumbprint extension.
7. The issued certificate is returned to the user and then loaded into the required store in the user's profile or on the hardware device. The certificate is now associated with the private key of the key pair and is ready to use.



**Figure 12-1** The certificate enrollment process



## Certificate Enrollment Methods

Windows Server 2003 Certificate Services provide several methods for enabling certificate enrollment. The methods range from manual methods that are initiated by a user performing the certificate request to automatic methods where the certificate request is initiated by Group Policy or a login script. The available certificate enrollment methods include:

- **Certificate Services Web Enrollment pages.** These Web pages allow a user to request both user and computer certificates from a Web browser. Certificate Services Web Enrollment pages allow the requestor to ask for specific certificate templates from an enterprise CA, submit certificate request files from a network device or another operating system, and check on pending certificate requests.



**Note** Certificate Services Web Enrollment pages can be loaded on the Windows Server 2003 CA or onto a front-end Web server. The following requirements must be met: the Web server is a member of the same forest as the CA; the computer account for the Web server is trusted for delegation; and the Web server is running Internet Information Services (IIS) 6.0 on Windows Server 2003, Standard Edition, or Windows Server 2003, Enterprise Edition.

- **Certificate Request Wizard.** This wizard permits a user to request certificates from an enterprise CA by selecting the enterprise CA and the certificate template, as well as defining additional settings, such as key length and CSP. The wizard can be launched from the Certificates console.



**Note** The Certificate Request Wizard is only available if the client computer is a member of the same forest as the enterprise CA.

- **Smart Card Enrollment Station.** Certificate Services Web Enrollment pages provide a mechanism for enrolling smart card certificates. The Smart Card Enrollment section of the Web Enrollment pages allows an enrollment agent to request smart card certificates on behalf of other users at a computer referred to as the smart card enrollment station. Once the enrollment agent confirms the requestor's identity, it can request a smart card certificate on behalf of the user.



**Note** Defining and securing the enrollment agent process is discussed in greater detail in Chapter 15, “Smart Card Deployment.”

- **Automatic Certificate Request Settings (ACRS).** This Group Policy setting allows the automatic deployment of version 1 computer certificates to computer accounts in the forest. The computer account must be in the domain or organizational unit (OU) where the Automatic Certificate Request Settings is defined. In addition, the computer account must belong to a group that is assigned the Read and Enroll permissions for the version 1 certificate template.
- **Autoenrollment Settings.** This combination of version 2 certificate templates and Group Policy settings allows automatic deployment of version 2 certificates to users and computers. All computers or user accounts within the domain or OU where the Autoenrollment Settings Group Policy setting is applied automatically receive any published version 2 certificate templates to which the user or computer account is assigned Read, Enroll, and Autoenroll permissions. Autoenrollment can be used for initial certificate deployment, as well as for certificate renewal.



**Note** For user and computer autoenrollment, the client computer must be running Windows XP or Windows Server 2003. Windows 2000 client computers do not recognize the Autoenrollment Settings Group Policy setting.

- **Certreq.exe.** This command-line utility allows a user to submit, retrieve, create, and accept certificate requests sent to a Windows Server 2003 CA. The requests can be sent to both standalone and enterprise CAs.
- **Custom scripting.** In some cases, such as when you want to automate user certificate enrollment at Windows 2000 client computers, you must create custom scripts. These scripts can use the CryptoAPI, CryptoAPI COM (CAPICOM) control, and the Certificate Enrollment Control (xenroll.dll) to automate enrollment at a Windows 2000 computer.
- **Simple Certificate Enrollment Protocol (SCEP).** SCEP is a Cisco proprietary protocol that allows Cisco Internetwork Operating System (IOS) devices to contact a CA, obtain IPsec certificates, and install trusted root certificates. SCEP requires that the Windows CA be configured to enable the SCEP protocol.



**Note** The SCEP installation file (cepsetup.exe) is available for download at [www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=9f306763-d036-41d8-8860-1636411b2d01](http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=9f306763-d036-41d8-8860-1636411b2d01) and can be used by any device that supports SCEP enrollment.

## Choosing an Enrollment Method

For each PKI-enabled application, you must choose the best way to deploy certificates to users, computers, and network devices. In most cases, you'll have a primary method and a secondary method.

### Choosing Among Manual Enrollment Methods

Manual enrollment is not well suited for mass certificate deployment because of the amount of time an organization must spend training personnel to use such a method. Table 12-1 shows the available manual enrollment methods for version 1 and version 2 certificate templates on Windows 2000, Windows XP, and Windows Server 2003 client computers.

**Table 12-1 Manual Enrollment Methods**

<b>Enrollment Method</b>	<b>Certificates MMC</b>	<b>Web Enrollment</b>
Manual enrollment on a Windows 2000 workstation	V1 template: Yes V2 template: No	V1 template: Yes V2 template: Yes
Manual enrollment on a Windows XP or Windows Server 2003 workstation	V1 template: Yes V2 template: Yes	V1 template: Yes V2 template: Yes
Request a certificate template that is pending for certificate manager approval	V1 template: No V2 template: No	V1 template: Yes V2 template: Yes

### Choosing Among Automatic Enrollment Methods

Autoenrollment lowers the cost of a PKI by reducing the time and effort required to deploy certificates. Table 12-2 shows the automatic enrollment methods available for common deployment scenarios.

**Table 12-2 Automatic Enrollment Methods**

Enrollment Method	ACRS	Autoenrollment Settings	Scripting
Automatic deployment of certificates to computers	V1 template: Yes	V1 template: No	V1 template: Yes
	V2 template: No	V2 template: Yes	V2 template: Yes
Automatic deployment of certificates to users	V1 template: No	V1 template: No	V1 template: Yes
	V2 template: No	V2 template: Yes	V2 template: Yes
Automatic renewal of expired certificates	V1 template: Yes	V1 template: No	V1 template: Yes
	V2 template: No	V2 template: Yes	V2 template: Yes

## Publishing Certificate Templates for Enrollment

Before enrolling a certificate manually, automatically, or through a scripting method, you must ensure that the certificate templates are available for enrollment at a CA. This process is known as “publishing the certificate template at the CA.”

The following procedure publishes a certificate template:

1. Log on at the CA computer as a user assigned the CA administrator role.
2. From Administrative Tools, open the Certification Authority console.
3. In the console tree, expand *CAName* (where *CAName* is the logical name of the CA) and click Certificate Templates.
4. In the console tree, right-click Certificate Templates, point to New and click Certificate Template to Issue.
5. In the Enable Certificate Templates dialog box, select one or more certificate templates not currently published at the CA and click OK.



**Note** Version 2 certificate templates are only available if the enterprise CA is running Windows Server 2003, Enterprise Edition, or Windows Server 2003, Data Center Edition. If the enterprise CA is running Windows Server 2003, Standard Edition, the Enable Certificate Templates dialog box only displays the available version 1 certificate templates.

Once you add the certificates, they are available for enrollment. The list of published certificate templates is defined on a CA-by-CA basis, allowing the availability of different certificate templates at each enterprise CA in the CA hierarchy.

If you want to remove a certificate template, select the certificate template or templates in the details pane and press Delete. After confirming the deletion, the certificate templates are no longer available for enrollment.

## Scripting the Publishing of Certificate Templates

---

Alternatively, you can use the `certutil` command to add or remove certificate templates from a CA. For example, the following script sample removes the default certificate templates and publishes only the Basic Encrypting File System (EFS), CA Exchange, EFS Recovery Agent, and Key Recovery Agent certificate templates:

```
::Remove the default templates for a W2K3 CA.
certutil -SetCAtemplates -Administrator
certutil -SetCAtemplates -DirectoryEmailReplication
certutil -SetCAtemplates -DomainControllerAuthentication
certutil -SetCAtemplates -EFSRecovery
certutil -SetCAtemplates -EFS
certutil -SetCAtemplates -DomainController
certutil -SetCAtemplates -WebServer
certutil -SetCAtemplates -Machine
certutil -SetCAtemplates -User
certutil -SetCAtemplates -SubCA

:Publish the required certificate templates

certutil -SetCAtemplates +EFS
certutil -setCAtemplates +KeyRecoveryAgent
certutil -setCAtemplates +EFSRecovery
certutil -setCAtemplates +CAExchange
```

As shown here, the `certutil -setCAtemplates` command can either add templates (+Template name) or remove templates (-Template name). You can use this command in a batch file to define the exact set of certificate templates that must be published at a specific CA.

## Performing Manual Enrollment

The sections that follow detail the procedures for requesting certificates from a Windows Server 2003 CA. A Certificate Services installation includes the Certificate Services Web Enrollment pages. The Web pages are only accessible if Internet Information Services (IIS) 6.0 is also installed at the CA.



**Note** The IIS 6.0 installation must enable Active Server Pages (ASP) for Certificate Services Web Enrollment pages installation.



**Note** If you did not install IIS 6.0 before you install Certificate Services, you must install IIS 6.0 and then type **certutil -vroot** at a command prompt to create the required virtual roots and file shares required by the Certificate Services Web Enrollment pages.

## Requesting a Certificate

Use the following procedure to request a certificate from the Certificate Services Web Enrollment pages:

1. Open Internet Explorer.
2. In Internet Explorer, open the URL *http://CertServerDNS/certsrv* (where *CertServerDNS* is the Domain Name System [DNS] name of the Windows Server 2003 CA).



**Note** The Certificate Server's DNS name should be added to the Local intranet site at all computers. If the Web site is not added to the Local intranet site, users are prompted for their user name and password. The process of adding the DNS name to the Local intranet site is described in Chapter 15, "Smart Card Deployment."

3. On the Welcome page, click the Request a certificate link.
4. On the Request a Certificate page, click the Advanced Certificate Request link.



**Note** This page only appears if the User certificate template is published at the CA. If the User certificate template is not published, step 4 does not occur.

5. On the Advanced Certificate Request page, click the Create and Submit a Request to this CA link.

6. On the Advanced Certificate Request page (see Figure 12-2), you can define the following options for the certificate request:

The screenshot shows a web browser window titled "Microsoft Certificate Services - Microsoft Internet Explorer". The address bar shows "Microsoft Certificate Services - Komar Consulting Issuing CA". The main content area is titled "Advanced Certificate Request".

**Certificate Template:** A dropdown menu is set to "User".

**Key Options:**

- Create new key set  Use existing key set
- CSP: Microsoft Enhanced Cryptographic Provider v1.0
- Key Usage:  Exchange
- Key Size: 1024 (Min: 384, Max: 1024, Common key sizes: 512 1024 2048 4096 8192 16384)
- Automatic key container name  User specified key container name
- Mark keys as exportable
- Export keys to file
- Enable strong private key protection
- Store certificate in the local computer certificate store  
*Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.*

**Additional Options:**

- Request Format:  CMC  PKCS10
- Hash Algorithm: SHA-1  
*Only used to sign request.*
- Save request to a file
- Attributes: (empty list)
- Friendly Name: User

A "Submit" button is located at the bottom right of the form.

**Figure 12-2** The Advanced Certificate Request page

- **Certificate template drop-down list.** Lists the certificate templates for which the user is assigned Read and Enroll permissions.
- **Key set.** Allows you to choose between generating a new key set or using the existing key set.
- **CSP drop-down list.** Allows you to select a CSP installed on the client computer to use for the certificate request.
- **Key size.** The length of the key pair generated for the certificate request.
- **Container name.** The key container where the certificate's key pair is stored.
- **Export options.** Allows you to request that the certificate's private key be exportable.
- **Strong key protection.** Requires a password each time the certificate's private key is accessed.

- **Store certificate in the local computer store.** Enable this option for computer certificates only, not for user certificates.
- **Request format.** You can choose between Certificate Management Message over Cryptographic Message Syntax (CMC) or Public Key Cryptography Standards (PKCS) #10 request formats. CMC is required for digitally signed requests and key archival requests.
- **Friendly name.** A logical name assigned to the certificate. This name is not part of the certificate. Rather, it is the logical display name when the certificate is viewed with Microsoft tools that can be changed without invalidating the signature applied to the certificate.



**Note** The default values shown on the Advanced Certificate Request page are based on the values defined in the certificate template.

7. Once all options are defined, click Submit on the Advanced Certificate Request page.
8. In the Potential Scripting Violation dialog box, allow the Web site to request a certificate on your behalf by clicking Yes.
9. On the Certificate Issued page, click the Install this Certificate link.
10. In the Potential Scripting Violation dialog box, accept that the Web site is adding a certificate to your computer by clicking Yes.
11. Ensure that the Certificate Installed page appears, indicating that the certificate has installed successfully.
12. Close Internet Explorer.



**Note** Microsoft Knowledge Base Article "Flaw in Certificate Enrollment Control May Cause Digital Certificates to Be Deleted" describes the MS02-048 security update, which introduced the Potential Scripting Violation dialog box. This dialog box warns the user anytime a certificate request is submitted to a CA or a CA-issued certificate is installed in the user's store.

## Retrieving a Pending Certificate Request

If the the CA Certificate Manager Approval option in the certificate template is enabled on the Issuance Requirements tab, the certificate request becomes pending until a certificate manager performs requestor validation. Once the certificate man-



ager verifies identity and issues the certificate, you can complete certificate installation as follows:

1. Open Internet Explorer at the same computer where the original request was submitted.
2. In Internet Explorer, open the URL *http://CertServerDNS/certsrv* (where *CertServerDNS* is the DNS name of the Windows Server 2003 CA).
3. On the Welcome page, click the View the Status of a Pending Certificate Request link.
4. On the View the Status of a Pending Certificate Request page, click the link for the pending certificate.



**Note** The computer where the certificate request is performed must have cookies enabled. If cookies are not enabled, the View the Status of a Pending Certificate Request page does not show any entries.

5. On the Certificate Issued page, click the Install this Certificate link.
6. In the Potential Scripting Violation dialog box, accept that the Web site is adding a certificate to your computer by clicking Yes.
7. Ensure that the Certificate Installed page appears, indicating that the certificate has installed successfully.
8. Close Internet Explorer.



**Note** If cookies are disabled in Internet Explorer, you cannot retrieve a pending certificate request.

### Submitting a Certificate Request from Network Devices

In some cases, the certificate request is generated at a network device or in another operating system, such as Linux. In these cases, the certificate request is commonly generated in a PKCS #10 format. Certificate Services Web Enrollment pages provide a facility to submit the PKCS #10 certificate request and issue a certificate based on the subject information and public key in the request.

Use the following procedure to request a certificate with a PKCS #10 file created by a network device or alternate operating system.

1. Open Internet Explorer.
2. In Internet Explorer, open the URL *http://CertServerDNS/certsrv* (where *CertServerDNS* is the DNS name of the Windows Server 2003 CA).
3. In the Welcome page, click the Request a Certificate link.
4. On the Request a Certificate page, click the Advanced Certificate Request link.
5. On the Advanced Certificate Request page, click the Submit A Certificate Request By Using A Base-64-Encoded CMC Or PKCS #10 File, Or Submit A Renewal Request By Using A Base-64-Encoded PKCS #7 File link.

## Reviewing the Certificate Request

A certificate manager should not accept any PKCS #10 request file without first reviewing the certificate request's contents. The `certutil` command allows you to review the contents by running `certutil -dump request.req` (where *request.req* is the name of the PKCS #10 request file).

```
402.203.0: 0x80070057 (WIN32: 87): ..CertCli Version
PKCS10 Certificate Request:
Version: 1
Subject:
    CN=Andy Ruth

Public Key Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.1 RSA
    Algorithm Parameters:
        05 00
Public Key Length: 1024 bits
Public Key: UnusedBits = 0
    0000 30 81 89 02 81 81 00 bc d6 cc 13 34 21 1e c9 dd
    0010 48 84 92 5b bf 7b 4e 1b 87 f8 3a 8e 9e 23 6c ce
    0020 5f 01 c5 3b 4a 01 5f b2 bb 67 3a 67 5f d7 76 15
    0030 78 f4 d8 f1 ba 3a b3 ab 56 69 bd e3 0d 39 22 f7
    0040 a4 18 96 61 c2 ee 12 b4 63 ba ee 04 cf ad fe d4
    0050 08 5e 95 51 44 3d 76 38 5c 00 77 c6 0e 7d 7b dd
    0060 96 58 70 8f 82 51 95 9b 75 be 45 a0 ea d3 a8 0a
    0070 52 5c 97 8e a4 c4 48 1a 4f 0f bd f9 20 a2 70 de
    0080 2f a9 22 6e a7 58 a5 02 03 01 00 01

Request Attributes: 4
4 attributes:

Attribute[0]: 1.3.6.1.4.1.311.13.2.3 (OS Version)
    Value[0][0]:
        5.1.2600.2

Attribute[1]: 1.3.6.1.4.1.311.21.20 (Client Information)
    Value[1][0]:
        Unknown Attribute type
        Client Id: = 1
        XECI_XENROLL -- 1
        User:
```

Machine: London.corp.microsoft.com  
Process: cscript

```
Attribute[2]: 1.2.840.113549.1.9.14 (Certificate Extensions)
Value[2][0]:
Unknown Attribute type
Certificate Extensions: 5
2.5.29.15: Flags = 1(Critical), Length = 4
Key Usage
    Digital Signature, Non-
Repudiation, Key Encipherment, Data Encipherment
(f0)

1.2.840.113549.1.9.15: Flags = 0, Length = 37
SMIME Capabilities
[1]SMIME Capability
    Object ID=1.2.840.113549.3.2
    Parameters=02 02 00 80
[2]SMIME Capability
    Object ID=1.2.840.113549.3.4
    Parameters=02 02 00 80
[3]SMIME Capability
    Object ID=1.3.14.3.2.7
[4]SMIME Capability
    Object ID=1.2.840.113549.3.7

2.5.29.14: Flags = 0, Length = 16
Subject Key Identifier
    7c 4e b0 7b ca b7 c1 66 a8 b5 c2 15 83 84 f2 7d a1 eb 43 ac

2.5.29.37: Flags = 0, Length = c
Enhanced Key Usage
    Client Authentication (1.3.6.1.5.5.7.3.2)

1.3.6.1.4.1.311.20.2: Flags = 0, Length = 16
Certificate Template Name
    ClientAuth
```

```
Attribute[3]: 1.3.6.1.4.1.311.13.2.2 (Enrollment CSP)
Value[3][0]:
Unknown Attribute type
CSP Provider Info
KeySpec = 1
Provider = Microsoft Enhanced Cryptographic Provider v1.0
Signature: UnusedBits=0
0000 9f f8 46 13 93 4c a4 79 bb 10 82 53 70 12 b9 8f
0010 48 05 8b 76 07 c8 8c d1 db 78 71 e3 44 c3 a3 2b
0020 c5 43 01 6d 15 1b c2 d3 aa 29 3f f5 3c 43 8a fa
0030 e1 2d 6a 71 da 26 ff 97 a7 58 59 73 d8 db 8d 53
0040 e7 25 3a bf 21 16 d5 1b 1c bc f7 1e 83 de 3e 92
0050 0a f0 70 d0 b5 9a 11 79 44 7f d6 aa 4d 70 4d cd
0060 25 83 9f 3a 3c 59 30 03 d0 05 24 1b 19 74 5e 24
0070 76 7e 76 8f cb 39 14 48 66 19 84 45 d8 08 b0 0d
0080 00 00 00 00 00 00 00 00

Signature Algorithm:
```

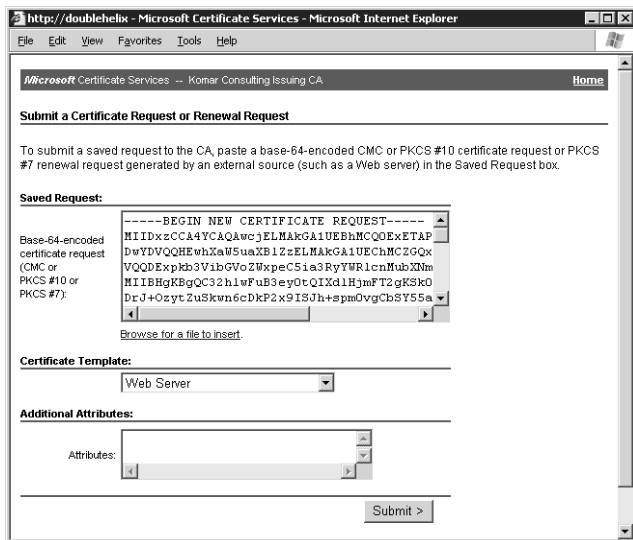
```

Algorithm ObjectID: 1.2.840.113549.1.1.5 sha1RSA
Algorithm Parameters:
05 00
Signature: UnusedBits=0
0000 31 84 ff 5d e4 0f 32 69 27 ca e4 fb 6a 34 f9 9c
0010 53 6e ac d0 80 98 19 ba d6 55 8f 9f 7b dd 2c 0e
0020 32 a6 cc 18 0e 34 2f a3 dc 11 49 e3 54 69 08 ad
0030 fa 15 8e 52 7b 16 b4 ad 98 bc 4f 0d 00 7a 20 29
0040 a8 ac e2 c6 48 d6 c7 e7 dd 77 9a 0b 37 f9 ef 77
0050 09 b1 28 01 f6 a1 40 12 2e a8 98 9d 16 b9 99 ff
0060 8b b3 59 0d ac 50 ca 8a 1f d5 8c 38 ac 92 a8 71
0070 28 f0 34 07 dc fb d2 68 4e ee d7 fc 5a 34 9b 11
Signature matches Public Key
Key Id Hash(sha1): 7c 4e b0 7b ca b7 c1 66 a8 b5 c2 15 83 84 f2 7d a1 eb
43 ac
CertUtil: -dump command completed successfully.

```

Before submitting the PKCS #10 request file to the CA, ensure that the subject information is correct, the correct key length and certificate template are selected, and the signature matches the public key. If these conditions are met, you can submit the certificate request to the CA.

- On the Submit a Certificate Request or Renewal Request page, right-click the Saved Request box and click Paste. (See Figure 12-3.) Ensure that the Certificate Template drop-down list is set to the required certificate template and click Submit.



**Figure 12-3** Submitting a PKCS #10 certificate request file



**Note** If the certificate is for a Secure Sockets Layer (SSL) accelerator or a third-party Web server, choose the Web Server certificate template.

If the certificate request is generated by a Cisco virtual private network (VPN) client, choose the User certificate template.

7. On the Certificate Issued page, select Base-64 encoded or DER encoded and click the Download Certificate or Download Certificate Chain link.
8. In the File Download dialog box, click Save.
9. In the Save As dialog box, select a folder and file name for the certificate and click Save.
10. Close Internet Explorer.

The issued certificate now must be installed on the network device or on the other operating system. The process to select depends on the network device or operating system where the PKCS #10 request file was generated.

## Using the Certificate Request Wizard

Another method of manually requesting a certificate is to use the Certificate Request Wizard. The Certificate Request Wizard can be used by Windows 2000, Windows XP, and Windows Server 2003 domain members when requesting certificates from an enterprise CA.



**Note** The Certificate Request Wizard does not show the same certificates when run from Windows 2000 versus Windows XP and Windows Server 2003. A Windows 2000 client computer only shows the available version 1 certificate templates, whereas Windows XP and Windows Server 2003 show all the available version 1 and version 2 certificate templates.

## Loading the Certificates MMC Console

The Certificate Request Wizard is launched from the Certificates MMC console focused on either the current user or the local machine. The following procedure allows you to request a certificate with the Certificate Request Wizard:

1. Open an empty MMC console.
2. From the File menu, click Add/Remove Snap-in.



**Note** If you are using Windows 2000, replace the File menu with the Console menu.

3. In the Add/Remove Snap-in dialog box, click Add.
4. In the Add Standalone Snap-in dialog box, in the Available Standalone Snap-ins list, select Certificates and click Add.
5. In the Certificates Snap-in dialog box, click My User Account to request a user certificate or Computer Account to request a computer certificate.
6. If you selected Computer Account, in the Select Computer dialog box, click Local Computer (The Computer this Console Is Running On) and click Finish. If you selected My User Account, click Finish.
7. In the Add Standalone Snap-in dialog box, click Close.
8. In the Add/Remove Snap-in dialog box, click OK.



**Tip** If you are using Windows XP or Windows Server 2003, you can run `certmgr.msc` to launch the Certificates console focused on the current user.

## Requesting a Certificate

Once you load the Certificates console, you can request a certificate by using the Certificate Request Wizard. Use the following procedure to request a certificate:

1. In the console tree, expand Certificates - Current User or Certificates (Local Computer), expand Personal, and click Certificates.
2. In the console tree, right-click the Personal folder, point to All Tasks and click Request New Certificate.
3. In the Certificate Request Wizard, click Next.
4. On the Certificate Types page, select the certificate template you want to request. The list is limited to the certificate templates for which either the current user or local machine have Read and Enroll permissions. Once you select the certificate template, click Next.
5. On the Certificate Friendly Name and Description page, in the Friendly Name box, type a descriptive name for the requested certificate and click Next.

6. On the Completing the Certificate Request Wizard page, click Finish.
7. In the Certificate Request Wizard message box, click OK.

If the certificate request is successful, the certificate appears in the details pane.

## Performing Automatic Enrollment

The Windows Server 2003 PKI provides two methods for automatically deploying certificates to users and computers:

- Automatic Certificate Request Settings
- Autoenrollment Settings

The sections that follow discuss the best uses and implementation for each automated enrollment method.

### Automatic Certificate Request Settings

ACRS is an automated enrollment process that is available in Windows 2000 Certificate Services and remains available in Windows Server 2003 Certificate Services. ACRS provides a method to automatically distribute certificates, but the supported scenarios are limited:

- Certificates can be distributed to Windows 2000, Windows XP, and Windows Server 2003 computers that are domain members.
- Only version 1 certificate templates can be distributed.
- Certificates cannot be distributed to user accounts.

Although limited, ACRS is useful for distributing Computer or IPSec certificates to all computers in a domain. To enable ACRS:

1. From Administrative Tools, open Active Directory Users and Computers.
2. In the console tree, right-click the domain or OU where you want to implement the Automatic Certificate Request Settings Group Policy setting and click Properties.



**Note** You can also define the ACRS Group Policy setting at a site by using the Active Directory Sites and Services console.

3. In the *DomainName* or *OUName* Properties dialog box, on the Group Policy tab, create and edit a new Group Policy Object (GPO), or link and edit an existing GPO.
4. In the Group Policy Object Editor, expand Computer Configuration, expand Windows Settings, expand Security Settings, expand Public Key Policies, and click Automatic Certificate Request Settings.
5. In the console tree, right-click Automatic Certificate Request Settings, point to New, and click Automatic Certificate Request.
6. In the Automatic Certificate Request Setup Wizard, click Next.
7. In the Certificate Template page, in the list of available certificate templates, choose the version 1 certificate template for computers to you want to deploy automatically, and click Next.
8. In the Automatic Certificate Request Setup Wizard, click Finish.

## Autoenrollment Settings

Autoenrollment Settings is a combination of Group Policy settings and version 2 certificate templates. The combination allows the client computer running Windows XP, Professional, or Windows Server 2003 to enroll user or computer certificates automatically.



**Note** Autoenrollment Settings is not supported for a user with Windows 2000, Professional, or Windows 2000 Server. Only Windows XP and Windows Server 2003 domain members recognize the Autoenrollment Settings Group Policy setting.

## Configuring Certificate Templates

Autoenrollment Settings require use of version 2 certificate templates.



**Note** Version 2 certificate templates can be issued by enterprise CAs running on Windows Server 2003, Enterprise Edition, or Windows Server 2003, Datacenter Edition, only.

To enable autoenrollment in a version 2 certificate template, make the following modifications to the certificate template:



- **Security tab.** Assign Read, Enroll, and Autoenroll permissions to the user, computer account, or group to which you want to deploy the certificate. If you use groups, assign the permissions to either global or universal groups.



**Tip** You should not assign certificate template permissions to a domain local group. The certificate template objects exist in the Configuration naming context, which is replicated to all domain controllers in the forest. If you use a domain local group, the group is only recognized in the forest root domain.

- **Request Handling tab.** If a certificate template is enabled for autoenrollment, you must decide how the user interacts with the autoenrollment process. If you do not want any user involvement, choose the Enroll subject without requiring any user input option. If you are using a smart card CSP, you require an ability to inform the user to put the smart card into the smart card reader. To enable this interaction, choose the Prompt the user during enrollment option.



**Note** You also must enable the Prompt the User During Enrollment option if you enable signing of the certificate request on the Issuance Requirements tab. Doing this allows the user to select the correct signing certificate before submitting the certificate request.

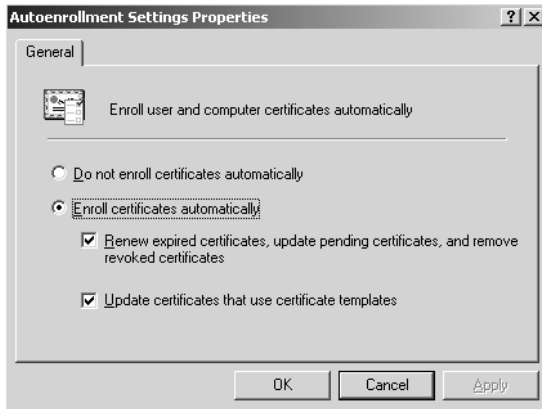
After autoenrollment has been enabled in the version 2 certificate template, the certificate template is ready to be published at a CA for enrollment.

## Configuring Group Policy

Once you define the certificate templates to be deployed with autoenrollment, you must implement a Group Policy setting at the domain or OU where the user or computer account exists. In either case, you must modify the Autoenrollment Settings policy in the following Group Policy locations:

- **Computer autoenrollment:** Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Autoenrollment Settings
- **User autoenrollment:** User Configuration\Windows Settings\Security Settings\Public Key Policies\Autoenrollment Settings

The same dialog box appears for both User and Computer autoenrollment when you double-click Autoenrollment Settings in the details pane. (See Figure 12-4.)



**Figure 12-4** The Autoenrollment Settings Properties dialog box

The options that must be enabled in the Autoenrollment Settings Properties dialog box are:

- **Enroll certificates automatically.** Enables certificate autoenrollment for the domain or OU where the GPO is linked.
- **Renew expired certificates, update pending certificates, and remove revoked certificates.** Enables certificate autoenrollment for certificate renewal, issuance of pending certificates, and removal of revoked certificates from the subject's certificate store.
- **Update certificates that use certificate templates.** Enables autoenrollment for superseded certificate templates.

## Performing Scripted Enrollment

This section will look at the Certreq.exe utility, which is included with Windows XP and Windows Server 2003, and the process of creating custom scripts based on the Certificate Enrollment Control for certificate deployment to users and computers.

### Certreq.exe

The Certreq.exe utility allows you to create batch files that can submit, retrieve, and accept certificate requests submitted to standalone and enterprise CAs. The primary switches used with the Certreq.exe for certificate enrollment are:

- **Certreq –new *Policyfile.inf RequestFile.req.*** Creates a certificate request file (*RequestFile.req*) based on the inputs provided in the *Policyfile.inf* file. The format of the *Policyfile.inf* file is shown here:

```
[NewRequest]
  PrivateKeyArchive = FALSE
  KeyLength = 1024
  SMIME = TRUE
  Exportable = TRUE
  UserProtected = FALSE
  KeyContainer = "..."/>

```

```
[RequestAttributes]
CertificateTemplate=User
```



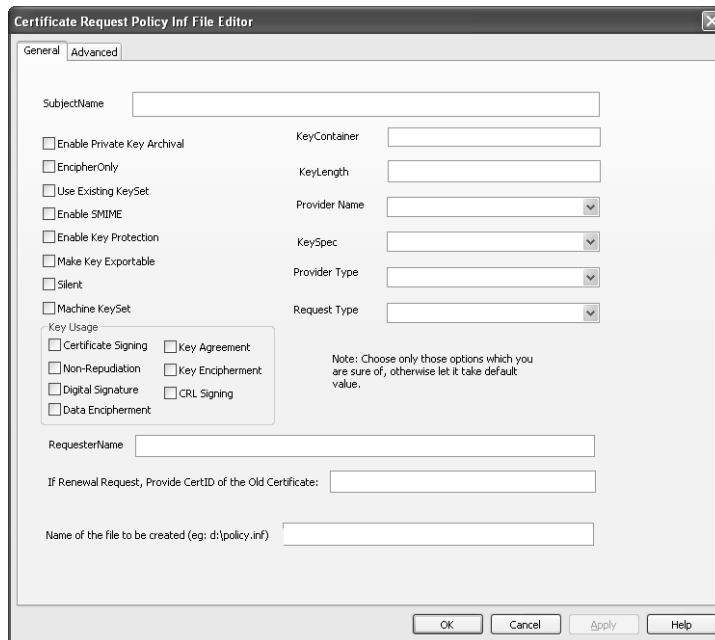
**Note** There are additional settings that can be implemented in the *Policy-File.inf* file, but the other settings are more likely to be required when you submit a certificate request to a standalone CA. When you submit the request to an enterprise CA, most of these additional settings are defined in the certificate template properties.

- **Certreq –submit –config *CADNSName\CALogicalName RequestFile.req.*** Submits the certificate request file to the designated enterprise CA. The command returns the request ID of the submitted certificate request.
- **Certreq –retrieve –config *CADNSName\CALogicalName RequestID Certfile.cer.*** Retrieves the issued certificate from the designated CA. The issued certificate is stored to the local file system in the designated *Certfile.cer*.
- **Certreq –accept *Certfile.cer.*** Ties the returned certificate to the private key generated during the creation of the certificate request file. Once accepted, the certificate can be used for the intended encryption or signing operations.

## Another Tool for Generating PolicyFile.inf

The compact disc with this book includes the RequestEditor.exe utility and associated files. The utility provides a graphical interface for creating the PolicyFile.inf file, which is used to generate a certificate request file.

RequestEditor.exe can be used to generate both CAPolicy.inf files and a .inf file for creating user or computer certificate request files. On the General tab, you can select the more common settings for a certificate request. (See Figure 12-5.)



**Figure 12-5** Creating PolicyFile.inf with RequestEditor.exe

If you are submitting a request to an enterprise CA, the generated PolicyFile.inf requires minor editing. You must add the [RequestAttributes] section indicating which certificate template is being requested. For example, if you wanted to request the User certificate template, you would add the following section at the bottom of the PolicyFile.inf file:

```
[RequestAttributes]
CertificateTemplate=User
```

## Custom Scripting

The Certreq.exe is more restricted on Windows 2000. For Windows 2000 clients, it is preferable to create custom scripts that automate the certificate request process. The scripts you develop use a combination of these development tools:

- **CryptoAPI.** Provides a set of functions that allow applications to programmatically encrypt or digitally sign data.
- **CAPICOM.** A reduced set of APIs that enables applications to encrypt or digitally sign data with far less code than CryptoAPI. In addition, CAPICOM uses the Component Object Model (COM), which allows scripting of CryptoAPI instructions.



**Note** CAPICOM requires Capicom.dll to be registered at all participating client computers.

- **Certificate Enrollment Control.** This control provides two COM interfaces to a Distributed Component Object Model (DCOM) server for generating certificate requests: the ICEnroll interface is primarily used by automation languages, such as Visual Basic, whereas the IEnroll interface is primarily used when developing in C++.
- **Certificate Request Control.** The Certificate Request Control is used to submit the certificate request generated by the Certificate Enrollment Control. The Certificate Request Control uses the ICertRequest2 COM interface to send the requests to the designated CA and receive the returned certificate.



**More Info** For more information on scripting using the Certificate Enrollment Control and the Certificate Request Control, see the article “Creating Certificate Requests Using the Certificate Enrollment Control and CryptoAPI” by David Hoyle referenced in the “Additional Information” section of this chapter.

## Sample Scripts

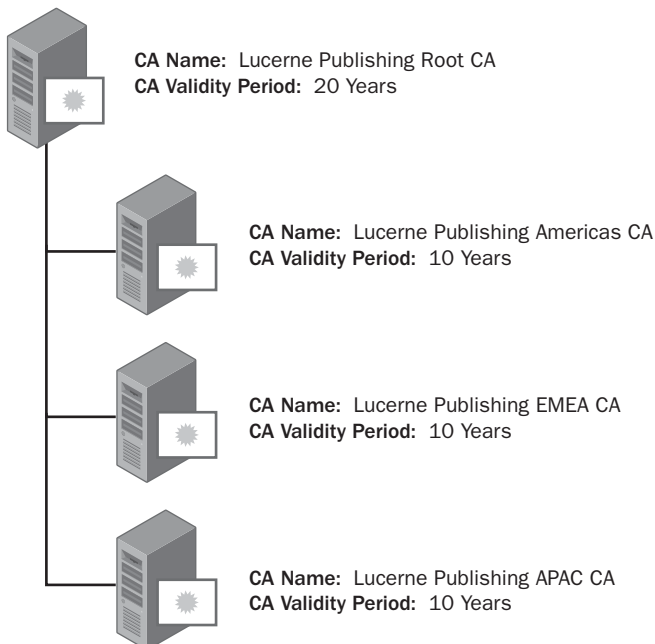
The actual coding of scripted solutions for certificate enrollment and certificate store queries are beyond the scope of this book. Two sample scripts are included on the compact disc with this book, however. They are:

- **Ctool.vbs.** The ctool.vbs script utilizes CAPICOM to query the contents of a certificate store. The tool can list certificates in the designated certificate store that match the search criteria. The tool also can be used to add and remove certificates from the designated certificate store.
- **Enroll.vbs.** The enroll.vbs script utilizes both CAPICOM and the Certificate Enrollment Control to generate certificate requests and submit the requests to the designated CA.

Both scripts can be executed by running `cscript ctool.vbs options` or `cscript enroll.vbs options`. For a complete list of options, run `cscript enroll.vbs /?`.

## Case Study: Selecting a Deployment Method

You are the PKI administrator for your organization, Lucerne Publishing. Lucerne Publishing has just deployed an enterprise PKI, with issuing CAs at each major hub on the network. The Lucerne Publishing CA hierarchy is shown in Figure 12-6.



**Figure 12-6** The Lucerne Publishing CA hierarchy

Lucerne Publishing deploys a single domain forest, LucernePublish.msft, with all Windows 2000, Windows XP, and Windows Server 2003 computers configured as domain members.

## Scenario

You identify several upcoming projects that require the deployment of certificates to users, computers, and network devices on the Lucerne Publishing network. You must recommend to management which enrollment method to use to deploy the certificates for each application.

The following projects require certificate deployment:

- **Code signing.** Lucerne Publishing implements several Microsoft Excel spreadsheets that track a new book's development process. The spreadsheets use several macros that require lowering macro security to a medium level. By signing the macros, Lucerne Publishing can increase the macro security to the highest level. Code signing certificates are to be issued only to the three members of the Quality Assurance team so that the macros are signed after extensive testing. The certificate template requires that the certificates be issued only after a face-to-face interview with the certificate manager.
- **EFS encryption.** An acquisition editor's laptop was recently stolen. The laptop contained information on the upcoming publishing schedule. Lucerne Publishing wants to protect all critical data on its Windows 2000 and Windows XP laptops by implementing EFS encryption. EFS certificates must be deployed to users automatically, and all recovery is to be performed by an EFS recovery agent. The same two EFS recovery agents are to be deployed at each issuing CA in the CA hierarchy.
- **IPSec tunneling.** Each remote office connects to the corporate office by using IPSec tunnel mode. The remote offices use third-party VPN devices, and the corporate office provides one Windows Server 2003 computer as a tunnel termination point. The VPN devices support certificates and provide an option to generate a PKCS #10 certificate request for the device.

## Case Study Questions

1. Assume that a custom version 2 certificate template is created for code signing that requires CA certificate manager approval. What enrollment method should you use for deploying the custom code signing certificates to the three members of the Quality Assurance team?
2. Assume that a custom version 2 certificate template is created for EFS certificates. What options must be enabled in the certificate template to permit autoenrollment for all users in the Lucerne Publishing forest?

3. Where must you configure Group Policy to enable autoenrollment of the custom EFS certificate to all users in the LucernePublish.msft domain?
4. Does autoenrollment deploy custom EFS certificates to all Windows 2000 and Windows XP laptop users? Why or why not?
5. What method of enrollment allows EFS certificates to be deployed to users with Windows 2000 laptops without user intervention?
6. Assume that the default EFS Recovery Agent certificate template is modified so that only the two EFS recovery agents are assigned Read and Enroll permissions for the certificate template. What enrollment method(s) can they use to acquire their EFS Recovery Agent certificates?
7. Assuming that the default IPsec certificate is used for the IPsec tunnel mode project, do you use ACRS or Autoenrollment Settings to automate the deployment of IPsec certificates to Windows Server 2003 computers at the corporate office?
8. What must be done to the IPsec certificate template and the Automatic Certificate Request Settings Group Policy setting to enable automatic enrollment of the IPsec certificates by Windows Server 2003 computers?
9. What must be done to the IPsec certificate template and the Autoenrollment Settings Group Policy setting to enable automatic enrollment of the IPsec certificates by Windows Server 2003 computers?
10. How do you deploy IPsec certificates to the third-party VPN devices at the remote offices?
11. If the VPN devices were Cisco VPN devices, what method could you use to automate the IPsec certificate distribution? What additional configuration is required at the enterprise CA?

## Additional Information

- Microsoft Official Curriculum, Course 2821: “Designing and Managing a Windows Public Key Infrastructure” ([www.microsoft.com/traincert/syllabi/2821afinal.asp](http://www.microsoft.com/traincert/syllabi/2821afinal.asp))
- “Implementing and Administering Certificate Templates in Windows Server 2003” ([www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03crtm.mspix](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03crtm.mspix))
- “Certificate Autoenrollment in Windows Server 2003” ([www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/autoenro.mspix](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/autoenro.mspix))
- “Windows Data Protection” (<http://msdn.microsoft.com/library/en-us/dnsecure/html/windataprotection-dpapi.asp>)



- CAPICOM Reference ([http://msdn.microsoft.com/library/en-us/security/Security/capicom\\_reference.asp](http://msdn.microsoft.com/library/en-us/security/Security/capicom_reference.asp))
- “The Cryptography API, or How to Keep a Secret” ([http://msdn.microsoft.com/library/en-us/dncapi/html/msdn\\_cryptapi.asp](http://msdn.microsoft.com/library/en-us/dncapi/html/msdn_cryptapi.asp))
- Certificate Enrollment Control ([http://msdn.microsoft.com/library/en-us/security/security/certificate\\_enrollment\\_control.asp](http://msdn.microsoft.com/library/en-us/security/security/certificate_enrollment_control.asp))
- Creating Certificate Requests Using the Certificate Enrollment Control and CryptoAPI (<http://msdn.microsoft.com/security/default.aspx?pull=/library/en-us/dncapi/html/certenrollment.asp>)
- Configuring the Cisco VPN 3000 Concentrator 4.1 to Get a Digital Certificate Using SCEP ([http://www.cisco.com/en/US/products/bw/vpndevc/ps2284/products\\_tech\\_note09186a008009406e.shtml](http://www.cisco.com/en/US/products/bw/vpndevc/ps2284/products_tech_note09186a008009406e.shtml))
- Knowledge Base Article 249125: “Using Certificates for Windows 2000 and Cisco IOS VPN Interoperation”
- Knowledge Base Article 309408: “Troubleshooting the Data Protection API (DPAPI)”
- Knowledge Base Article 310389: “HOW TO: Request a Certificate by Using the Certificates Snap-In in Windows 2000”
- Knowledge Base Article 326474: “HOW TO: Troubleshoot VPN with Extensible Authentication Protocol (EAP) Authentication”
- Knowledge Base Article 330389: “Internet Explorer Stops Responding at ‘Downloading ActiveX Control’ Message When You Try to Use a Certificate Server”
- Knowledge Base Article 323172: "Flaw in Certificate Enrollment Control May Cause Digital Certificates to Be Deleted"



**Note** Microsoft Knowledge Base articles can be found at <http://support.microsoft.com>. Enter the article number in the Search the Knowledge Base text box.



## Chapter 13

# Creating Trust Between Organizations

When an organization creates its own certification authority (CA) hierarchy, the certificates are usually trusted only by that organization. With technologies such as code signing and secure e-mail, it is often necessary for certificates to be trusted by other organizations.

This chapter will introduce several methods for deciding what certificates issued externally will be trusted by your organization. The chapter focuses on using qualified subordination, wherein an organization defines trust criteria so that certificates that meet the defined criteria will be trusted by your organization.

## Methods of Creating Trust

When you implement a Microsoft Windows Server 2003 Public Key Infrastructure (PKI) in an Active Directory environment, several methods exist for creating trust between organizations, including:

- **Certificate trust list (CTL).** A CTL is a signed list of hashes. Each hash in the list is a hash performed against a root CA's public keys. The CTL itself is signed by the holder of a Certificate Trust List Signing certificate. A CTL allows you to specify what certificate types—specifically what Extended Key Usages (EKUs)—must exist in the certificates that your organization trusts. For example, your organization could choose to trust only certificates with the Client Authentication object identifier (OID) in the EKU extension.
- **A common root CA.** If two organizations have CA hierarchies that share a common root CA, all certificates issued within the common CA hierarchy are trusted by both organizations. Alternatively, if two organizations must trust the certificates issued by the other organization, each organization can designate the other organization's root CA as a trusted root CA.
- **Cross-certification.** An organization can issue Cross Certification Authority certificates to a CA in another organization's CA hierarchy. After the certificate is issued, all certificates chained to this CA are trusted.

- **Qualified subordination.** An extension of cross-certification, qualified subordination places conditions on the Cross Certification Authority certificate that restrict what certificates are considered trusted from the partner organization. The constraints can restrict certificates based on namespace, certificate use, or issuance method.
- **Bridge CA.** This method allows multiple organizations to establish certificate trust. Every organization issues a certificate to a common bridge CA, which issues certificates to a CA in each organization's CA hierarchy.

These methods are discussed in greater detail in the sections to follow.

## Certificate Trust Lists

A CTL is a Microsoft solution for trusting certificates from other organizations. This solution works with most Microsoft operating systems, but it is not extensible beyond Microsoft operating systems.

CTLs allow you to designate which foreign root CAs your organization trusts. You can then define restrictions on the root CA certificate, including designating the length of time you trust certificates that chain to the root CA certificate and what Enhanced Key Usage OIDs must be in a trusted certificate. If a certificate from a foreign CA hierarchy is presented with an Enhanced Key Usage OID that is not on the list, the certificate is not trusted.

CTLs are defined in Group Policy in the Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Enterprise Trust container. The Group Policy Object (GPO) containing the defined CTL can be linked to any site, domain, or organizational unit (OU) in your Active Directory, allowing the trust to be limited only to computer accounts where the GPO is applied.

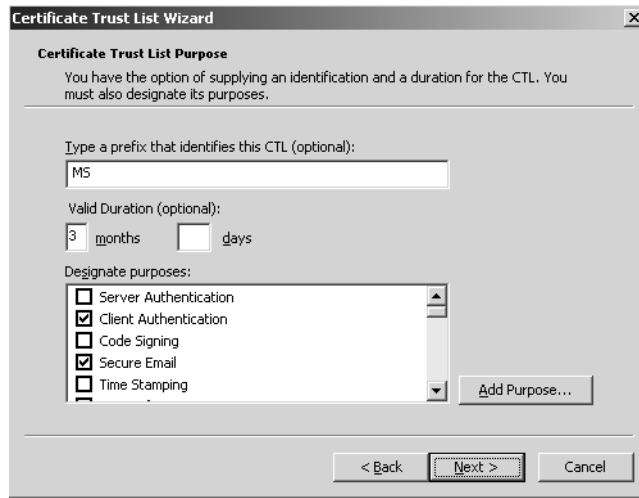


**Note** CTLs also can be defined in the User Configuration\Windows Settings\Security Settings\Public Key Policies\Enterprise Trust container, but it is recommended that you define CTLs in the Computer Configuration of GPO so that the CTLs are applied to all users of a computer.

The following procedure outlines the steps for defining a new CTL:

1. Log on to a domain for which you have administrative privileges to manage the GPO.
2. Open the GPO you want to edit.

3. In the console tree, expand Computer Configuration, expand Windows Settings, expand Security Settings, expand Public Key Policies, and click Enterprise Trust.
4. On the Action menu, point to New and click Certificate Trust List.
5. On the Welcome to the Certificate Trust List Wizard page, click Next.
6. On the Certificate Trust List Wizard page (see Figure 13-1), enter a Valid Duration period in months and days. In the Designate Purposes list, select all valid application policy OIDs from the listing and click Next.



**Figure 13-1** Defining the CTL duration and purpose

7. On the Certificates in the CTL page, add one or more root CA certificates from a file and click Next.
8. On the Signature Certificate page, click Select from Store and select a certificate with the Microsoft Trust List Signing application policy OID. When you select the certificate, click Next.



**Note** The Administrator certificate template includes the Microsoft Trust List Signing Enhanced Key Usage OID (1.3.6.1.4.1.311.10.3.1). Alternatively, a custom version 2 certificate template can be created that enables the Microsoft Trust List Signing OID.

9. On the Timestamping page, you can choose whether to submit the CTL to a timestamping service. You must provide the correct URL and then click Next.

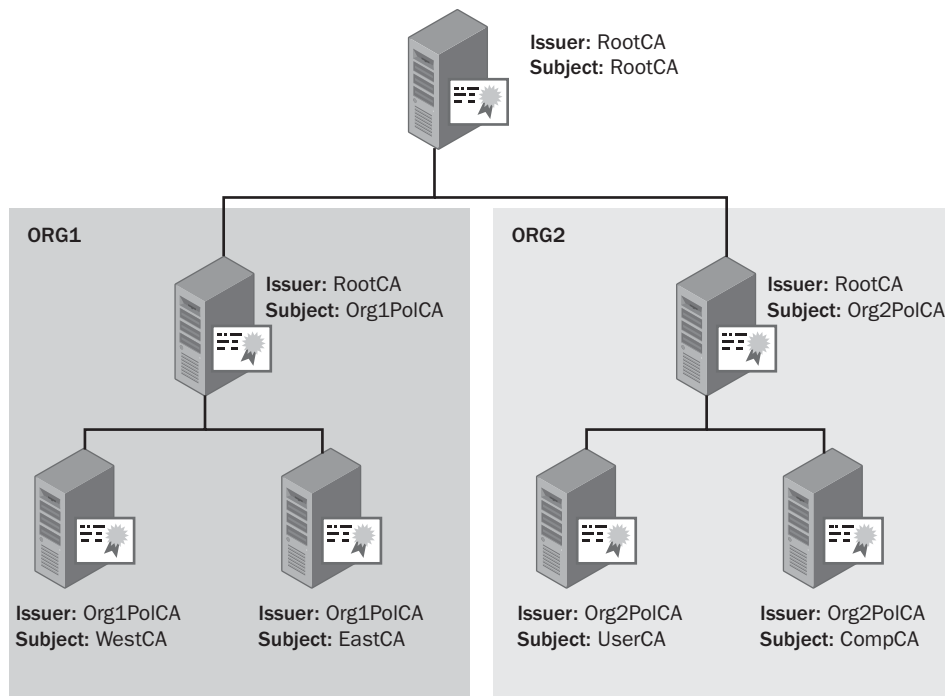


**Note** A timestamping service applies a date and time stamp to the CTL when it is signed with the Microsoft Trust List Signing certificate. This allows the certificate to be checked to see whether it was valid at the time of signing, in case the signing certificate is later revoked.

10. On the Name and Description page, enter a name and description for the CTL and click Next.
11. On the Completing the Certificate Trust List Wizard page, click Finish.

## Common Root CAs

When a common root CA is implemented, it is used by two or more organizations as their organization's root CA. A common root CA allows an organization to trust any certificate issued by a CA that chains to the same common root CA. When a common root CA is used, all certificates are trusted, subject to any constraints defined in the subordinate CA certificates. This means that if the operator of the root CA issues subordinate CA certificates to a third organization, the two original organizations trust certificates issued to the third organization. A common root CA can be deployed with subordinate CAs existing at two separate organizations. (See Figure 13-2.)



**Figure 13-2** A common root CA used by both ORG1 and ORG2

In this example, both ORG1 and ORG2 have established policy CAs below the common root CA, as well as issuing CAs that issue certificates to users, computers, and network devices in the organization.

The root CA is not necessarily a root CA from a commercial vendor, such as VeriSign or RSA. It also can be a root CA hosted by one of the two organizations. The merits of each configuration are discussed in greater detail in the sections to follow.

## Commercial CAs

When an organization outsources root CA management to a commercial vendor, it is often for the following reasons:

- To increase the trust of the certificates issued by the organization.
- To take advantage of the PKI expertise provided by the commercial vendor.

When a root CA is hosted by a commercial vendor, the organization's CAs must follow the commercial CA organization's security policy and certificate policies. If an organization does not follow these policies, the commercial CA can revoke the immediate subordinate CA's certificate, resulting in all certificates being effectively revoked.



**Note** An organization can implement policy requirements that are more secure than the commercial CA's policies, as long as none of the requirements in the policies conflict.

When you purchase a subordinate CA certificate from a commercial vendor, you must pay for use and management of the trusted root. These costs can be quite high. Typically, you pay an annual fee for the subordinate CA certificate, as well as fees for every issued certificate.

## Umbrella Groups

As an alternative, some organizations establish a root CA hosted by one of the participating organizations. Both companies can then establish subordinate CAs below the common root CA. There still will be management costs for maintaining and operating the common root CA, but they can be shared between the participating organizations.

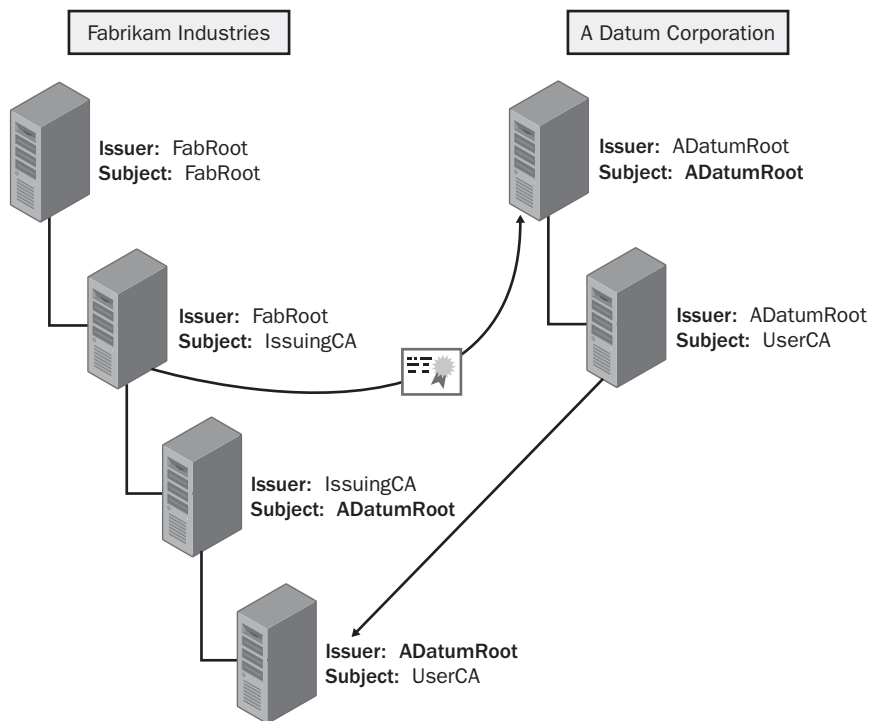
This configuration is often used by large organizations that own several sub-organizations. The holding company can deploy a common root CA for all organizations within the umbrella group and then deploy separate CAs for each participating organization. The holding company maintains control of the root CA in this configuration, but it is able to delegate PKI branch management to each organization within the umbrella group.



**Note** This configuration works well when mergers and acquisitions occur. With the root CA already created, CA hierarchy design can focus on the specific subordinate CA requirements for the merged organization.

## Cross-Certification

Cross-certification allows you to issue a Cross Certification Authority certificate from a CA in your organization to a CA in another organization. The effect of the Cross Certification Authority certificate is to “glue” the partner organization’s CA structure below the CA that issues the Cross Certification Authority certificate. (See Figure 13-3.)



**Figure 13-3** The effect of a Cross Certification Authority certificate

In this example, the IssuingCA of Fabrikam Industries issues a Cross Certification Authority certificate to the root CA of the A Datum Corporation CA hierarchy. The effect of this Cross Certification Authority certificate is that the ADatumRoot CA appears as a subordinate CA of the IssuingCA when the certificate



is presented to a computer at Fabrikam Industries. The Cross Certification Authority certificate glues the A Datum Corporation CA hierarchy to the Fabrikam Industries CA hierarchy. The CA that is listed in the subject of the Cross Certification Authority certificate appears to be a subordinate CA of the CA that issued the Cross Certification Authority certificate.



**Note** If the Cross Certification Authority certificate is issued to the UserCA rather than to the ADatumRoot CA, then the UserCA appears to be directly subordinate to the IssuingCA when presented to a computer belonging to Fabrikam Industries.

The advantage of cross-certification is that you do not have to reissue any certificates to your organization's users. The partner organization simply chooses a CA in your CA hierarchy to receive the Cross Certification Authority certificate. All certificates that exist below that point in the hierarchy are considered trusted by the issuing organization.



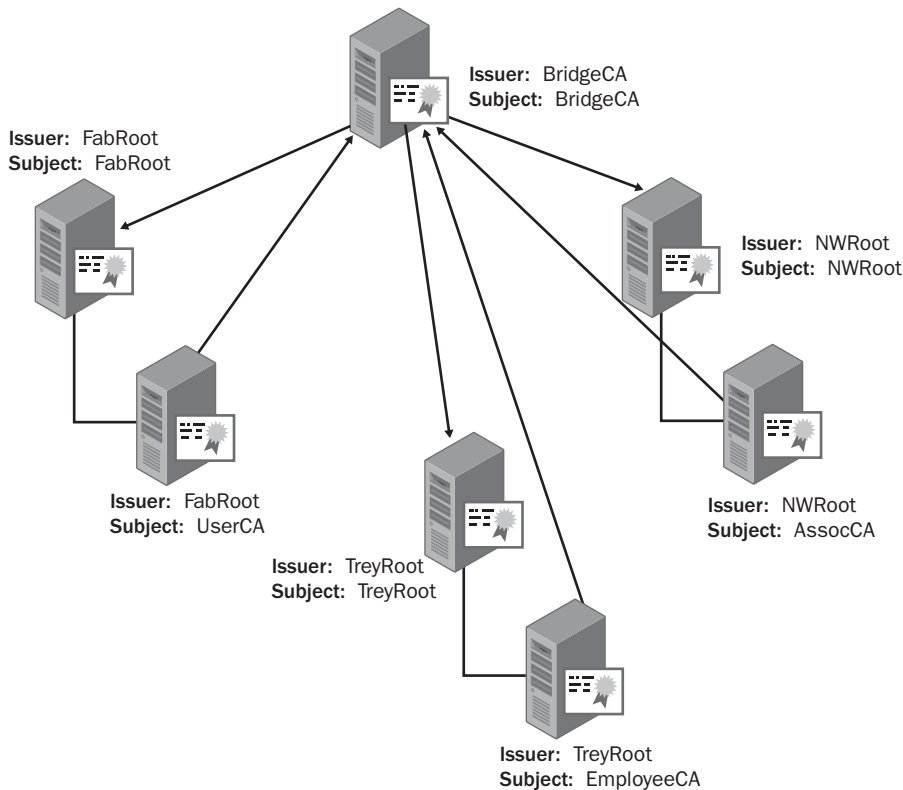
**Note** To define criteria for trusting specific certificates, the issuing organization must define qualified subordination conditions, which are implemented as extensions in the Cross Certification Authority certificate. These extensions filter out nonmatching certificates and only trust certificates that meet the defined conditions.



**Important** Only Windows XP and Windows Server 2003 support Cross Certification Authority certificates. If you have Windows 2000 or earlier computers on the network, you must also implement CTLs to define the trust of another organization's certificates.

## Bridge CAs

An alternative to cross-certification is to implement a bridge CA. (See Figure 13-4.)



**Figure 13-4** A bridge CA hierarchy

A bridge CA allows multiple organizations to recognize certificates issued by the CA hierarchies of the other organizations. The main component of the bridge CA hierarchy is the bridge CA itself. Every participating organization must issue a certificate to the bridge CA, which in turn issues a certificate to a CA in each CA hierarchy.



**Note** Organizations typically issue the bridge CA its certificate from an issuing CA rather than an offline CA. This allows faster recognition of a certificate revocation if the organization leaves the bridge CA hierarchy. If the bridge CA certificate is issued from a root or offline policy CA, the certificate revocation list (CRL) cannot be published for a long period, usually three months to a year, while an issuing CA can publish its CRL on a daily or weekly basis.

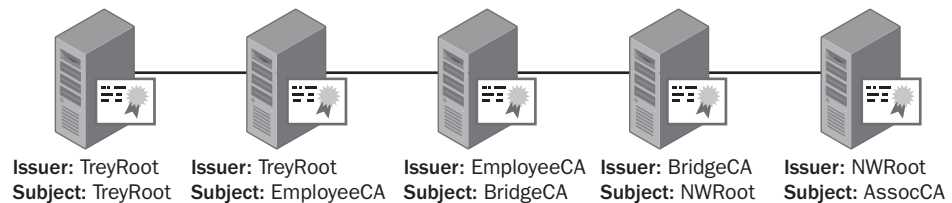
In Figure 13-4, three organizations are participating in a bridge CA hierarchy. If the certificates issued by Northwind Traders CA hierarchy (on the far right) are evaluated by a computer at Fabrikam Industries, the certificate chain is built by the certificate chaining engine. (See Figure 13-5.)



**Figure 13-5** Viewing a Northwind Traders certificate at Fabrikam Industries

In the certificate chain, note that the certificate issued to the BridgeCA was issued by the UserCA in the Fabrikam CA hierarchy. Likewise, the certificate issued to the NWRoot CA was issued by the bridge CA.

If the same certificate issued by the Northwind Traders CA hierarchy is evaluated by a computer in the Trey Research organization, a different certificate chain is built by the certificate chaining engine. (See Figure 13-6.)



**Figure 13-6** Viewing a Northwind Traders certificate at Trey Research

This chain has the same TreyRoot CA as the root CA of the hierarchy. In this case, the BridgeCA certificate was issued by the Employee CA in the Trey Research hierarchy. In both cases, the certificates issued by the Northwind Traders CA hierarchy chain to the root CA of the organization evaluating the certificate.

## The Federated Bridge Certification Authority

The bridge CA hierarchy design is based on the Federated Bridge Certification Authority, created to allow certificate recognition among all U.S. federal departments, even when different CA hierarchies issue the certificates. For more information on this topic, visit [www.cio.gov/fbca](http://www.cio.gov/fbca).

## Qualified Subordination Conditions

Qualified subordination allows your organization to define conditions that must be met for certificates issued by another CA hierarchy to be considered trustworthy by your organization. The conditions apply to any certificate issued by the CA that issues the Cross Certification Authority certificate with qualified subordination extensions and, potentially, CAs subordinate to that CA.



**Note** Qualified subordination conditions are sometimes referred to as Cross Certification conditions or Cross Certification constraints. All of these reference the same topic.

The following extensions related to qualified subordination are available for inclusion in a Cross Certification Authority certificate:

- **Basic constraint.** Defines that the certificate is a certificate issued to a CA. This constraint also defines the maximum number of CAs from a partner's CA hierarchy that can be included in a certificate's certification path.
- **Name constraint.** Defines what namespaces are acceptable in certificates issued by a partner's CA hierarchy. The constraint can define both allowed and disallowed namespaces.
- **Application policies.** Defines the purposes that are allowed for certificates issued by a partner's CA hierarchy. For example, you can choose to only trust certificates whose purpose is client or server authentication.



**Note** In certificates based on Microsoft certificate templates, the OIDs included in the Application policies extension also exist in the Enhanced Key Usage extension if the certificate is based on a version 2 certificate template. If the certificate is based on a version 1 certificate template or does not include the Application Policy extension, qualified subordination will apply any application policy constraints to the OIDs defined in the EKU extension.

- **Certificate policies.** Defines what assurance level is required for certificates issued by a partner's CA hierarchy. For example, your organization can decide to only trust certificates that the partner's CA hierarchy issues after face-to-face interviews.

The sections to follow provide more detailed information on each of the qualified subordination conditions that can be defined in a Cross Certification Authority

certificate. The conditions are defined in one of two configuration files: `Policy.inf` or `CAPolicy.inf`. These constraints also can be applied to a subordinate CA certificate to apply qualified subordination conditions to certificates issued by the subordinate CA. Each solution requires a separate configuration file:

- **Policy.inf.** Defines qualified subordination conditions for Cross Certification Authority certificates.
- **CAPolicy.inf.** Defines qualified subordination conditions for root CA certificates.



**Note** The syntax of the files is the same when defining qualified subordination conditions. The difference is how the file is read. `Policy.inf` is read when you generate the request for the Cross Certification Authority certificate by using the `Certreq.exe -policy` command. The `CAPolicy.inf` is read when you install Certificate Services on the root CA.

## Name Constraints

Name constraints define the namespaces that are allowed or disallowed in certificates issued by CAs subordinate to the CA that issues the Cross Certification Authority certificate. For example, if you want to implement name constraints on a CA owned by A Datum Corporation, you can define allowed namespaces for all forms of the `Adatum.msft` domain used in certificates you wish to recognize. This can include the following formats:

- `DirectoryName = "DC=Adatum,DC=msft"`
- `E-mail = @adatum.msft`
- `UPN = .adatum.msft`
- `UPN = @adatum.msft`



**Note** You must define each name format that can be used in a certificate issued by the partner organization. Omission of one of the name formats leads to certificate rejection, even if it should pass the defined name constraints. You can turn off the default behavior for name constraint validation for Windows Server 2003 and Windows XP SP2 by defining the `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SystemCertificates\Root\ProtectedRoots` registry key to a value of `0x20` to disable name constraint enforcement for undefined name types.

## Processing Name Constraints

When name constraints are defined, you can define both permitted and excluded namespaces. The following processing rules are used when multiple namespaces are defined:

- A certificate is accepted if all names in the certificate match the corresponding permitted name constraints.
- A certificate is rejected if any names in the certificate request match are excluded name constraints.
- If a namespace is defined in both a permitted and an excluded name constraint, the excluded name constraint takes precedence.
- If name constraints only define excluded namespaces, then all other namespaces are implicitly permitted.
- If name constraints only define permitted namespaces, then all other namespaces are implicitly excluded.
- Name constraints are applied to the Subject field and any existing Subject Alternative Name extensions.

## Name Formats

Many name formats are allowed when defining name constraints for qualified subordination. Name formats can include:

- **Relative distinguished name.** Identifies the names of objects stored in directories, such as Active Directory. The following entries are examples of relative distinguished names:
  - **DirectoryName="DC=nwtraders,DC=msft".** Includes all objects in the nwtraders.msft domain.
  - **DirectoryName="OU=Marketing,DC=nwtraders,DC=msft".** Includes all objects within the Marketing OU structure.
- **DNS name.** Identifies the Domain Name System (DNS) name of a computer or network device. This constraint is used for the evaluation of computer certificates only, as users are not assigned DNS names. The following entries are examples of relative distinguished names:
  - **DNS=www.nwtraders.msft.** Limits the DNS namespace to a single host, *www.nwtraders.msft*.
  - **DNS=.nwtraders.msft.** Limits the DNS namespace to all hosts within the nwtraders.msft DNS domain. This includes *www.nwtraders.msft* and *dc1.east.nwtraders.msft*, as both names end with nwtraders.msft.

- **Uniform Resource Identifier (URI).** Identifies resources on the Internet that use protocol identifiers such as Uniform Resource Locator (URL), File Transfer Protocol (FTP), and Hypertext Transfer Protocol (HTTP). The following entries are examples of URI names:
  - **URL=http://www.nwtraders.msft.** Limits the acceptable certificates to only *www.nwtraders.msft* using HTTP.
  - **URL=ftp://.nwtraders.msft.** Limits the namespace to all hosts within the *nwtraders.msft* DNS domain using FTP.
- **Email name.** Identifies acceptable email names in a certificate's subject or Subject Alternative Name extension. The following entries are examples of email names:
  - **Email=@nwtraders.msft.** Matches any e-mail address that is part of the *nwtraders.msft* namespace.
  - **Email=.nwtraders.msft.** Matches any e-mail address that is part of the *nwtraders.msft* namespace.
  - **Email=komar@nwtraders.msft.** Matches any e-mail address that contains *komar@nwtraders.msft*. This matches both *komar@nwtraders.msft* and *bkomar@nwtraders.msft*.
- **User Principal Name (UPN).** Like the email name, the UPN constraint defines the acceptable UPNs within the certificate's Subject Alternative Name extension. UPN formats are the same as the name formats for e-mail addresses. The following entries are examples of UPNs:
  - **UPN=@nwtraders.msft.** Matches any UPN with the suffix of *@nwtraders.msft*.
  - **UPN=.nwtraders.msft.** Matches any UPN with the suffix of *nwtraders.msft*, including *east.nwtraders.msft* and *west.nwtraders.msft*.
- **IP address.** Identifies the IP address of a computer or network device. This constraint allows you to choose either specific IP addresses or ranges of IP addresses. The following entries are examples of IP addresses:
  - **IPADDRESS=192.168.3.0/255.255.255.0.** Matches any IP address in the 192.168.3.0 network, which encompasses IP addresses 192.168.3.0 through 192.168.1.255
  - **IPADDRESS=192.168.2.244/255.255.255.255.** Matches a specific IP address, 192.168.2.244.

## Defining Name Constraints

When you enforce name constraints, an application will use a certificate only if each name in the certificate's subject or Subject Alternative Name matches at least one name constraint enforced in the Cross Certification Authority certificate. For example, if a certificate contains a Lightweight Directory Access Protocol (LDAP) distinguished name format in the subject and the UPN in the Subject Alternative Name, both names must match permitted name constraints. If one of the subject names does not match, an application will use the certificate.

You implement name constraints by defining the permitted and excluded name constraints in the *[NameConstraintsExtension]* section of a Policy.inf file for Cross Certification Authority certificates or a CAPolicy.inf file for root certification authority certificates.

```
[NameConstraintsExtension]
Include = NameConstraintsPermitted
Exclude = NameConstraintsExcluded
Critical = True

[NameConstraintsPermitted]
DirectoryName = "DC=nwtraders, DC=msft"
email = @nwtraders.msft
UPN = .nwtraders.msft
UPN = @nwtraders.msft

[NameConstraintsExcluded]
DirectoryName = "DC=Contoso, DC=msft"
email = @contoso.msft
UPN = .contoso.msft
UPN = @contoso.msft
```

In this example, all name formats of the nwtraders.msft domain are permitted, but all name formats of contoso.msft are excluded. This is a common configuration for a Cross Certification Authority certificate issued by contoso.msft to nwtraders.msft. It ensures that Northwind Traders includes only its namespace in its certificates and enforces that Northwind Traders does not issue certificates to Contoso's employees.

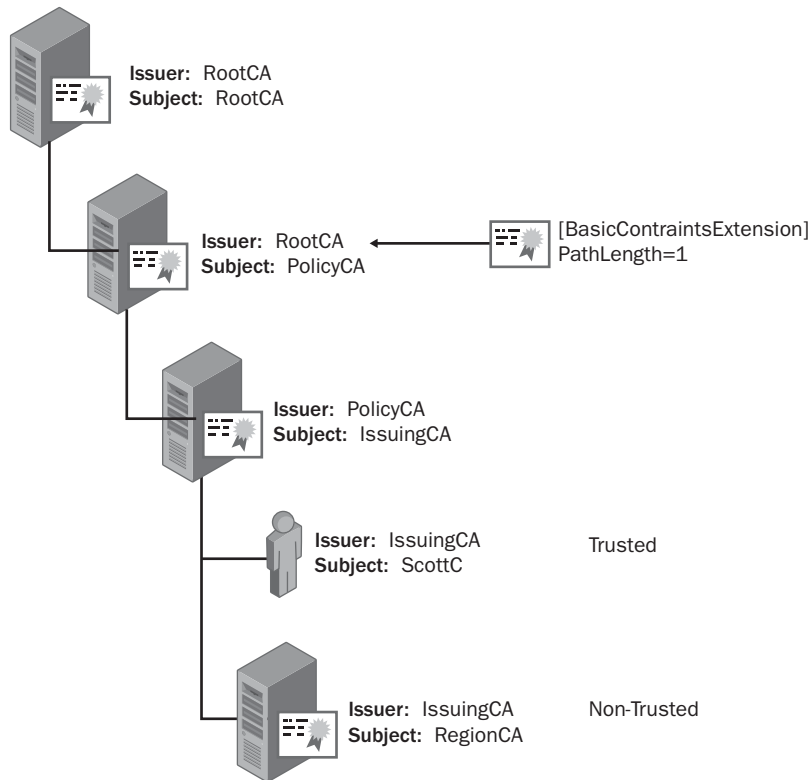
## Basic Constraints

Basic constraints have two purposes within a certificate:

- Define whether the certificate is issued to a CA or non-CA object. If the certificate is issued to a CA, the basic constraint allows the certificate to sign other certificates in a certificate chain.
- Allow you to limit the path length of a CA hierarchy below the CA where the basic constraint PathLength is defined.



You can define a basic constraint in a Cross Certification Authority certificate by adding a `[BasicConstraintsExtension]` section to the `Policy.inf` file. The `[BasicConstraintsExtension]` defines the maximum depth of a partner's CA hierarchy from which you accept certificates. For example, Figure 13-7 shows a CA hierarchy where a Cross Certification Authority certificate is issued to the PolicyCA in the CA hierarchy.



**Figure 13-7** Implementing basic constraints

If a basic constraint is defined in the Cross Certification Authority certificate issued to the PolicyCA, where the path length is defined as one, only certificates issued by the Policy CA or CAs that are one level below the PolicyCA are trusted. In Figure 13-7, this means that only certificates issued by the PolicyCA and IssuingCA are trusted. When this basic constraint is defined, the certificate issued to ScottC is trusted, as it is issued by a CA that is one level below the PolicyCA. The certificate issued to RegionCA is not trusted because it is a CA certificate. Likewise, certificates issued by the RegionCA are not trusted.



**Note** When you implement basic constraints, you must be careful when you choose the CA to issue the Cross Certification Authority certificate. For example, if you want to trust certificates issued by CAs at the same level of the CA hierarchy, it is best to issue the Cross Certification Authority certificate to the parent CA of the two CAs with a path length of 1. If you only want to trust certificates issued by a specific CA, you can define a basic constraint with a path length of 0.

## Application Policies

Applications use application policy OIDs to determine whether a certificate can be used for a given purpose, such as authenticating a user, encrypting data, or signing a device driver. When an application receives signed information from a user, it reviews the certificate associated with the private key and verifies that the certificate contains the required application policy OID. Likewise, if the application queries the user's certificate store for an application to use for signing, the application filters the list to include only those certificates with the required application policy OIDs.



**Note** Application policies are a Microsoft proprietary extension that provide the same functionality as a certificate's EKU extension. Both Application policies and EKUs indicate the purposes for which a certificate can be used and are represented by OIDs. If the application policy extension is not present in a certificate, an application or service examines the EKU extension for the required OIDs. Typically, a certificate has matching OID lists if the certificate includes both EKU and application policy extensions.

When defining qualified subordination conditions, you can limit the applications that can be used between organizations. Also, you can specifically limit the application policy OIDs that must be in the partner certificates you deem trustworthy.

By including a list of approved application policies in the defined qualified subordination conditions, you can designate that your organization only trusts certificates issued by a partner's CA hierarchy that are intended for code signing and client authentication. The listing of approved application policy OIDs is included in the issued Cross Certification Authority certificate.

## Determining Application Policy OIDs

The following procedure obtains application policy OIDs in an Active Directory environment:

1. Open the Certificate Templates console (certtmpl.msc).
2. In the console tree, right-click Certificate Templates and click View Object Identifiers.
3. In the list of Available Object Identifiers, select the application policy OID you want to copy and click Copy Object Identifier.

The OID is then copied to the Windows clipboard and can be pasted into the Policy.inf file.

## Defining Application Policies

When you issue a Cross Certification Authority certificate, you can configure a Policy.inf file to specify which application policy OIDs are permitted in partner-issued certificates. Likewise, you can define a CAPolicy.inf file to specify which application policy OIDs are permitted in root certification authority certificates.

To configure application policies in a Policy.inf or CAPolicy.inf file, create the following sections:

```
[ApplicationPolicyStatementExtension]
Policies = AppCodeSign, AppCTL, AppClientAuth
CRITICAL = FALSE

[AppCodeSign]
OID = 11.3.6.1.5.5.7.3.3 ; Code Signing

[AppCTL]
OID = 1.3.6.1.4.1.311.10.3.1; Trust List Signing

[AppClientAuth]
OID = 1.3.6.1.5.5.7.3.2 ; Client Authentication
```

### Using Custom Application Policies

Some organizations define their own application policy OIDs for custom applications. While most application policy OIDs are predefined and used universally, it might be necessary to define the mapping between your organization's application policy OID and a partner's application policy OID if custom application policies are defined.

To define the mapping, you must create a section that maps your organization's application policy OID to a similar application policy OID at the partner organization. This mapping is defined in a *[ApplicationPolicyMappingsExtension]* section in the Policy.inf or CAPolicy.inf file, as shown here:

```
[ApplicationPolicyMappingsExtension]
1.3.6.1.4.1.311.21.64 = 1.2.3.4.98
1.3.6.1.4.1.311.21.65 = 1.2.3.4.100
critical = true
```

Enabling the criticality flag enforces that an application processing this extension must understand the contents of the extension or not trust the certificate that contains the extension. (For more information on the criticality flag, review the definitions of X.509 version 3 certificates in Chapter 2, "Primer to PKI.")

## Certificate Policies

Certificate policies, also known as issuance policies, can identify the methods taken to validate a subject's identity before certificate issuance. A certificate policy can also describe the protection level of the private key associated with a certificate. For example, a private key protected by a hardware security module (HSM) is considered more secure than one stored in the Local Machine store protected by the Data Protection Application Programming Interface (DPAPI). You can use qualified subordination to only accept certificates with specific certificate policy OIDs in the certificate policy extension.

### Default Certificate Policies

When you deploy a Windows Server 2003 PKI in an Active Directory environment, the initial installation of the updated certificate templates creates four default certificate policies:

- **Low Assurance (1.3.6.1.4.1.311.21.8.a.b.c.1.400).** Indicates that minimal effort is used to validate the certificate subject's identity. For example, the certificate can be issued if the requestor knows the user account's name and password.
- **Medium Assurance (1.3.6.1.4.1.311.21.8.a.b.c.1.401).** Indicates that some effort is used to identify the certificate's subject. For example, the pending certificate can require a certificate manager to approve the request.
- **High Assurance (1.3.6.1.4.1.311.21.8.a.b.c.1.402).** Indicates that additional measures are taken to identify the certificate's subject and protect the certificate's private key. For example, the same validation tests can be performed for both a medium and high assurance certificate, but a high assurance certificate's private key can be stored on a two-factor device, such as a smart card, while the medium assurance certificate's private key can be stored on the local disk subsystem.



**Note** The definitions of the Low Assurance, Medium Assurance, and High Assurance certificate policies are just a recommendation. Your organization can define each certificate policy to meet its certificate policy requirements.

- **All Issuance (2.5.29.32.0).** Allows the acceptance of any certificates that have any issuance policy OIDs. Typically, this OID is assigned only to certificates issued to CAs.



**Note** The *a.b.c.* portion of the OID is a randomly generated numeric sequence that is random for each forest with the Windows Server 2003 schema extensions.

## Custom Certificate Policies

In many cases, an organization creates its own custom OIDs for certificate policies. This allows the organization to define certificate policy OIDs in its organization's OID space rather than use the default Microsoft OIDs.



**Note** For more information on obtaining an OID tree for your organization, review Chapter 6, "Implementing a CA Hierarchy."

Custom certificate policies also allow an organization to programmatically define the exact issuance process and certificate usage. For example, an organization can create a certificate policy called *Notarized*, which is included in a digital signing certificate issued to the organization's notary publics. To receive a certificate with the Notarized certificate policy, a requestor's application must prove to a certificate manager that he or she is a notary public. This could be accomplished by showing the certificate manager proof of the designation.

If you implement custom certificate policies, a partner company will not be using the same OID to represent a similar certificate policy. For example, a partner company can have a similar certificate policy named *Notary Publics*. In this case, the two companies must define a mapping between the OIDs to ensure that a certificate with the Notary Publics OID is recognized as equivalent to a certificate with the Notarized OID.

## Implementing Certificate Policies

To implement certificate policies when defining qualified subordination conditions, you must map the certificate policy OIDs you require in a partner's certificates to OIDs that exist within your environment. The mappings are defined in the Policy.inf file so that the certificate policy mappings are included in the issued Cross Certification Authority certificate.

You can create the following sections in the Policy.inf file to define certificate policies:

```
[PolicyStatementExtension]
Policies = Notarized
CRITICAL = FALSE

[Notarized]
OID = 1.3.6.1.4.1.311.509.3.1
```



**Note** Certificate policy extensions are only recognized by computers running Windows XP or the Windows Server 2003 family. If the extension is marked critical, the Cryptographic API (CryptoAPI) passes the extension to the application. It is up to the calling application to enforce the certificate policy OID requirement.

The example shows that a single certificate policy is defined, named Notarized, and is assigned the 1.3.6.1.4.1.311.509.3.1 OID.



**Note** This is a fabricated OID based on Microsoft's OID space. It is not an actual production OID. Microsoft owns the 1.3.6.1.4.1.311 OID tree.

Once you define your organization's certificate policies, you must map your OID to the partner's OID. For example, if the partner organization assigns the Notary Publics certificate policy with the 1.3.6.1.4.1.311.600.4.2 OID, you must define that the Notary Publics certificate policy is equivalent to your organization's Notarized certificate policy.

The following example shows how certificate policy mapping is configured in a Policy.inf file:

```
[PolicyMappingsExtension]
1.3.6.1.4.1.311.509.3.1 = 1.3.6.1.4.1.311.600.4.2
```

This line states that the Notarized OID (1.3.6.1.4.1.311.509.3.1) is equivalent to the Notary Publics OID (1.3.6.1.4.1.311.600.4.2).

## Guidelines for Qualified Subordination Conditions

When planning qualified subordination conditions in either a Policy.inf or CAPolicy.inf file, follow these guidelines:

- **Define only the required conditions.** If you do not see a need for restricting certificate policies, do not define them.
- **Exclude your namespace in all name constraints.** By excluding your namespace in the Cross Certification Authority certificate, you prevent the partner organization from issuing unauthorized certificates representing your users, computers, or network devices. This prevents a certificate issued by a partner to be used to represent one of your employees or resources.
- **Involve the legal department in negotiations with the partner organization.** Qualified subordination opens your network to certificates issued by another organization. Your legal department might want to define compliance requirements, such as requiring audits to ensure that certificate policies are followed when issuing certificates for use in your organization.
- **Issue separate Cross Certification Authority certificates for each purpose.** If you must trust a partner's organization for multiple projects with different requirements, issue a separate Cross Certification Authority certificate for each project.

## Implementing Qualified Subordination

This section will describe the steps involved in cross certifying your organization's CA hierarchy with a partner's CA hierarchy. The first step is to create a Qualified Subordination Signing certificate template. By default, there is no certificate template that meets the requirements for qualified subordination requests, so a custom version 2 certificate template must be created.

The certificate template must include the Qualified Subordination application policy OID (1.3.6.1.4.1.311.10.3.10). You can also enforce CA certificate manager approval and limit Read and Enroll permissions to designated users or groups.



**Important** The Qualified Subordination application policy OID must be included in the certificate template because the Cross Certification Authority certificate template requires that the requestor sign the certificate request with a certificate that contains the Qualified Subordination application policy OID.

## Creating the Qualified Subordination Signing Certificate Template

The following procedure creates a version 2 certificate template that meets the Qualified Subordination Signing requirements:

1. Log on as a user assigned the permissions to create and modify certificate templates.
2. Open the Certificate Templates console (certtmpl.msc).
3. In the details pane, right-click Enrollment Agent and click Duplicate Template.
4. In the Properties of New Template dialog box, on the General tab, in the Template Display Name box, type Qualified Subordination Signing, and click OK.
5. In the details pane, double-click Qualified Subordination.
6. In the Qualified Subordination Properties dialog box, on the Extensions tab, in the Extensions Included in this Template list, select Application Policies, and click Edit.
7. In the Edit Application Policies Extension dialog box, in the Application policies list, select Certificate Request Agent and click Remove.
8. In the Edit Application Policies Extension dialog box, click Add.
9. In the Add Application Policy dialog box, in the Application policies list, select Qualified Subordination and click OK.
10. In the Qualified Subordination dialog box, on the Security tab, assign Read and Enroll permissions to a global or universal group that contains the users that will request the Qualified Subordination Signing certificate.
11. Click OK.

## Publishing the Qualified Subordination Signing Certificate Template

Once you create the Qualified Subordination Signing certificate template, you must publish it at an enterprise CA so that it is available for enrollment. You also must publish the Cross Certification Authority certificate template. Both certificate templates are required to generate a Cross Certification Authority certificate with qualified subordination extensions.

The following procedure publishes the Qualified Subordination Signing and Cross Certification Authority certificate templates:

1. Ensure you are logged on as a CA administrator.
2. Open the Certification Authority console.
3. In the Certification Authorities console, in the console tree, expand *CAName* (where *CAName* is the logical name of your CA) and click Certificate Templates.



4. In the console tree, right-click Certificate Templates, click New, and click Certificate Template to Issue.
5. In the Enable Certificate Templates dialog box, select Qualified Subordination Signing and Cross Certification Authority and click OK.
6. In the details pane, verify that the Qualified Subordination Signing and Cross Certification Authority certificate templates appear.



**Note** You might have to modify the Cross Certification Authority certificate template before publication. By default, only members of the forest root domain's Domain Admins and Enterprise Admins groups have Read and Enroll permissions. Unless the user accounts that will be issued the Qualified Subordination Signing certificates are members of these groups, the permissions of the Cross Certification Authority certificate template must be modified. You must assign these user accounts Read and Enroll permissions either directly or through a group membership.

Once the certificate templates are published, ensure that all designated users acquire the Qualified Subordination Signing certificate.

## Implementing the Policy.inf File

The Policy.inf file defines the qualified subordination conditions in a Cross Certification Authority certificate request. The conditions only include the conditions required for establishing a relationship between your CA hierarchy and the partner's CA hierarchy.

The Policy.inf file:

- **Does not exist by default.** The Policy.inf file must be created and defined manually.
- **Can exist in any folder on the network.** Unlike CAPolicy.inf, the Policy.inf file must be accessible to the person generating the Cross Certification Authority certificate request file. This can include the local file system or a network share.
- **Does not have to be named Policy.inf.** Unlike CAPolicy.inf, the certreq -policy command allows you to designate the location and name of the Policy.inf file.



**Tip** Provide a descriptive name for the Policy.inf file so that its purpose is easily recognizable. For example, *NWTraders to Fabrikam for code signing.inf* is a much better name than Policy2.inf.

- **Is read during the processing of a Cross Certification Authority certificate request.** The Policy.inf file is only read during the execution of the certreq -policy command. The file is not read during the installation of Certificate Services or when a CA certificate is renewed.



**Note** A sample of the Policy.inf file is available in Appendix A of “Planning and Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003.” The Web address for this white paper is listed later in this chapter under “Additional Information.”

## Acquiring a Partner’s CA Certificate

Once you create the Policy.inf file, you must obtain the partner’s CA certificate. This certificate represents the CA to which you are going to issue the Cross Certification Authority certificate.

The certificate is used to generate the Cross Certification Authority certificate’s subject name. By using the CA’s certificate to obtain the CA’s name, the process is protected against a user making typographic errors during subject input. Using the CA’s certificate also ensures that the Cross Certification Authority certificate preserves the subject name from the provided certificate.

## Generating the Cross Certification Authority Certificate

The following elements are required to generate a Cross Certification Authority certificate:

- The Policy.inf file with all required qualified subordination conditions defined.
- The CA certificate of the target CA in the partner’s CA hierarchy.
- A Qualified Subordination Signing certificate and private key stored in the current user’s profile.

## Creating the Cross Certification Authority Request File

1. Copy the partner's CA certificate and Policy.inf file to a common folder.
2. At a command prompt, type **certreq -policy** to create the certificate request file that enforces all the qualified subordination conditions defined in the Policy.inf file.
3. In the Open Request File dialog box, in the Files of Type box, select Certificate Files (\*.cer, \*.crt, \*.der), select the target CA's certificate, and click Open.
4. In the Open Inf File dialog box, select the configured Policy.inf file and click Open.
5. In the Certificate List dialog box, select your Qualified Subordination Signing certificate and click OK.
6. In the Save Request dialog box, in the File Name box, type a name for the Cross Certification Authority certificate request file and click Save.



**Note** The Cross Certification Authority certificate request file is a Certificate Management Message over Cryptographic Message Syntax (CMC) request file that contains all the defined qualified subordination extensions and is signed with the requestor's Qualified Subordination Signing certificate.

## Submitting the Cross Certification Authority Request

Once the CMC certificate request file is generated, it must be submitted to an enterprise CA to request the Cross Certification Authority certificate. The Cross Certification Authority certificate template must be published at the CA where the request is submitted. Use the following procedure to submit the request:

1. Open the Certification Authority console.
2. In the console tree, right-click *CAName* (where *CAName* is the name of the enterprise CA), point to All Tasks, and click Submit New Request.
3. In the Open Request File dialog box, select the request file you created in the previous process and click Open.
4. In the Save Certificate dialog box, indicate a name for the issued certificate file and click Save.

## Publishing to Active Directory

The certificate object is published automatically into the `CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,ForestRootDomain` container as a CrossCA object. The certificate is never distributed to the target CA in the other organization's CA hierarchy. Instead, it is downloaded via autoenrollment to all domain member computers so that the Cross Certification Authority certificate can be used to build certificate chains between the two CA hierarchies. This allows recognition of the partner CA's certificates that meet the qualified subordination conditions.



**Note** When the autoenrollment process is triggered by Winlogon or a Group Policy refresh interval, the operating system queries Active Directory to download the appropriate certificate stores into the local store on the client machine—for example, root CA certificates, Cross Certification Authority certificates, and the NTAAuth container.

When participating in a bridge CA hierarchy structure, the Cross Certification Authority certificates issued by the bridge CA must be manually published by each organization participating in the bridge CA hierarchy structure. This is because the bridge CA is not a member of your organization's forest and is unable to publish its issued Cross Certification Authority certificates into your forest automatically.

You can use the following `certutil.exe` command to manually publish a Cross Certification Authority certificate into Active Directory:

```
certutil -f -dspublish <CrossCertFile.crt> CrossCA
```

## Verifying Qualified Subordination

Once you publish the necessary Cross Certification Authority certificates to Active Directory, you should verify their publication. The recommended verification method is the `certutil` command described here.

1. Open a command prompt.
2. At the command prompt, type **`certutil -viewstore "CN=CAName,CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,ForestRootDN?crossCertificatePair"`** (where *CAName* is the name of the CA to which the Cross Certification Authority certificate is issued, and *ForestRootDN* is the LDAP distinguished name of the forest that issued the Cross Certification Authority certificate).
3. In the View Certificate Store dialog box, select the Cross Certification Authority certificate you want to view and click View Certificate.

4. In the Certificate dialog box, on the Certification Path tab, ensure that the certification path shows that the *CAName* certificate is chained to your organization's root CA certificate.

This process should be repeated for each Cross Certification Authority certificate published in your organization's Active Directory.

## Case Study: Trusting Certificates from Another Forest

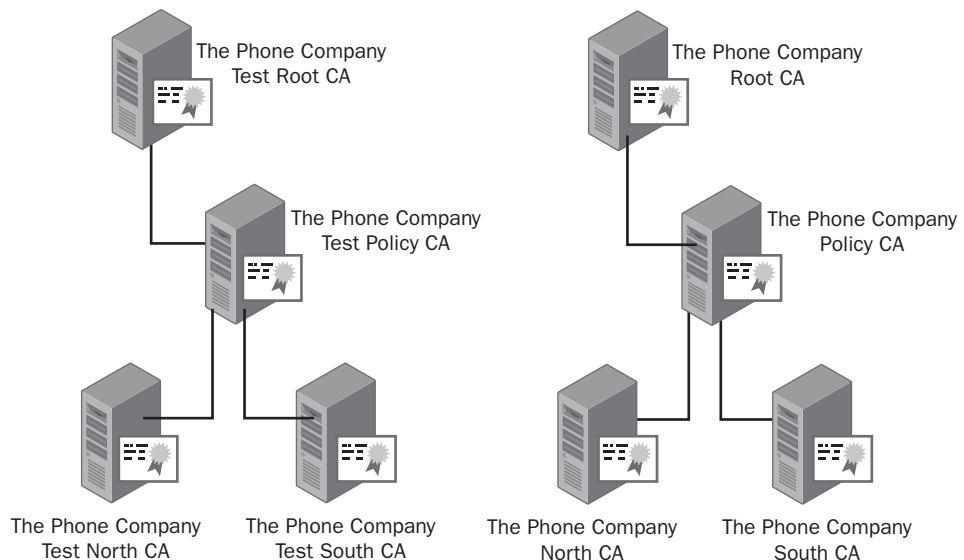
The software development group at The Phone Company, a large telecom provider in Europe, recently started to develop ActiveX controls for Web-based applications for internal projects. To download the ActiveX controls, they must be signed with a Code Signing certificate.

The Phone Company implements two forests on its corporate network:

- **test.thephonecompany.msft.** The certification forest.
- **ad.thephonecompany.msft.** The production forest.

All ActiveX controls must be created and tested in the certification forest before they are deployed to the production forest. Once application testing is complete, the plan is for the software development manager to sign the ActiveX control on behalf of The Phone Company, indicating that the ActiveX control is suitable for deployment on the production network.

You are the PKI manager. To better replicate the production network in a test environment, the same CA hierarchy structure is deployed in the certification forest and the production forest, as shown in Figure 13-8.



**Figure 13-8** The two CA hierarchies at The Phone Company

Both CA hierarchies implement two issuing CAs to allow CAs to be placed at the London and Barcelona offices of The Phone Company. The offline CAs are stored at the company's Munich office. For both forests, the CAs are deployed at the actual locations rather than in a test lab. The software development manager prepared the following requirements to enable code signing recognition between the forests:

- The ActiveX controls must be signed in the certification forest only. The signing process must not be duplicated when the ActiveX control is deployed to the production forest. The same signature must be recognized in both the certification and production networks.
- The subject of the code signing certificate issued to the manager has the following Active Directory common name: CN=The Phone Company,OU=PKI Roles,DC=ad,DC=thephonecompany,DC=msft. Only the distinguished name is included in the code signing certificate subject.
- The certificate is issued by The Phone Company South CA in the production network. The Phone Company North CA does not issue code signing certificates.
- The code signing certificate issued to the software development manager contains the following extensions:
  - Enhanced Key Usage: code signing (1.3.6.1.5.5.7.3.3)
  - Issuance policies: None

You must perform cross-certification between the two CA hierarchies so that qualified subordination conditions allow the certification forest to trust only the manager's code signing certificate. You must design the qualified subordination conditions as restrictive as possible so that no other code signing certificates are accepted.

## Case Study Questions

1. Which CA in the production hierarchy must be issued the Cross Certification Authority certificate to meet the design requirements?
2. What CA must be used to issue the Cross Certification Authority certificate on the certification network to meet the design requirements?
3. If the Cross Certification Authority certificate is issued to the The Phone Company Policy CA, what lines must be included in the Policy.inf file to recognize certificates issued by the The Phone Company South CA?
4. If the Cross Certification Authority certificate is issued to the The Phone Company South CA, what lines must be included in the Policy.inf file to recognize certificates issued by the The Phone Company South CA?

5. What name constraints are required in the Policy.inf to limit permitted certificates to the single certificate issued to the software development manager?
6. What application policy entries are required in the Policy.inf to limit the certificates to only code signing certificates?
7. Assuming that the Cross Certification Authority certificate is issued by The Phone Company Test South CA to The Phone Company South CA, how does the certificate chain for the manager's certificate look when viewed at a Windows XP computer in the certification forest?
8. Assuming that the Cross Certification Authority certificate is issued by The Phone Company Test South CA to The Phone Company South CA, how does the certificate chain for the manager's certificate look when viewed at a Windows XP computer in the production forest?

## Additional Information

- Microsoft Official Curriculum, Course 2821: “Designing and Managing a Windows Public Key Infrastructure” ([www.microsoft.com/traincert/syllabi/2821afinal.asp](http://www.microsoft.com/traincert/syllabi/2821afinal.asp))
- “Implementing and Administering Certificate Templates in Windows Server 2003” ([www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03crtm.mspx](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03crtm.mspx))
- RFC 3280, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” ([www.ietf.org/rfc/rfc3280.txt](http://www.ietf.org/rfc/rfc3280.txt))
- “Qualified Subordination Overview” ([www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/sag\\_CS\\_Using\\_QSub.asp](http://www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/sag_CS_Using_QSub.asp)).
- “How to Perform Qualified Subordination” ([www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/sag\\_cs\\_procs\\_qs.asp](http://www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/sag_cs_procs_qs.asp)).
- “Planning and Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003” ([www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03qsup.mspx](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03qsup.mspx)).





## **Part III**

# **Deploying Application-Specific Solutions**



## Chapter 14

# Archiving Encryption Keys

You can archive the private keys for encryption certificates at a Microsoft Windows Server 2003 enterprise certification authority (CA) to allow recovery of the private key if a user's private key is lost or corrupted. This functionality is available on a Windows Server 2003 enterprise CA running on Windows Server 2003, Enterprise Edition, or Windows Server 2003, Datacenter Edition.

An organization should specify key archival and recovery in its security policy. If an organization does not specify that it allows key archival and recovery, it is almost impossible for the organization to implement key archival and recovery, as there are no guidelines for the implementation. If the security policy allows key archival, the policy must state when it is permissible for a certificate's private key to be recovered from the CA database.

Key recovery is only possible only when the private key material is stored on the local file system. When a software cryptographic service provider (CSP) is used, the private key material is stored in the `\Documents and Settings\UserName\Application Data\Microsoft\Crypto\RSA` or the `\Documents and Settings\UserName\Application Data\Microsoft\Crypto\DSS` folder. An organization's security policy typically lists the following reasons for allowing key recovery:

- **A user profile is deleted.** When an encryption private key is stored in a user's profile folder, the private key is lost if anyone deletes that specific profile. Many organizations use profile deletion to fix problems with user logon. For example, if the desktop fails or takes a long time to appear, many organizations prescribe deleting the user's profile and generating a new profile. This results in deletion of the user's private key material.
- **A hard disk is corrupted.** The corruption of a hard disk can cause users to lose access to their profiles. This can mean a total loss of access or loss of access to the private key material within the user profile.
- **The operating system is reinstalled.** When the operating system is reinstalled, access to the previous user profiles is lost, including any private keys stored in the user's profile.
- **A computer is stolen or lost.** When a computer is stolen or lost, access to the private key material in the user profile is lost or compromised.

A difference among the reasons listed, however, is that a computer theft or loss can mean the user's private key is compromised and, therefore, the certificate associated with the private key should be revoked. There is no reason to revoke the certificate for the other reasons in this list because the user's private key is not compromised.

## Roles in Key Archival

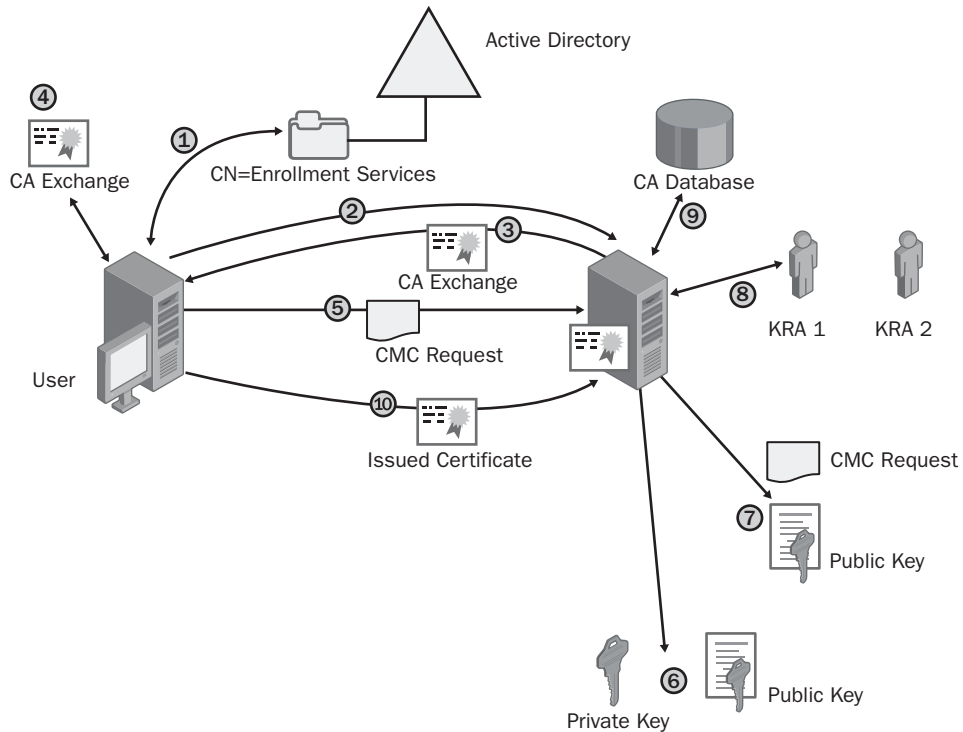
When you enable key archival at a Windows Server 2003 enterprise CA, the key recovery process has two management roles:

- **Certificate manager.** The certificate manager Common Criteria role is responsible for extracting the encrypted private key from the CA database in a binary large object (BLOB) file format. The certificate manager also determines which key recovery agent can decrypt each encrypted private key.
- **Key recovery agent.** The key recovery agent is responsible for decrypting the private key from the BLOB file extracted by the certificate manager. Once the key recovery agent extracts the private key, the PKCS #12 file must be distributed to the original user.

Although it is recommended that you assign separate people to the certificate manager and key recovery agent roles, a single person can hold both. Because the key recovery agent role is not a required or defined Common Criteria role, there are no operating system restrictions on one user holding both roles. Your organization's security policy for data recovery must determine whether these two roles must be held by separate employees.

## The Key Archival Process

When a certificate template specifies key archival, the private key associated with a certificate request must be securely transmitted from the requesting client computer to the CA for archival in the CA database. When the client requests a certificate that has key archival enabled, the process shown in Figure 14-1 takes place:



**Figure 14-1** The key archival process

1. The client queries the `CN=Enrollment Services,CN=Public Key Services,CN=Services,CN=Configuration,DC=ForestRootDomain` container to find an enterprise CA.
2. The client makes an authenticated Distributed Component Object Model (DCOM) connection to the selected enterprise CA and requests its CA Exchange certificate.
3. The CA sends the CA Exchange certificate to the client computer.
4. The client performs the following tests on the CA Exchange certificate:
  - Verifies that the CA Exchange certificate is signed by the CA's signing certificate. This ensures that the private key is being sent to the correct CA and only the intended CA can decrypt the private key.
  - Performs a certificate validation and revocation status check on the CA Exchange certificate.
5. The client encrypts the private key corresponding to the request with the CA Exchange certificate's public key, builds a Certificate Management Message over Cryptographic Message Syntax (CMC) request, and sends a CMC full PKI request to the CA.

6. The CA validates that the encrypted private key is the matched key to the public key in the CMC request.
7. The CA validates the signature on the request with the public key in the request to ensure that the contents of the request are not modified.
8. The CA encrypts the user request's private key with a random 3DES symmetric key and then encrypts the symmetric key with one or more Key Recovery Agent certificate public keys defined in the CA's properties.
9. The CA saves the encrypted key BLOB—which contains the encrypted private key and the symmetric key encrypted with one or more Key Recovery Agent certificate's public keys—to the CA database.
10. The CA processes the certificate request normally and responds to the client with a CMC full PKI response containing the certificate issued to the requestor.

The result of this process is that the client receives a certificate signed by the issuing CA, and the certificate and the associated private key are archived in the CA database. Because of the encryption, only a designated key recovery agent can decrypt the private key material stored in the CA database.

## The Key Recovery Process

When a user loses access to his or her encryption private key because of any of the reasons given in this chapter, the key recovery process proceeds as in the following steps:

1. A certificate manager for the CA that issued the certificate determines the certificate's serial number, which uniquely identifies an issued certificate;  
or  
A certificate manager searches the issuing CA and finds the certificate and private key in the database.
2. The certificate manager extracts the encrypted private key and certificate from the CA database. The BLOB file is encrypted with the public key of one or more Key Recovery Agent certificates.
3. The certificate manager transfers the BLOB file to the key recovery agent. Because the BLOB file is encrypted so that only a defined key recovery agent can recover the encrypted certificate and private key, no additional security is required.
4. The key recovery agent recovers the private key and certificate from the encrypted BLOB file at a secure workstation, also known as the recovery workstation. The private key and certificate are stored in a PKCS #12 file and are protected with a password assigned by a key recovery agent.
5. The key recovery agent supplies the PKCS #12 file and the password to the user, who then imports the certificate and private key into his or her certificate store by using the Certificate Import Wizard.

## Requirements for Key Archival

The following conditions must be met to enable key archival at a Windows Server 2003 CA:

- One or more users must acquire a certificate with the Key Recovery Agent application policy or the Enhanced Key Usage (EKU) object identifier (OID). This certificate allows the private key holder to decrypt private key material stored in the CA database. By default, the Key Recovery Agent certificate template requires certificate manager approval for issuance to ensure that only authorized personnel receive the Key Recovery Agent certificate.
- The CA must be configured and enabled for key archival. In the CA's properties, you must designate one or more Key Recovery Agent certificates that the CA must use to encrypt the private keys archived in the CA database. If at least one Key Recovery Agent certificate is designated, key archival is enabled at the CA (once Certificate Services is restarted).



**Important** All designated Key Recovery Agent certificates must be valid. If any of the Key Recovery Agent certificates are revoked, or fail any certificate validation test, key archival is not possible at the CA and certificate requests that require key archival will fail.

- A certificate template is enabled for key archival. A certificate template must enable the Archive Subject's Encryption Private Key check box to enable key archival. In addition, the certificate template may require private key export and be published at a CA that enabled key archival.



**Note** Private key export is only required if the certificate is requested from a script running on a Windows 2000 client computer. Only Windows XP and Windows Server 2003 computer recognize that a certificate template with key archival enabled allows export of the private key during the initial certificate request. Windows 2000 computers require enabling key export to allow the private key to be included in the certificate request.

- The CSP must support key export or the crypt\_archivable flag for key generation. If the CSP does not allow key export or archiving of the private key, a certificate request using the CSP will fail if the certificate template attempts to archive the private key. The CSP will not allow the private key to be sent to the CA.

## Defining Key Recovery Agents

To define a key recovery agent, you must ensure that a Key Recovery Agent certificate is issued to the designated user. The default Key Recovery Agent certificate template requires that certificate issuance be validated by a certificate manager. The process described in the next section assumes that this requirement does not change.



**Note** The holder of the private key associated with the Key Recovery Agent certificate is, ultimately, the key recovery agent. In that respect, the subject name of the certificate is inconsequential.

### Requesting the Key Recovery Agent Certificate

The following process performs the initial certificate request for the Key Recovery Agent certificate. The process assumes that the certificate template has the default settings, though the permissions are defined to allow a custom global or universal group Read and Enroll permissions:

1. Log on to the domain from a Windows 2000 or Windows XP computer with an account assigned Read and Enroll permissions for the Key Recovery Agent certificate template.
2. Open Microsoft Internet Explorer.



**Note** You must use Internet Explorer for the certificate request because the Certificate Enrollment Wizard does not support pending requests. The Certificate Services Web Enrollment pages provide content to allow you to check the status of a pending certificate request. The link is maintained through a cookie issued at the requesting computer.

3. In Internet Explorer, open the URL *http://CertSrvDNS/certsrv* (where *CertSrvDNS* is the Domain Name System name of the CA issuing the Key Recovery Agent certificates).
4. On the Welcome page, click the Request a Certificate link.
5. On the Advanced Certificate Request page, click the Create and Submit a Request to this CA link.
6. On the Advanced Certificate Request page, in the Certificate Template dropdown list, select Key Recovery Agent.





**Note** You can further increase the security of the Key Recovery Agent certificate template by creating a custom certificate template that implements a smart card CSP. With the default smart card CSPs, you must also reduce the key length to 1024 bits to allow storage on a smart card.

7. On the Advanced Certificate Request page, in the Friendly Name box, type Key Recovery Agent, and click Submit.
8. In the Potential Scripting Violation dialog box, allow the Web site to request a certificate on your behalf by clicking Yes.
9. On the Certificate Pending page, ensure that the Web page states that the request ID is in a pending state.
10. Close Internet Explorer.

This process must be repeated for each key recovery agent required in the forest.

### Issuing the Key Recovery Agent Certificate

Once the certificate request is pending, the key recovery agent must have his or her identity validated by a certificate manager. The method used to identify the key recovery agent depends on your organization's certificate policies. With the requestor's identity validated, a certificate manager can issue the Key Recovery Agent certificate using the following process:

1. Log on to the issuing CA as a user assigned the Issue and Manage Certificates permission.
2. Open the Certification Authority console.
3. Expand the certification authority name and click Pending Requests.
4. Ensure that the Key Recovery Agent certificate requestor has met the defined certificate policy, right-click the pending certificate request in the details pane, point to All Tasks, and click Issue.
5. Close the Certification Authority console.

This process must be repeated for all pending Key Recovery Agent certificates. When the certificate is issued, the CA publishes the certificate to the CN=KRA, CN=Public Key Services, CN=Services, CN=Configuration, DC=ForestRootDomain container. Publication in this container allows the Key Recovery Agent certificate to be added to the configuration of an enterprise CA in the forest, enabling key archival.

## Installing and Exporting the Key Recovery Agent Certificates

Once a certificate is issued, the Key Recovery Agent certificate requestor can complete the installation by performing the following process:

1. Open Internet Explorer at the same computer where the original request was submitted.



**Important** The private key material, as well as the cookie that has information about the pending certificate request, only exists at this computer. If you implemented a smart card CSP for the Key Recovery Agent certificate template, you also must have the smart card used to generate the certificate request.

2. In Internet Explorer, open the URL *http://CertSrvDNS/certsrv* (where *CertSrvDNS* is the Domain Name System name of the certification authority issuing the Key Recovery Agent certificates).
3. On the Welcome page, click the View the Status of a Pending Certificate Request link.
4. On the View the Status of a Pending Certificate Request page, click the Key Recovery Agent Certificate (Date and Time) link.
5. On the Certificate Issued page, click the Install this Certificate link.
6. In the Potential Scripting Violation dialog box, accept that the Web site is adding a certificate to your computer by clicking Yes.
7. Ensure that the Certificate Installed page appears, indicating that the certificate has been installed successfully.
8. Close Internet Explorer.

## Exporting the Certificate and Private Key

Once you successfully enroll the Key Recovery Agent certificate, it is recommended that you export the certificate and private key to a PKCS #12 file and remove the key material from the hard drive of the computer where the request was performed. This process allows key recovery to take place at any computer where the private key is imported. It also ensures that the private key no longer remains on the computer where the request was performed.



**Note** Alternatively, if you store the Key Recovery Agent certificate on a smart card, you ensure that the private key material is never stored on the local drive. A smart card also makes the Key Recovery Agent certificate and private key portable, allowing its use at any computer with a smart card reader and the required CSP installed.

To export the certificate and private key, ensure you are logged on as the user who requested the Key Recovery Agent certificate and use the following process:

1. From the Start menu, click Run, type **certmgr.msc** and then click OK.
2. In the console tree, expand Personal and click Certificates.
3. In the details pane, right-click the Key Recovery Agent certificate, point to All Tasks and click Export.
4. On the Welcome to the Certificate Export Wizard page, click Next.
5. On the Export Private Key page, click Yes, Export the Private Key; and click Next.
6. On the Export File Format page, click Personal Information Exchange—PKCS #12 and enable the following check boxes:
  - Include all certificates in the certification path, if possible
  - Enable strong protection
  - Delete the private key if the export is successful
7. On the Export File Format page, click Next.
8. On the Password page, type and confirm a password to secure the PKCS #12 file and click Next.



**Tip** Use a complex password to protect the PKCS #12 file.

9. On the File to Export page, type a location to export the file to (preferably removable media such as a floppy disk or USB drive) and click Next.
10. On the Completing the Certificate Export Wizard page, click Finish.
11. In the Certificate Export Wizard message box, click OK.
12. Close the Certificates console, remove the floppy disk or USB drive from the computer, and log off the network.

This process must be repeated for all defined key recovery agents.

## Enabling a CA for Key Archival

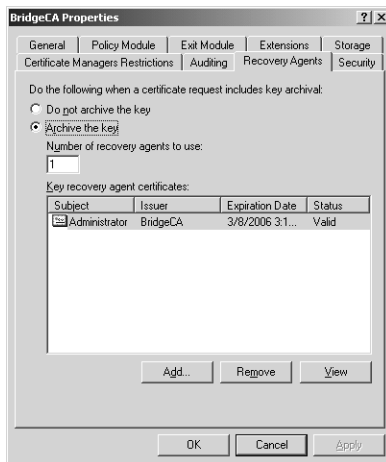
Once the Key Recovery Agent certificates are published to Active Directory, you can enable key archival on an enterprise-CA-by-enterprise-CA basis.



**Note** The CA must be an enterprise CA running on Windows Server 2003, Enterprise Edition, or Windows Server 2003, Datacenter Edition. Key archival is not supported on Windows 2000 Certificate Services or on Windows Server 2003, Standard Edition.

The following procedure enables key archival at an enterprise CA:

1. Log on at the enterprise CA as a user assigned the Manage CA permissions (known as a CA Admin).
2. On the Start menu, click Administrative Tools and click Certification Authority.
3. In the console tree, right-click the *CA name* and click Properties.
4. In the *CA name* Properties dialog box, click the Recovery Agents tab. (See Figure 14-2.)



**Figure 14-2** The Recovery Agents tab

5. On the Recovery Agents tab, click Archive the Key; in the Number of Recovery Agents to Use box, type **1**; and click the Add button.
6. In the Key Recovery Agent Selection dialog box, select the one or more Key Recovery Agent certificates and click OK.

## Choosing the Number of Key Recovery Agents

On the Recovery Agents tab, you typically set the Number of Recovery Agents to Use box to be the same value as the number of Key Recovery Agent certificates added to the CA. If you define the value to be lower than the total number of Key Recovery Agent certificates, Certificate Services randomly selects the number of designated certificates from the pool of available certificates for each encryption procedure.

This adds complexity to the encryption process, however, and is considered overkill in most cases. Instead, consider setting the Number of Recovery Agents to Use box to be the same value as the number of Key Recovery Agent certificates added.

7. In the *CA name* Properties dialog box, click Apply.



**Note** When you click the Apply button, the CA performs a certificate validation test against each designated Key Recovery Agent certificate. If any certificate fails the validation test, the failure is designated once you restart Certificate Services.

8. In the Certification Authority dialog box, click Yes to restart certificate services.
9. On the Recovery Agents tab, ensure each added Key Recovery Agent certificate's status is reported as Valid and click OK.



**Warning** You might have to close and reopen the CA Name Properties dialog box to see the change in certificate status.

10. Close the Certification Authority console.

The CA is enabled for key archival and can now issue certificates based on certificate templates that enable key archival.

## Enabling Key Archival in a Certificate Template

Once the CA is enabled for archival, you can create and publish certificate templates that enable key archival. To enable key archival in a certificate template, the first thing that you must do is set the purpose of the certificate template to either *Encryption* or *Signature and Encryption*. Key archival is only possible for certificate templates with these purposes. In fact, if the certificate template's purpose is Signature or Signature and Smart Card Logon, it is not possible to enable key archival for the certificate template.

Once you define the purpose of the certificate template as Encryption or Signature and Encryption, the following properties must be configured on the Request Handling tab of the certificate template:

- **Archive subject's encryption private key.** Enable this check box.
- **Allow private key to be exported.** Enable this option if you want to allow manual export of the certificate's private key by the holder of the private key. This option is also required if the certificate will be requested by Windows 2000 clients by using the Certificate Services Web Enrollment pages.
- **CSP.** Select a CSP that enables key export. For example, a smart card CSP might not allow key export and archival.

## Performing Key Recovery

When a private key must be recovered from a CA, the certificate manager and key recovery agent must work together to extract the encrypted BLOB from the CA database, decrypt the private key from the encrypted BLOB, and distribute the PKCS #12 file to the original user.

This process can be performed from the command line using the certutil.exe utility or from the GUI using the Key Recovery tool (krt.exe) from the Windows Server 2003 Resource Kit.



**Note** You can download a free copy of the Windows Server 2003 Resource Kit tools from [www.microsoft.com/downloads/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cffd](http://www.microsoft.com/downloads/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cffd).

### Certutil

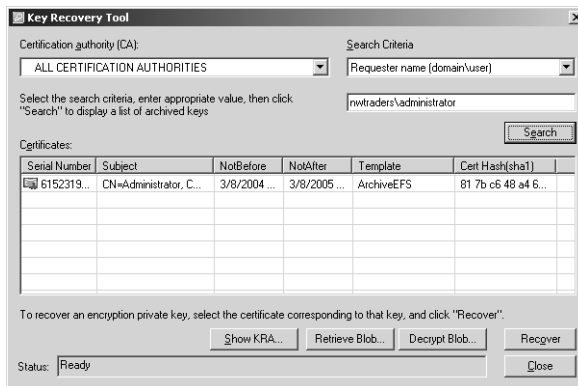
The certutil.exe command is used by both the certificate manager and the key recovery agent when key recovery is performed from the command line.

1. The certificate manager first determines the serial number of the affected certificate by viewing the properties of the certificate in the Certification Authority console.
2. Once the serial number is known, the certificate manager can extract the encrypted BLOB file by running **certutil -getkey SearchToken OutputBlob** in a Command Prompt window at the CA. The *SearchToken* can be the serial number of the certificate, the Common Name of the certificate, the Thumbprint of the certificate, the certificate requestor's user account name (domain\username), or the requestor's User Principal Name (UPN) (user@domain.com). The *OutputBlob* is a file name for the output file.
3. The key recovery agent can then log on and use the **certutil -recoverkey OutputBlob PKCS#12File** command to recover the private key from the BLOB file into a PKCS #12 file. This process defines the file name and sets a password on the PKCS #12 file.

Now the resulting PKCS#12 file can be transported to the user and then imported by the user at his or her computer, allowing access to the private key at the computer.

## Key Recovery Tool

The Key Recovery Tool provides a graphical front end for the certutil command. (See Figure 14-3.)



**Figure 14-3** The Key Recovery Tool

The Key Recovery Tool offers several advantages over the certutil command, including:

- The Key Recovery Tool searches across multiple CAs (in the same forest).
- The Key Recovery Tool interface is more intuitive than the certutil command line options.

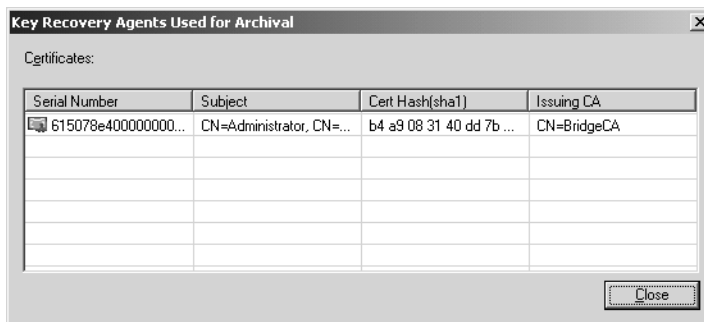
The first step of key recovery with the Key Recovery Tool is for a certificate manager to extract the encrypted BLOB file from the CA database. This requires the following process:

1. A certificate manager logs in and opens the Key Recovery Tool (krt.exe).
2. The certificate manager chooses the following options to search for the certificate in a CA database:
  - **Certification Authority.** Choose All Certification Authorities or designate a specific CA.
  - **Search Criteria.** Choose whether to search by common name (Brian Komar), requester name (REDMOND\bkomar), UPN (bkomar@microsoft.com), certificate thumbprint (9afc8c070a32d075d103164e7af62254ef64c242), or certificate serial number (1cc3967100000000dbf) and supply the search text.
3. Once the search criteria are input, the certificate manager clicks the Search button.



**Note** The Certificates listing shows all certificates that match the search criteria and have an archived private key.

4. From the Certificates listing, choose the certificate whose private key you wish to recover and click the Show KRA button.
5. In the Key Recovery Agents Used for Archival dialog box (see Figure 14-4), record the details for the designated key recovery agent(s) and click OK.



**Figure 14-4** Identifying the key recovery agents for an archived private key

6. From the Certificates listing, choose the certificate whose private key you wish to recover and click the Retrieve Blob button.
7. In the Save As dialog box, select a path and file name for the BLOB file and then click Save.



8. In the Key Recovery Tool, click Close.
9. The certificate manager then places the \*.blob file on a network share or other location accessible by the identified key recovery agent.

Once the BLOB file is extracted, the key recovery agent can decrypt it using the Key Recovery Tool.

1. The key recovery agent logs on to the network and runs the Key Recovery Tool (krt.exe).
2. In the Key Recovery Tool, the key recovery agent clicks the Decrypt Blob button.
3. In the Open dialog box, in the File Name box, type the full Universal Naming Convention (UNC) path to the BLOB file and click Open.
4. In the Save As dialog box, provide the following information, and then click Save.
  - **File Name:** The name of the PKCS #12 file you are saving. Be sure to also designate the path where you are saving the file.
  - **Save as Type:** Personal Information Exchange Files (\*.pfx).
  - **Password:** A complex password used to protect the private key.
  - **Confirm password:** Confirmation of the complex password.



**Note** The password should be complex and not easily guessed. If attackers gain access to the PKCS #12 file, they also need to know this password to import the private key into the current user's profile.

5. In the Key Recovery Info message box, click OK.
6. In the Key Recovery Tool, click Close.

## Importing the Recovered Private Key

Once the key recovery agent recovers the private key, the private key must be imported back into the original user's profile at his or her computer. The process is independent of which tool—certutil or the Key Recovery Tool—is used to retrieve the private key from the CA database.

To import the private key, the key recovery agent must provide the user with the PKCS #12 file and the password required to import the file. To ensure that an attacker cannot easily gain access to both the PKCS #12 file and its associated password, these two pieces of information should be transmitted to the original user separately. For example, the key recovery agent can send the PKCS #12 file to the user by e-mail and send the associated password to the user's voice mailbox.

Once the user receives both the PKCS #12 and the associated password, the following process imports the private key into the user's profile:

1. Ensure that you are logged on as the user associated with the private key is logged on at their computer.
2. Double-click the provided PKCS #12 file.
3. On the Certificate Import Wizard page, click Next.
4. On the File to Import page, click Next.
5. On the Password page, in the Password box, type the password provided by the key recovery agent.
6. Click Mark This Key as Exportable. This allows you to back up or transport your keys at a later time. Then click Next.
7. On the Certificate Store page, click Automatically Select the Certificate Store Based on the Type of Certificate and click Next.
8. On the Completing the Certificate Import Wizard page, click Finish.
9. In the Certificate Import Wizard message box, click OK.

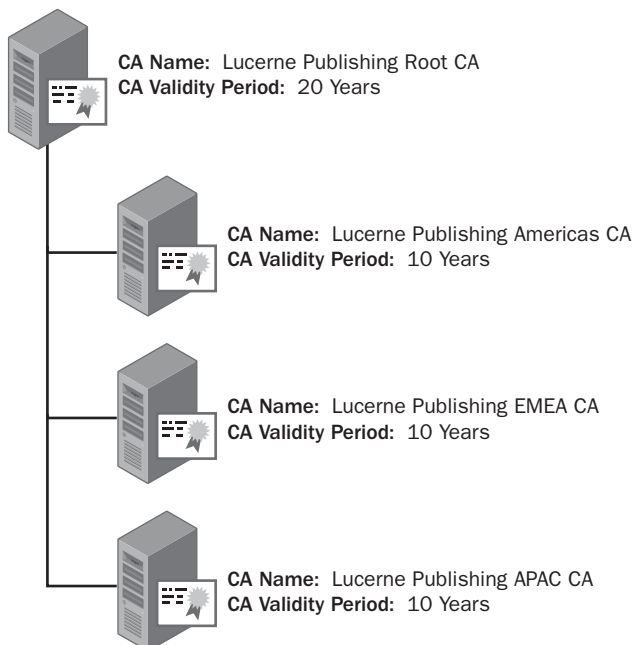
## Best Practices

- **Determine whether a certificate needs to be revoked before initiating the key recovery process.** You only have to revoke the associated certificate if the private key is compromised—for example, if the private key is located on a stolen laptop. There is no need to revoke the associated certificate if the private key was lost due to the deletion of a user's profile or the rebuild of a computer.
- **Develop a secure method for transporting private keys to the original owner.** After the key recovery agent retrieves the PKCS #12 file, he or she must securely transfer the file and its associated password to the original owner of the private key. Never send the two together. For example, consider sending the PKCS #12 file in an e-mail and leave the password in the user's voice mailbox or send the password to the user's manager.
- **Do not archive private keys for high-value certificates.** If a certificate is used to encrypt high-value data, in some circumstances it is better to lose access to the encrypted data rather than allow private key recovery.
- **Do not archive private keys used for digital signing.** Do not enable key archival for certificates with the Signature and Encryption purpose. Access to this private key can lead to impersonation for signing operations.
- **Do not combine the certificate manager and key recovery agent roles.** Require that two people be involved in the recovery process to prevent a single person from recovering a user's private key.

- **Limit the number of CAs enabled for key archival.** Do not archive keys for users at many CAs in the CA hierarchy, as recovery operations become confusing.
- **Enable the CA to audit the storage and retrieval of archived keys.** This ensures that all retrieval of archived private keys is captured in the Windows Security Log.
- **Never leave the Key Recovery Agent certificate and private key in a user's profile.** Once you complete any key recovery operation, log off the network and delete the profile directory of the user account used to perform the key recovery operation. This prevents leaving additional copies of the Key Recovery Agent certificate and private key on the network.
- **Protect the Key Recovery Agent certificate and private key by using a smart card or other two-factor device.** A smart card protects the Key Recovery Agent certificate's private key with two-factor authentication. The key recovery agent must have access to the smart card and must know the PIN of the smart card. A smart card also prevents the Key Recovery Agent certificate's private key from ever being stored on the local file system of the computer.

## Case Study: Lucerne Publishing

You manage the CAs for Lucerne Publishing. Lucerne Publishing is a global publishing company that has implemented a two-tier CA hierarchy, as shown in Figure 14-5.



**Figure 14-5** The Lucerne Publishing CA hierarchy

## Scenario

Lucerne Publishing is planning to deploy encryption certificates that will require key archival at a Windows Server 2003 enterprise CA. Applications that could be considered for key archival include the Encrypting File System (EFS) and Secure Email using Secure/Multipurpose Internet Mail Extensions (S/MIME).

The following design requirements have been identified for encryption certificates:

- Key recovery must be possible for both a centralized key recovery agent and a regional key recovery agent.
- The centralized key recovery agent certificate and private key will be located at the corporate office in Chicago, Illinois, USA.
- The regional key recovery agent certificates will be located at the major network hub site for that specific region. The regional hub sites are:
  - EMEA: Frankfurt, Germany
  - APAC: Kuala Lumpur, Malaysia
  - Americas: Winnipeg, Canada
- Common Criteria role separation is enforced at all issuing CAs.
- All key recovery operations must involve at least two persons.

## Case Study Questions

1. At what CAs in the CA hierarchy must you enable key archival? How many key recovery agents must be defined at each CA?
2. What operating system must be installed on the issuing CAs to allow key archival?
3. Can you combine the key recovery agent role with the roles of CA administrator, certificate manager, auditor or backup operator? Why or why not?
4. What Common Criteria role is blocked from being a key recovery agent due to the design requirements?
5. What certificate template must be available to allow secure transmission of the requestor's private key to the issuing CA?
6. What certutil command is used by a certificate manager to extract the encrypted BLOB from the CA database?
7. What certutil command is used by a key recovery agent to decrypt the PKCS #12 file within the encrypted BLOB file?
8. What risk is there to allowing the key recovery agent to send the PKCS #12 file and password to the user in the same e-mail message?
9. What risk is there to archiving a certificate template with the purpose of Signature and Encryption?

## Additional Information

- Microsoft Official Curriculum, Course 2821: “Designing and Managing a Windows Public Key Infrastructure” ([www.microsoft.com/traincert/syllabi/2821afinal.asp](http://www.microsoft.com/traincert/syllabi/2821afinal.asp))
- “Key Archival and Management in Windows Server 2003” ([www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/kyacws03.mspix](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/kyacws03.mspix))
- “Implementing and Administering Certificate Templates in Windows Server 2003” (<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03crtm.mspix>)



## Chapter 15

# Smart Card Deployment

Many organizations are implementing two-factor authentication solutions to increase network security. Two-factor authentication increases security by requiring something you have, a smart card or other device with a smart card chip, such as a USB token, and something you know, such as the personal identification number (PIN) for the smart card or USB token.

To use smart card authentication, an organization must deploy the related hardware and software to each desktop.

- **Hardware.** A smart card reader, as well as a smart card that is on the Microsoft Windows hardware compatibility list or includes drivers for Windows 2000, Windows XP, or Windows Server 2003 clients on your network. Alternatively, a USB token, which is a combination USB reader and card, can be used.
- **Software.** A smart card cryptographic service provider (CSP) that allows the Microsoft cryptographic application programming interface (CryptoAPI) to interact with the smart card.



**Note** The Windows operating system ships with default CSPs manufactured by GemPlus, Infineon, and Schlumberger. The default CSPs do not work with all versions of smart cards by these manufacturers, however. You must determine whether updated CSPs are needed for the smart cards selected by your organization.

## Using Smart Cards in an Active Directory Environment

Both Windows 2000 and Windows 2003 Active Directory environments support smart card authentication, which is an extension to Kerberos authentication. This means that only Windows 2000, Windows XP, and Windows Server 2003 client computers can be used with smart cards in an Active Directory environment.

## Smart Cards and Kerberos


Smart cards allow Kerberos authentication through Public Key Initialization (PKINIT) extensions to the Kerberos protocol. PKINIT extensions allow a public/private key pair to be used to authenticate users when they log on to the network.

### Kerberos Authentication Review

---

The Kerberos authentication process is comprised of three related message exchanges:

1. **Authentication Service (AS) Exchange.** This initial message exchange is used by a domain controller to provide a user with a logon session key and a Kerberos ticket-granting ticket (TGT) for future service ticket requests. A Kerberos Authentication Service Request (KRB\_AS\_REQ) is sent from the authenticating user or computer to a domain controller, and a Kerberos Authentication Service Response (KRB\_AS\_REP) is returned from the authenticating domain controller to the requesting user or computer.



**Note** If the authentication attempt fails, the domain controller sends a KRB\_ERROR response indicating the reason for the failure.

2. **Ticket-Granting Service (TGS) Exchange.** Once a user or computer receives a TGT, it can request a service ticket. The TGS exchange is initiated by the requesting user or computer when it requests access to a server resource and is comprised of a Kerberos Ticket-Granting Service Request (KRB\_TGS\_REQ) message sent from the authenticating user or computer. The message includes the TGT issued previously. If the request is successful, the domain controller responds with a Kerberos Ticket-Granting Service Response (KRB\_TGS\_REP) that contains a service ticket. This service ticket is encrypted using a master key shared by the domain controller and the target server so that only the target server can decrypt the service ticket.
3. **Client/Server (CS) Exchange.** Once a user or computer has a service ticket for the target server, it must present the service ticket to authenticate with the target server. The user or computer sends a Kerberos Application Request (KRB\_APP\_REQ) message that contains the service ticket. If the request is successful, the target server responds with a successful Kerberos Application Response (KRB\_APP\_REP) message.





**Important** Smart cards can only be used for Active Directory authentication. You cannot use a smart card to authenticate with an account in the local account database of the computer because this form of authentication is not a Kerberos authentication, but an NTLM or NTLMv2 authentication process.

When smart cards are implemented in a Windows 2000 or Windows Server 2003 Active Directory environment, a small modification is made to the Kerberos authentication process. This modification only affects the AS exchange. Rather than using a KRB\_AS\_REQ and KRB\_AS\_REP, the public key infrastructure (PKI) authentication service request (PA\_PK\_AS\_REQ) and PKI authentication service response (PA\_PK\_AS\_REP) messages are used.

For the PA\_PK\_AS\_REQ message, the user's smart card private key is used to encrypt the pre-authentication data (typically the current time at the computer where the user is performing the logon attempt). Upon receipt of the message, the domain controller decrypts the pre-authentication data with the public key obtained from the smart card certificate. When the PA\_PK\_AS\_REP message is returned to the user, the session key and TGT are encrypted with the user's public key. This ensures that only the user can decrypt the session key and TGT with his or her smart card private key.

The authenticating domain controller determines the authenticating user's identity by reading the user's User Principal Name (UPN) from the subject alternative name extension of the smart card certificate. This UPN value is then looked up at a global catalog server to determine the associated user account.



**Note** UPN values must be unique in a Windows 2000 or Windows 2003 Active Directory environment.

## Requirements for Smart Card Certificates

To deploy smart cards in a Windows 2000 or Windows Server 2003 Active Directory environment, the following requirements must be met:

- All domain controllers and computers in the forest must trust the root certification authority (CA) of the smart card certificate's certificate chain.
- The CA that issues the smart card certificate must be included in Active Directory's NT Authority (NTAuth) store. When a CA certificate is added to the NTAuth object in Active Directory (CN=NTAuthCertificates,CN=Public Key Services,

CN=Services,CN=Configuration,DC=*ForestRootDomain*), the thumbprint of the CA's certificate is automatically distributed to all Windows 2000 and later domain members in the HKEY\_LOCAL\_MACHINE\Software\Microsoft\EnterpriseCertificates\NTAuth\Certificates registry key.



**Note** You can verify the CA certificates included in the NTAuth store by using the PKI Health Tool (pkiview.msc) included in the Windows Server 2003 Resource Kit.

- The smart card certificate must contain the Smart Card Logon (1.3.6.1.4.1.311.20.2.2) and Client Authentication (1.3.6.1.5.5.7.3.2) object identifier (OID) in the Enhanced Key Usage (EKU) extension or in the Application Policies extension.



**Important** The Smart Card Logon and Client Authentication OIDs must be valid in the entire certificate chain.

- The smart card certificate must contain the user's UPN in the subject alternative name extension.

A Windows Server 2003 Enterprise Edition CA meets these requirements. Alternatively, a third-party CA can issue a smart card certificate, as long as the requirements are met. The requirements are detailed in Microsoft Knowledge Base Article 281245, "Guidelines for Enabling Smart Card Logon with Third-Party Certification Authorities," referenced in the "Additional Information" section at the end of the chapter.

## Planning Smart Card Deployment

Planning a smart card deployment involves several interrelated steps, including:

- Determining the assurance level required for smart card issuance.
- Identifying the required certificate templates.
- Determining certificate distribution methods.
- Designing and configuring the required certificate templates.
- Deploying a smart card management system.

## Increasing the Assurance of Smart Card Certificates

A smart card increases protection for a certificate's private key. To compromise a smart card's private key, an attacker must obtain the smart card and know the associated PIN. As added protection, a smart card blocks access the smart card's private key(s) after a designated number of PIN failures. The private key can only be accessed after the smart card is unlocked.

You can increase the security of the smart card distribution by requiring face-to-face interviews during enrollment. This requires the user to meet with either the enrollment agent requesting the smart card certificate or with another person, sometimes referred to as a local registration authority (LRA), who verifies the user's identity.

To indicate that you have performed a face-to-face interview before issuing a smart card, you can add a custom certificate policy OID to the Issuance Policies extension that indicate the measures taken to validate the smart card holder's identity before issuance.



**Warning** Ensure that the process indicated in the certificate policy is used for *all* smart card certificates. Failure to follow the certificate policy can result in the need to revoke *all* smart card certificates if it is discovered that some certificates were issued without identity validation.

## Identifying the Required Certificate Templates

To deploy smart card certificates using face-to-face validation, your organization must provide certificates for the two roles in smart card deployment:

- Enrollment agent
- Smart card holder

### Enrollment Agent Certificate

An enrollment agent must hold a certificate that allows him or her to request a smart card certificate on behalf of another. This is made possible by including the Certificate Request Agent OID (1.3.6.1.4.1.311.20.2.1) in the Enhanced Key Usage or Application Policies extension of the certificate.



**Warning** You cannot prevent a certificate holder with the Certificate Request Agent OID from requesting certificates for specific users in Active Directory. The holder can request a certificate for any user in Active Directory, including members of the Enterprise Admins or Schema Admins groups.

The Enrollment Agent certificate template is the default certificate template that allows a user to act as an enrollment agent. Some organizations choose to create a version 2 certificate template, based on the Enrollment Agent certificate template to enable the following modifications:

- Require certificate manager approval for issuance.
- Add a certificate policy to describe the issuance method of the Enrollment Agent certificate, which increases the assurance level of the smart card certificate.

## Smart Card Certificate

The smart card holder must have a certificate that includes the Smart Card Logon (1.3.6.1.4.1.311.20.2.2) and Client Authentication (1.3.6.1.5.5.7.3.2) OIDs in the certificate's Enhanced Key Usage or Application Policies extension.



**Note** You can include other application policy OIDs if you want to use the smart card certificate for additional purposes. For example, some organizations add the Secure Email OID (1.3.6.1.5.5.7.3.4) to the custom certificate template to allow the smart card to be used for Secure/Multipurpose Internet Mail Extensions (S/MIME) e-mail.

There are two default certificate templates for smart card logon: Smart Card Logon and Smart Card User. The difference between them is that the Smart Card User certificate template adds the Secure Email OID to the certificate's Extended Key Usage extension.

Some organizations choose to implement version 2 certificate templates based on either the Smart Card Logon or Smart Card User certificate templates. A version 2 certificate template allows an organization to make the following modifications:

- Enable autoenrollment for certificate renewal.
- Add a certificate policy to describe the issuance method of the smart card certificate.
- Add application policies to the smart card certificate.
- Enforce a specific smart card CSP for a particular template/certificate.

## Determining Certificate Distribution Methods

Once you determine which certificate templates to implement for enrollment agents and smart cards, the next step is to decide how to get the certificates to the desired holders. The methods vary depending on the type of certificate.

## Enrollment Agent

The default Enrollment Agent certificate template requires manual enrollment from either the Certificates console or the Certificate Services Web Enrollment pages.

The most common modification to the Enrollment Agent certificate template is to create a version 2 certificate template that requires CA certificate manager approval. If certificate manager approval is enabled, the Certificate Services Web Enrollment pages are required for enrollment, as this allows you to return to the Web pages and complete the certificate installation once a certificate manager approves the request. The Certificate Services Web Enrollment pages use browser cookies to maintain the status of the certificate request.

## Initial Smart Card

Smart cards increase the security of authentication and signing processes. Because a smart card (or other two-factor device) requires possession of the physical device and knowledge of the PIN protecting the private key material, organizations take additional measures to validate the employee's identity before issuing a smart card to the user.

The default smart card certificate templates limit enrollment to members of the Enterprise Admins and forest root domain's Domain Admins groups who have a certificate with the Certificate Request Agent OID in the Application Policies or Enhanced Key Usage extensions. You can increase the assurance level of the smart card certificates by implementing further validation of the smart card holder's identity. This can range from showing a company photo identification to undergoing a background check.

In some organizations, the tasks of requesting a smart card certificate and performing identity checks is split between two groups. In this scenario, the requestors of the certificates are known as enrollment agents, while the person(s) who perform the identity checks are known as LRA(s).

The enrollment agent must use the Certificate Services Web Enrollment pages to request the smart card certificate on behalf of another user. The Smart Card enrollment page uses an untrusted ActiveX control that can only be downloaded if the Certificate Services Web Enrollment site is added to the Local intranet site and the Initialize and Script ActiveX Controls Not Marked as Safe option is enabled for ActiveX downloads. This option can be set to Prompt rather than Enable to allow a user to choose to enable the ActiveX control at the time of download.



**Note** The actual process for adding the Certificate Services Web site to the Local intranet site and modifying the ActiveX download options is described later in this chapter under “Enabling ActiveX Controls.”

## Renewing the Smart Card

Under the default settings, the process of smart card certificate renewal is the same process used for initial enrollment. In other words, if you have to undergo a background check to receive your initial smart card, you must undergo the same background check to renew the certificate.

You can reduce the security requirements for smart card renewal. In other words, if you can prove that you have already undergone the background check, there is no need to undergo it again. Two solutions exist to meet this type of deployment:

- You can configure the certificate template to renew the certificate automatically if users hold existing certificates based on the existing version of the certificate template. By holding an existing certificate, users prove they have undergone the required validation process.
- You can require users to sign the certificate renewal request with the existing smart card certificate. By signing the certificate request, the requestors prove they can access the private key of the previous smart card certificate, thus proving that they requested the original certificates.

## Designing Certificate Templates for Smart Cards

Once you determine how smart cards are to be used in your organization and how the certificates are deployed, you can define the certificate templates.

### Enrollment Agent

Most organizations use the default Enrollment Agent certificate template. If you implement the default Enrollment Agent certificate template, the only recommendation is to modify the permissions to allow a custom global or universal group only (in the case of a multiple domain forest) Read and Enroll permissions. Remove the Enroll permission assignment for members of the Enterprise Admins and forest root domain's Domain Admins groups to prevent unauthorized registration of the Enrollment Agent certificate template.

If you want to implement certificate manager approval for enrollment agent certificates, you must create a version 2 certificate template based on the version 1 Enrollment Agent certificate template. Table 15-1 lists the recommended modifications to the version 2 certificate template.

Once the required enrollment agents have obtained their Enrollment Agent certificates, consider removing the Enrollment Agent certificate templates from all CAs in the organization. To help prevent unauthorized certificate enrollment of Enrollment Agent certificates, only publish the certificate template on a CA when a new enrollment agent must be designated or when certificate renewal is required.

**Table 15-1 Custom Enrollment Agent Certificate Template**

<b>Tab</b>	<b>Recommendations</b>
General	Create a custom Template Display Name and Template Name, based on the organization name, that references that the certificate template is for enrollment agents. The validity period is typically no longer than one year.
Request Handling	No modifications are required.
Subject Name	No modifications are required.
Issuance Requirements	Enable the CA certificate manager approval check box.
Superseded Templates General	Designate the Enrollment Agent version 1 certificate template as a superseded template.
Extensions	Add a custom Issuance Policy that indicates that the certificate holder's identity is validated before issuance.
Security	Assign a custom universal group Read and Enroll permissions. Consider removing Enroll permissions for the Enterprise Admins and Domain Admins group from the forest root domain.

## Initial Smart Card

In the case of smart cards, it is recommended to create a custom version 2 certificate template based on either the default Smart Card Login or Smart Card User version 1 certificate templates. The version 2 certificate templates give you greater flexibility in the configuration of the certificate contents.

Table 15-2 lists the recommended modifications to the version 2 certificate template.

**Table 15-2 Custom Initial Smart Card Certificate Template**

<b>Tab</b>	<b>Recommendations</b>
General	Create a custom Template Display Name and Template Name, based on the organization name, that references that the certificate template is for enrollment agents. The validity period is typically no longer than one year.
Request Handling	<p>Make the following changes on the Request Handling tab:</p> <p>Change the Purpose drop-down list to Signature and Smart Card Logon to prevent the smart card from being used for encryption. This setting ensures that the user is prompted during enrollment to input the smart card's PIN.</p> <p>Increase the minimum key size to 1,024 bits if using smart cards with 8 KB or more storage space.</p> <p>Define the specific smart card CSP you want to use with the certificate template.</p>

**Table 15-2 Custom Initial Smart Card Certificate Template**

Tab	Recommendations
Subject Name	The only required name format for smart card login is to ensure that the UPN option is enabled. Enable the e-mail name options if you intend to use the smart card for S/MIME e-mail purposes.
Issuance Requirements	To enable enrollment by an enrollment agent, configure the certificate template to require one authorized signature, with the signing certificate containing the Certificate Request Agent OID.
Superseded Templates	Add both the Smart Card User and Smart Card Login certificate templates, designating that the custom version 2 certificate template is the organization's preferred version.
Extensions	For application policies, include the Smart Card Logon and Client Authentication. If you want to use the smart card for signing e-mail, include the Secure Email OID. In addition, add a custom application policy OID that indicates that the certificate is your organization's smart card. This OID can be used in applications, such as Microsoft's Remote Authentication Dial-In User Service (RADIUS) server, to restrict certificate usage to only certificates with this custom OID.
Security	Add a custom certificate policy OID that defines the process used for the smart card certificate. The custom issuance policy OID can also include a Web URL reference that provides a text description of the process.  Modify the permissions for the certificate template so that only a custom global or universal group that contains all enrollment agents has Read and Enroll permissions. Consider removing the Enroll permission assignment from the Enterprise Admins and forest root's Domain Admins groups.

This certificate template can be published at multiple CAs for fault tolerance and must be available at all times to allow an enrollment agent to create a smart card for any user at any time.

## Renewing a Smart Card

If your organization's security policy requires the same subject validation process for initial smart card enrollment and renewal, you can use the custom certificate template just described. When a smart card certificate is expiring, users can return to the enrollment agent, who can re-enroll on their behalf, providing them with a replacement certificate.

If your company uses Windows XP computers, there is an alternative that takes advantage of autoenrollment and the ability to sign a certificate with the initial smart card certificate.

You create a custom version 2 certificate template that enables autoenrollment if the certificate request is signed with a previous smart card certificate. When the previous smart card certificate is near expiration, the autoenrollment process will prompt the user to sign the certificate request with his or her existing smart card certificate. When the renewal is performed, the previous smart card certificate is archived and the updated certificate remains as the active certificate.



Table 15-3 lists how to configure a version 2 certificate template to provide the ability to use autoenrollment for smart card certificate renewal. The certificate template can be based on either the Smart Card Login or Smart Card User certificate template.

**Table 15-3 Custom Renewal Smart Card Certificate Template**

Tab	Recommendations
General	<p>Create a custom Template Display Name and Template Name, based on the organization name, that references that the certificate template is for smart card renewal only. Set the validity period is no longer than one year.</p> <p>To prevent the user from continually requesting the replacement smart card certificate, enable Publish Certificate in Active Directory and Do Not Automatically Re-Enroll if a Duplicate Certificate Exists in Active Directory. This publishes the issued certificate in the <i>userCertificate</i> attribute of the user account and prevents re-enrollment if a certificate is already published to the user account.</p>
Request Handling	<p>Change the Purpose drop-down list to Signature and Smart Card Logon, increase the minimum key size to 1,024 bits if using smart cards with 8 KB or more storage space, and define the specific smart card CSP you want to use with the certificate template.</p>
Subject Name	<p>The only required name format for smart card login is to ensure that the UPN option is enabled. Also, enable the e-mail name options if you intend to use the smart card for S/MIME e-mail purposes.</p>
Issuance Requirements	<p>Configure the Issuance Requirements tab to require one authorized signature, with the signing certificate containing the Smart Card Logon OID. If you have implemented a custom application policy OID based on your organization, require this custom application policy OID for signing instead of the Smart Card Logon OID.</p>
Superseded Templates	<p>Add the initial smart card logon certificate template defined in Table 15-2. The addition of the superseded template allows autoenrollment to initiate.</p>
Extensions	<p>For application policies, ensure that you include the Smart Card Logon and Client Authentication. If you want to use the smart card for signing e-mail, include the Secure Email OID. In addition, continue adding a custom application policy OID that indicates that the certificate is your organization's Smart Card to allow continued autoenrollment processing for certificate renewal when the certificate expires.</p> <p>For issuance policies, add a custom certificate policy OID that defines the process used for the smart card certificate. The custom issuance policy OID can also include a Web URL reference that provides a text description of the process.</p>
Security	<p>Modify the permissions for the certificate template so that only a custom global or universal group that contains all smart card holders has Read, Enroll, and Autoenroll permissions.</p>

The renewal smart card certificate template can be published at multiple CAs for fault tolerance and must be available at all times to allow an enrollment agent to create a smart card for any user at any time.

## Deploying a Smart Card Management System

A smart card deployment must look beyond the issuance of smart card certificates. In addition to getting the smart cards to the users, the deployment must address the following topics:

- **Customization of the smart card enrollment pages.** You can customize the default enrollment pages. These modifications can include including your organization's logo on the Web pages, changing the signing requirements for a smart card certificate, or simplifying the user experience by removing the multitude of options available when the user requests a certificate.
- **Smart card PIN resets.** By default, most smart cards lock the user out of accessing the smart card's private key if the smart card PIN is entered incorrectly three consecutive times. Your organization must develop custom software or use commercial software to allow the remote reset of a user's smart card. For these solutions, look to the software development kits for the specific smart card vendor or to third-party management systems, such as those available from Alacris ([www.alacris.com](http://www.alacris.com)) and Spyrus ([www.spyrus.com](http://www.spyrus.com)).

## Procedures

A few common procedures can assist you as you deploy smart cards, including:

- Enabling ActiveX control.
- Requesting smart card certificates on behalf of other users.
- Enabling autoenrollment for smart card renewal requests.

### Enabling ActiveX Controls

The Certificate Services Web Enrollment site must be defined as a Local intranet site for all computers in the forest. This allows the automatic passing of authentication credentials to the CA by using Windows Integrated authentication. In addition, the download settings for ActiveX controls must be modified to allow the activation and use of required ActiveX controls.



**Note** For smart card deployment, the ActiveX control settings are only required at the smart card enrollment station. But, if you plan to use the Certificate Services Web Enrollment pages for other certificate distribution, it is recommended that you define the Certificate Services Web Enrollment site as a Local Intranet site at *all* computers in the forest.

The following process defines the Local intranet Web sites:

1. Log on to a Windows XP or Windows 2000 computer as a user who can define Group Policy settings.
2. Open Internet Explorer.
3. From the Tools menu, click Internet Options.
4. Click the Security tab.
5. Click Local Intranet and click Sites.
6. In the Local Intranet dialog box, click Advanced.
7. In the Local Intranet dialog box, add the following Web sites for each network:
  - *http://\*.company.com* (where *company.com* is the DNS namespace used within your organization).
  - *https://\*.company.com* (where *company.com* is the DNS namespace used within your organization).
8. In the Local Intranet dialog box, click OK.
9. In the Local Intranet dialog box, click OK.
10. In the Internet Options dialog box, ensure that Local Intranet is selected and click Custom Level.
11. In the Security Settings dialog box, adjust the following settings (leave all other options at their current settings):
  - Download signed ActiveX controls: Enable
  - Download unsigned ActiveX controls: Disabled
  - Initialize and script ActiveX controls not marked as safe: Prompt
  - Run ActiveX controls and plug-ins: Enable
  - Script ActiveX controls marked safe for scripting: Enable

12. In the Security Settings dialog box, click OK.
13. In the Warning! dialog box, click Yes to change the security settings for the zone.
14. In the Internet Options dialog box, click OK.

Once the correct settings are defined for the Local intranet security zone, you must create a Group Policy Object (GPO) for the application of the Local intranet security zone settings. The following procedure details this process:

1. Open an MMC console.
2. From the Console menu, click Add/Remove Snap-in (use the File menu if using Windows XP).
3. In the Add/Remove Snap-in dialog box, click Add.
4. In the Add Standalone Snap-in dialog box, select Group Policy and click Add.
5. In the Group Policy Wizard, click Browse.
6. In the Browse for a Group Policy Object dialog box, ensure that the Look In drop-down list is focused on the desired domain, right-click the Domains, OUs, and linked Group Policy Objects list, and then click New.
7. Name the new GPO Local Intranet Web Sites.
8. Select Local Intranet Web Sites and click OK.
9. Click Finish.
10. Click Close.
11. Click OK.

Once the GPO is created, you must import the locally defined settings for the Local intranet zone using the following procedure:

1. In the console tree, expand Local Intranet Web Sites, expand User Configuration, expand Windows Settings, expand Internet Explorer Maintenance, and click Security.
2. In the details pane, double-click Security Zones and Content Ratings.
3. In the Security Zones and Content Ratings dialog box, click Import the Current Security Zones and Privacy Settings, and click Modify Settings.
4. Click Local Intranet and click Sites.
5. In the Local Intranet dialog box, click Advanced.
6. Ensure that the *http://\*.company.com* and *https://\*.company.com* Web sites are listed, and click Close.

7. Click OK.
8. Click OK.
9. Click OK.
10. Close the MMC console without saving changes.

The Local Intranet Sites GPO must be linked to each domain in your organization's forest or to an organizational unit (OU) containing the user accounts so that it affects all users in the domain.



**Important** Only a member of the local Administrators group can install the Smart Card Enrollment ActiveX control. The ActiveX control must be pre-downloaded by a local Administrator or a member of the Power Users group. Alternatively, you can add the enrollment agent's user account to either the local Administrators or Power Users group at the smart card enrollment station.

## Requesting Smart Card Certificates on Behalf of Other Users

Once the enrollment agent enrolls a certificate with the Certificate Request Agent application policy OID, he or she can begin enrolling certificates on behalf of other users.

To enroll a smart card from the default Certificate Services Enrollment Web pages:

1. Log on as an enrollment agent.
2. Ensure that a smart card reader is attached to the smart card enrollment station and recognized by the operating system.
3. Verify the user's identity, based on the defined certificate policy. Provide the smart card and PIN to the user only on completion of identity validation.
4. Open Internet Explorer.
5. Open the URL <http://CADNSName/certsrv> (where CADNSName is the DNS name of the CA computer).
6. On the Welcome page, click the Request a Certificate link.
7. On the Advanced Certificate Request page, click Request a Certificate For A Smart Card On Behalf Of Another User By Using The Smart Card Certificate Enrollment Station.
8. In the Internet Explorer dialog box, click Yes to allow the ActiveX control download.

9. Complete the following information on the Smart Card Certificate Enrollment page and click Select User:
  - **Certificate Template:** The required smart card certificate template
  - **Certification Authority:** The nearest CA available in the drop-down list
  - **Cryptographic Service Provider:** Your organization's smart card CSP
  - **Administrator Signing Certificate:** *UserName* (where *UserName* is the user name of the enrollment agent)
10. In the Select User dialog box, in the Enter the Object Name to Select box, type the user account name for the smart card holder, and click OK.



**Important** If the Enrollment Agent certificate is stored on a smart card, the Enrollment Agent smart card and the user's smart card *must* use different CSPs. If the two smart cards use the same CSP, the enrollment request will fail with a message stating that too many smart cards of the same type are inserted.

11. On the Smart Card Certificate Enrollment Station page, click Enroll.
12. In the Confirm Smart Card PIN dialog box, type the PIN for the smart card, click Change PIN After Confirmation, and click OK.
13. In the Change Smart Card PIN dialog box, type a new PIN in the New PIN and Confirm New PIN boxes, and click OK.



**Note** The dialog boxes in steps 12 and 13 might vary, depending on the smart card CSP that your organization deploys.

14. Ensure that the status reports a successful certificate enrollment.
15. Remove the smart card from the smart card reader.
16. Close Internet Explorer.

## Enabling Autoenrollment

If your organization uses autoenrollment for smart card renewal, make sure that the user's account is added to the custom global or universal group assigned Read, Enroll, and Autoenroll permissions for the renewal smart card certificate template. Also ensure that a GPO that enables all user autoenrollment settings is linked to the OU or domain where the smart card user accounts exist.

# Implementing Additional Security for Smart Cards

In addition to deploying smart cards to the users in your organization, security settings in Active Directory and other services further increase network security. They include:

- Requiring smart cards for interactive logon
- Requiring smart cards for remote access logon
- Defining smart card removal behavior
- Using smart cards for administrative tasks

## Requiring Smart Cards for Interactive Logon

Through group policy, you can define whether smart cards are required for interactive logon by using the Interactive Login: Smart Card Required Group Policy setting. This setting—defined in Computer Settings\Windows Settings\Security Settings\Local Policies\Security Options—enforces smart card logon for all users on computers where the Group Policy setting is defined.

Alternatively, you can enable the Smart Card Is Required For Interactive Logon option on the Account tab of the user's object in Active Directory. This method gives you more flexibility in that you can enforce smart cards on a user-by-user basis.



**Warning** Do not enable the Smart Card Is Required For Interactive Logon and the User Must Change Password At Next Logon options for a user account. When you enable the Smart Card Is Required For Interactive Logon option in a Windows Server 2003 environment, the operating system takes over user password management. The operating system assigns a maximum-length password that is equivalent to 255 characters and ensures that the password meets complexity requirements, effectively blocking the user from logging on to the network using a password.



**Important** When you enforce smart card logon in your domain, you must ensure the validity and availability of the CRL Distribution Point (CDP) and Authority Information Access (AIA) URLs in the smart card certificates and all CA certificates in the certification chain. The domain controller accepting the smart card authentication attempt will perform a revocation check on the smart card certificate during the logon process.

## Requiring Smart Cards for Remote Access

To enforce smart card authentication for remote access, you must configure a remote access policy at a remote access server or a RADIUS server to require Extensible Authentication Protocol with Transport Layer Security (EAP/TLS) authentication in the profile settings. When you enforce EAP/TLS authentication, you can select to restrict client certificates to a smart card or other certificate. Designating the Server Authentication certificate used by the server for mutual authentication is the only additional configuration required at the Routing and Remote Access server or the Internet Authentication Services (IAS) server.

## Defining Smart Card Removal Behavior

Group Policy also allows you to define what action takes place when users remove their smart cards from a smart card reader by using the Interactive Login: Smart Card Removal Behavior Group Policy setting. This setting, defined in Computer Settings \Windows Settings\Security Settings\Local Policies\Security Options, ensures that smart card removal behavior is consistent for all computer accounts in the OU or domain where the Group Policy is applied.

In this Group Policy setting, you can define the removal behavior one of three ways:

- **No Action.** The default setting. The removal of the smart card does not lock the workstation or log off the current user.
- **Lock Workstation.** The removal of the smart card causes the workstation to lock. The user must press Log On Interactively or provide the PIN for the smart card to unlock the workstation.
- **Force Logoff.** The user currently logged on is automatically logged off.

## Using Smart Cards for Administrative Tasks

In a pure Windows 2000 network, it was not possible to use smart cards for all administrative tasks. Several tasks still required the input of user credentials and passwords, lessening the security gains accomplished through the issuance and usage of smart cards.

The Windows XP and Windows Server 2003 operating systems offer enhancements that enable additional usage of smart cards in administrative activities, including:



- **The RunAs command.** The RunAs command allows you to run a program in the security context other than that of the currently logged on user. For example, if administrators have day-to-day accounts and smart cards for administrative tasks, they can use the RunAs command to run administrative tasks with their smart cards, whether accessed via the graphical user interface (GUI) or from the command line. From the command line, you can add the /smartcard switch; from the GUI, you can select to use a smart card for authentication.
- **The Net Use command.** Like the RunAs command, you can choose to use a smart card to provide credentials for network drive mapping. From the command line, you must use the /smartcard switch to designate that the credentials are read from a smart card. Likewise, from the GUI, you can choose to connect with a different user name and then select the smart card from the list of available credentials.
- **The DCPromo command.** If the computer you are promoting to a domain controller is already a member of the forest, you can use a smart card to validate your identity in the DCPromo wizard. The computer must be a member of the forest before running DCPromo, otherwise the option is not available. This option is only available on Windows Server 2003 computers.
- **Terminal Services.** A user can use his or her smart card to connect to the Remote Desktop Service (or Terminal Services) running on Windows XP or Windows Server 2003, as long as the computer is a member of an Active Directory domain. The Windows XP and Windows Server 2003 Remote Desktop client accepts smart cards as a form of authentication and passes the credentials to the remote computer.



**Warning** If you are using a third-party CSP, it must be loaded at both the remote client and the remote desktop server so that the smart card is recognized at each end of the Terminal Services connection.

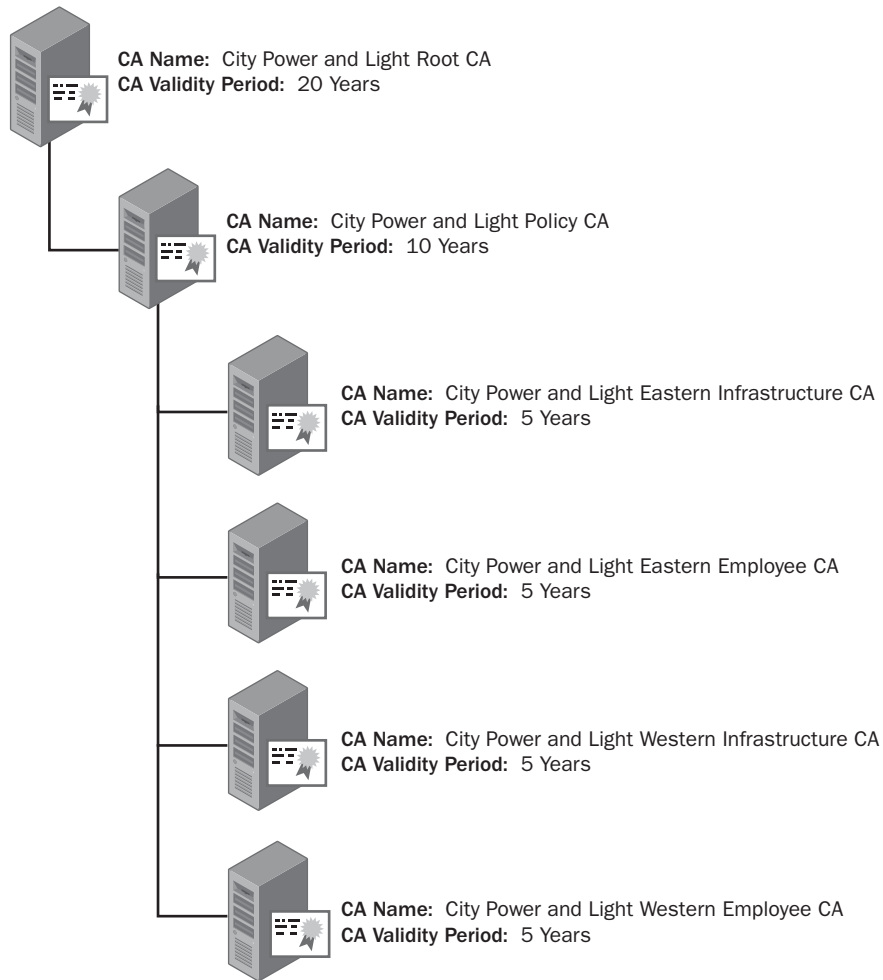
## Best Practices

- **Add the Certificate Services Web Enrollment pages to the Local intranet security zone in Internet Explorer.** Allows you to ensure that the Local intranet zone has the correct ActiveX settings to enable download of the Smart Card Enrollment ActiveX control.

- **Choose one smart card vendor for smart card deployment.** Reduces the complexity of smart card management, allowing a single toolset to be used.
- **Create a custom version 2 certificate template, based on the Enrollment Agent certificate, that requires CA certificate manager approval.** Increases the assurance level of the certificate by requiring approval of a certificate manager before the certificate is issued. Consider performing background checks on enrollment agents before issuing the certificate to ensure they meet your organization's security policies.
- **Establish a smart card management system before deploying smart card certificates.** Ensures that your management system addresses the initial assignment of PINs to the smart cards, remote unlocking of smart cards, and remote resets of smart card PINs.
- **If using a custom version 2 smart card certificate, add an issuance requirement to sign the request with a certificate with the Certificate Request Agent OID.** Ensures that the custom smart card certificate is available for enrollment on the Smart Card Enrollment Page.
- **Limit access to the Enrollment Agent certificate template.** The holder of an Enrollment Agent certificate can request a smart card certificate on behalf of any user in Active Directory. Only assign Read and Enroll permissions to a custom global or universal group with limited permissions.
- **Remove the Enrollment Agent certificate template from all CAs, unless enrollment is required.** Ensures that no Enrollment Agent certificates are accidentally deployed to unauthorized users.
- **Use an enrollment agent for all initial smart card requests.** Increases the assurance of the smart card certificates, allowing the enrollment agent to perform any identity validation requirements defined by an organization's certificate policy before issuing the smart card certificate.
- **Use autoenrollment for smart card certificate renewal only.** Autoenrollment does not enforce strong validation of the user's identity. You can increase the assurance level of autoenrollment by requiring the user to sign the request with his or her existing smart card certificate.

## Case Study: City Power and Light

You manage the team deploying PKI-enabled applications for City Power and Light, the largest power producer in the region. The CA hierarchy deployed by City Power and Light is shown in Figure 15-1.



**Figure 15-1** The City Power and Light CA hierarchy

City Power and Light wants to deploy smart cards to network administration staff so that smart cards, rather than accounts and passwords, are used for administrative authentication. The following design requirements have been identified for the administrator smart card deployment:

- All administrators will have two user accounts: one for day-to-day tasks and one for all network administrative tasks.
- Smart cards must be enforced for authenticating all administrative tasks. The smart cards will not be used for any purpose other than authentication.

- The company will use 32 KB Schlumberger Cryptoflex cards.
- Andy will be the only enrollment agent for all smart cards issued.
- The Enrollment Agent certificate issued to Andy must be authorized by the certificate manager at the Atlanta office where the City Power and Light Eastern Employee CA is located.
- All administrators must present their current City Power and Light employee badges for identity validation before smart card issuance.
- For new administrative hires, employee badges must be issued before Andy can issue administrative smart cards.
- Smart card certificates can be issued by the City Power and Light Eastern Employee CA or the City Power and Light Western Employee CA.
- For administrators, smart card logon will be enforced for both interactive and remote access logons.
- When an administrative smart card certificate expires, the administrator must return to Andy for identity validation before the smart card certificates are renewed.
- All administrators will be issued Windows XP desktop computers with an integrated smart card reader in the keyboard.

## Case Study Questions

1. Can you use the default Enrollment Agent certificate template to meet the design requirements for City Power and Light? Why or why not?
2. If you create a custom certificate template for the enrollment agent, how do you enforce that only Andy receives a custom enrollment agent certificate?
3. How do you enforce the Atlanta certificate manager's authorization of the Enrollment Agent certificate issued to Andy?
4. Can you use the default Smart Card User certificate template for the administrative smart cards?
5. Do you have to use a custom certificate template to meet the design goals of City Power and Light?
6. How do you limit enrollment of the smart card certificate template to Andy?
7. Assuming that the administrators can log on from both servers and desktop workstations spread among any OU in the forest, how do you enforce smart cards for interactive logon for the Administrator accounts?

8. If the administrators are to use Terminal Services to administer servers, where must you install the updated Schlumberger smart card CSP?
9. How do you enforce smart card authentication for remote access connections by the administrative staff?

## Additional Information

- Microsoft Official Curriculum, Course 2821: “Designing and Managing a Windows Public Key Infrastructure” ([www.microsoft.com/traincert/syllabi/2821afinal.asp](http://www.microsoft.com/traincert/syllabi/2821afinal.asp))
- “The Smart Card Deployment Cookbook” ([www.microsoft.com/technet/Security/topics/smrtdcb/default.msp](http://www.microsoft.com/technet/Security/topics/smrtdcb/default.msp))
- “The Smart Card Cryptographic Service Provider Cookbook” (<http://msdn.microsoft.com/library/en-us/dnscard/html/smartcardcspcook.asp>)
- “Windows 2000 Server: How to Configure the Windows 2000 Environment for Smart Cards” ([www.microsoft.com/technet/community/events/windows2000srv/tnt1-49.msp](http://www.microsoft.com/technet/community/events/windows2000srv/tnt1-49.msp))
- “Troubleshooting Windows 2000 PKI Deployment and Smart Card Logon” ([www.microsoft.com/windows2000/techinfo/administration/security/smrtdtr.asp](http://www.microsoft.com/windows2000/techinfo/administration/security/smrtdtr.asp))
- “Spyrus SIGNAL Identity Manager” ([www.spyrus.com/content/products/SIGNALIdentityManager\\_N7.asp](http://www.spyrus.com/content/products/SIGNALIdentityManager_N7.asp))
- “Alacris idNexus Registration Authority” ([www.alacris.com/products/products\\_idNexus.htm](http://www.alacris.com/products/products_idNexus.htm))
- Knowledge Base Article 227873: “Smart Card Removal Options in Windows 2000”
- Knowledge Base Article 248753: “Description of PKINIT Version Implemented in Kerberos in Windows 2000”
- Knowledge Base Article 257480: “Certificate Enrollment Using Smart Cards”
- Knowledge Base Article 259880: “Configuring a VPN to Use Extensible Authentication Protocol (EAP)”
- Knowledge Base Article 281245: “Guidelines for Enabling Smart Card Logon with Third-Party Certification Authorities”
- Knowledge Base Article 295663: “How To: Import a Third-Party Certificate into the NTAAuth Store”

- Knowledge Base Article 313490: “How To: Enroll a Certificate on Behalf of Another for Smart Cards Users”
- Knowledge Base Article 313629: “Custom Smartcard Template Is Not Available on the Smart Card Enrollment”
- Knowledge Base Article 326474: “HOW TO: Troubleshoot VPN with Extensible Authentication Protocol (EAP)”



**Note** Microsoft Knowledge Base articles can be found at <http://support.microsoft.com>. Enter the article number in the Search the Knowledge Base text box.

## Chapter 16

# Encrypting File System

The Encrypting File System (EFS) provides a method to encrypt files on a local file system in Microsoft Windows 2000, Windows XP, and Windows Server 2003, but it is important to note that file encryption takes place on the local file system only. For example, if you store a file on a file server, it is encrypted on the file server's local file system. When the file is accessed, it is decrypted at the file server and then transmitted (in an unencrypted state) to the remote computer.



**Note** Of course, there is an exception to every rule. If you use Web Distributed Authoring and Versioning (WebDAV), or Web folders, rather than Server Message Blocks (SMBs) or Common Internet File System (CIFS), the file is encrypted locally at the remote computer and the encrypted file is transferred to and from the remote file server.

This chapter will focus on the public key infrastructure (PKI) aspects of deploying EFS on your organization's network. There are many more design decisions that must be addressed before you enable EFS. For a larger discussion of those decisions, see "Encrypting File System in Windows XP and Windows Server 2003," referenced at the end of this chapter under "Additional Information."



**Tip** This chapter will demonstrate how to distribute certificate(s) based on custom version 2 templates with the required Encrypting File System OID to users so that the certificate exists in their certificate store when they attempt to encrypt their first file. This certificate is typically distributed through Autoenrollment settings so that the certificate exists in the user's certificate store prior to file encryption.

## EFS Processes

Before addressing the PKI-related design decisions for EFS, it's important to understand how EFS protects data on a Windows 2000, Windows XP, or Windows Server 2003 computer. This section looks at the following processes:

- How Windows chooses an EFS encryption certificate.
- The EFS encryption process for a local file.
- The EFS encryption process for files stored on a remote file server.
- The EFS encryption process for files stored using WebDAV.
- The EFS decryption process.
- The EFS recovery process.

### How Windows Chooses an EFS Encryption Certificate

When a user performs the first file encryption using EFS, the following process takes place to designate or acquire an EFS-enabled certificate:

1. The user's registry is queried to determine whether a certificate is currently designated as the default EFS encryption certificate.



**Note** The actual registry value queried is `HKCU\Software\Microsoft\Windows NT\CurrentVersion\EFS\CurrentKeys\CertificateHash`. This registry value contains the contents of the thumbprint property of the designated EFS encryption certificate.

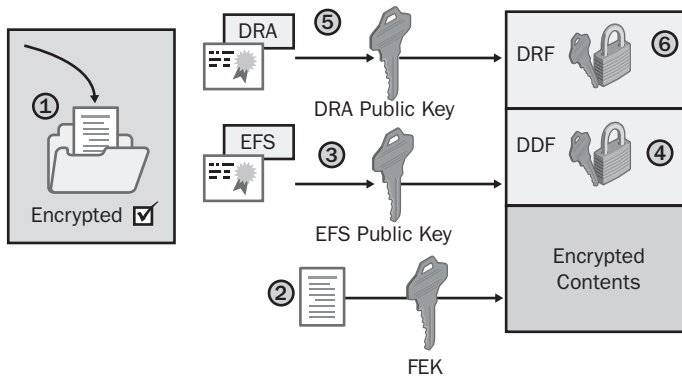
2. If a default certificate is not designated, EFS must determine whether the user has an acceptable certificate for EFS encryption (before encrypting a file), as follows:
  - a. The user's certificate store is queried to determine whether a certificate exists with the Encrypting File System object identifier (OID): 1.3.6.1.4.1.311.10.3.4. If a certificate is found with this OID in the application policy or Enhanced Key Usage (EKU) extension, this certificate is designated as the EFS encryption certificate.
  - b. If no certificate is found with the Encrypting File System OID and the computer is a member of a domain, an automated request for a Basic EFS certificate is sent, one at a time, to each enterprise CA in the forest. When the certificate is enrolled successfully, it is designated as the EFS encryption certificate in the user's registry.



- c. If the Basic EFS certificate template is not available at an enterprise CA or the computer is not a member of a domain, EFS generates a self-signed certificate with the Encrypting File System OID. The self-signed certificate is issued by and to the user. It is then designated as the default EFS encryption certificate in the user's registry.

## Local EFS Encryption

Once an EFS encryption certificate is designated, the EFS encryption process can begin. (See Figure 16-1.)



**Figure 16-1** The EFS encryption process

1. A user must choose to encrypt a file. This can be done by enabling an individual file for EFS encryption or by creating a file in a folder that is enabled for EFS encryption.
2. The user's computer generates a random encryption key, called a File Encryption Key (FEK), used to encrypt the file. The symmetric encryption algorithm used by the FEK depends on the version of the computer's operating system:
  - For Windows 2000, the Data Encryption Standard XORed (DESX) algorithm is used to encrypt the file.
  - For Windows XP with no services packs, the Triple DES (3DES) algorithm can be used to encrypt the file, instead of DESX.
  - For Windows XP with Service Pack 1 or later or Windows Server 2003, the Advanced Encryption Standard (AES) with a 256-bit key is used to encrypt the file.



**Note** For more information on how these encryption algorithms work, review Chapter 1, “Basics of Cryptography.”

3. The computer retrieves the user's designated EFS certificate and obtains the user's public key from the certificate.
4. The computer encrypts the FEK by using the Rivest Shamir Adleman (RSA) asymmetric encryption algorithm with the user's public key and places the encrypted FEK in the Data Decryption Field (DDF) in the file's header.



**Note** In Windows XP or Windows Server 2003, the DDF can contain multiple entries, allowing multiple users to share an encrypted file. In Windows 2000, only a single DDF can be defined through the user interface.

5. The computer retrieves the certificate for each EFS recovery agent—also known as the data recovery agent (DRA)—from the local computer configuration for workgroup members or by determining the resultant set of policy for Microsoft Active Directory for domain members, and extracts each EFS recovery agent's public key.
6. The computer encrypts the FEK by using the RSA encryption algorithm with the retrieved EFS Recovery Agent's public key and places the encrypted FEK in the Data Recovery Field (DRF) in the file's header.



**Note** If multiple EFS Recovery Agents are designated, multiple entries will be stored in the DRF, one for each defined EFS Recovery Agent.

## Remote EFS Encryption Using SMB

When you perform remote file encryption using server message block (SMB), the file is encrypted at a remote file server in a share created on the file server. Encryption is performed by allowing the remote file server to impersonate the user.



**Important** The computer account of the remote file server must have the Trusted for Delegation option enabled for its computer object in Active Directory. This allows the computer to impersonate the user through Kerberos delegation.

When the computer account impersonates a user, it loads a user profile for the user account on the local file system and follows the same process to determine whether an EFS certificate exists for the user account. If you implement roaming profiles, the same EFS encryption certificate is used at the remote file server. If you do not implement roaming profiles, a different EFS encryption certificate will be used at each file server where EFS encryption is enabled.

## Remote EFS Encryption Using WebDAV

An alternative to allowing EFS encryption on file servers by using CIFS is to implement WebDAV, or Web folders, at the remote file server. Rather than connecting to the file server on TCP port 445 (or TCP port 139 for the older SMB protocol), the server allows connections through the Hypertext Transmission Protocol (HTTP) port, TCP port 80 or TCP port 443 if Secure Socket Layers (SSL) is implemented.

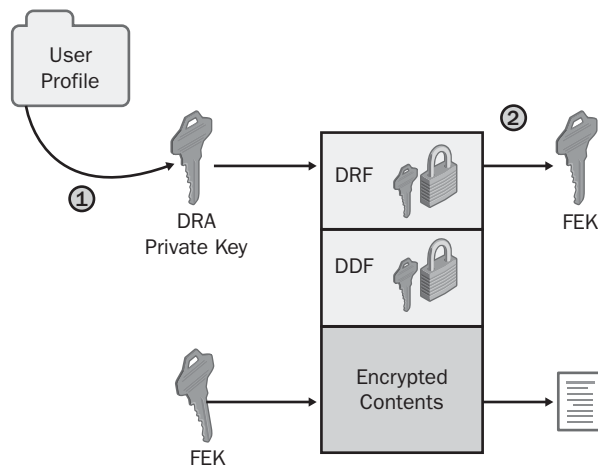
The benefit of using WebDAV is that file encryption takes place on the local computer rather than the remote file server. This provides better data protection as the file is transmitted from the client's computer to the remote file server.

When a Windows XP client connects to a WebDAV access point on a remote server, files are encrypted locally on the client and then sent to the WebDAV server as an encrypted file using an HTTP PUT command.

Likewise, when a Windows XP client connects to the WebDAV access point to open a previously encrypted file, the encrypted file is transmitted to the Windows XP client via an HTTP GET command and then decrypted locally on the client.

## EFS Decryption

When an EFS-encrypted file is opened by a user with access to the FEK in the DDF information, EFS decryption (see Figure 16-2) takes place, as follows:



**Figure 16-2** The EFS decryption process

1. When the user attempts to open the encrypted file, the computer retrieves the private key of the certificate used to encrypt the FEK in the DDF. The private key is retrieved from the current user's personal store.



**Note** As long a user has access to a private key associated with the public key used to encrypt the FEK in a DDF, they can open an EFS-encrypted file. The user's name does not have to match the user name stored in the subject of the certificate.



**Note** The user attempting to open the EFS encrypted file must be assigned the Read and Execute and Read NTFS permissions to open the file.

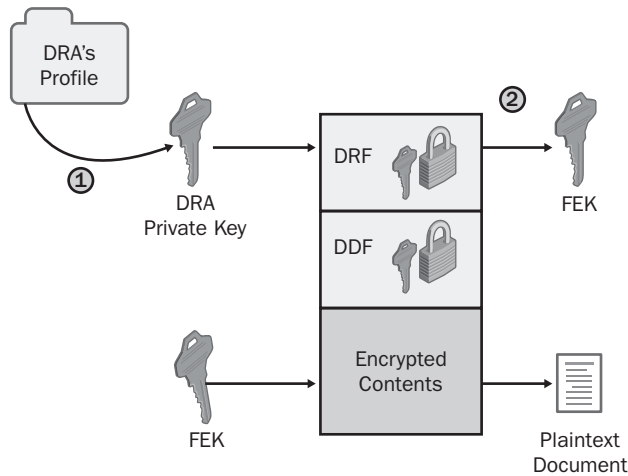
2. The computer uses the private key from the user's store to decrypt the FEK from the DDF.
3. The user's computer uses the FEK to decrypt the file.



**Note** The file is decrypted in memory so that the application accessing the file can read the unencrypted file. The version of the file stored on the hard drive remains encrypted.

## EFS Data Recovery

When a designated EFS recovery agent attempts to access an EFS-encrypted file, a process similar to the EFS decryption process takes place. (See Figure 16-3.) The only difference is that the FEK is retrieved from the DRF rather than the DDF. When the recovery agent attempts to open the file:



**Figure 16-3** The EFS recovery process

1. The computer retrieves the private key of the certificate used to encrypt the FEK in the DRF.



**Note** The name of the user does not have to match the subject name in the EFS certificate. As long as the user has access to a private key associated with the public key used to encrypt the FEK in a DDF, he or she can open the EFS-encrypted file.



**Note** The Recovery Agent's user name does *not* have to match the user name in the EFS Recovery Agent certificate's subject. The recovery agent only has to have access to the PKCS #12 file containing the Recovery Agent certificate and private key and import the certificate and private key into his or her user profile.

2. The computer uses the private key from the EFS Recovery Agent's user store to decrypt the FEK from the DRF.
3. The user's computer uses the FEK to decrypt the file.

## One Application, Two Recovery Methods

With the introduction of Windows Server 2003 PKI, EFS now allows two methods to recover an EFS-encrypted file when a user no longer has access to his or her EFS-encryption private key:

- **Data recovery.** An EFS Recovery Agent disables EFS encryption. Once the file is decrypted, the user can open the plaintext file and then re-encrypt the file using a newly issued certificate with the Encrypting File System OID.
- **Key recovery.** The user's original certificate and private key are recovered from the CA database and restored to the user's profile. Recovery of the user's certificate and private key allows the user to access the FEK stored in the DDF of the EFS-encrypted file, returning access to the file to the user.

The following sections discuss some of the design decisions an organization faces when choosing between data recovery and key recovery, or a mix of both.

## Data Recovery

Data recovery allows a designated EFS Recovery Agent to decrypt all EFS-encrypted files on a computer. By default, where the private key associated with the EFS Recovery Agent certificate exists depends on the domain membership of a computer. If the computer is a member of:

- **A domain** The EFS recovery agent's certificate and private key are stored in the Administrator's profile of the first domain controller in a domain. When the first domain controller is promoted as a domain controller for the newly created domain, the local administrator's EFS Recovery Agent certificate is designated as the domain's EFS Recovery Agent.
- **A workgroup** The EFS Recovery Agent's certificate and private key are stored in the user profile of the first member of the local Administrators group who logs on at the Windows 2000 computer. This is usually the local Administrator account, but it can be another account.



**Caution** Deploying EFS in a workgroup environment is risky. The storage of the EFS Recovery Agent's key pair on the local file system makes the computer subject to alternate operating system attacks, such as the Nordahl attack, that attempt to gain access to the key pair through other operating systems. It is recommended to deploy Syskey.exe with the system set to require either a password or a disk with the system key password at boot up before allowing access to the local hard disk. For more information on the system key, see Chapter 13, "Securing Mobile Computers," and Chapter 14, "Implementing Security for Domain Controllers," in my book with Ben Smith, *Microsoft Windows Security Resource Kit* (Microsoft Press, 2003).

A common misconception is that the Administrator account is the EFS Recovery Agent. Remember that EFS is a PKI-enabled application and has nothing to do with the user account. It only depends on who has the EFS Recovery Agent certificate's associated private key. You can lose access to the EFS Recovery Agent's private key in the following circumstances:

- If you remove the first domain controller in a domain environment.
- If you overwrite the Administrator profile with a roaming profile created at another computer.
- If you delete the Administrator profile on the first domain controller in the domain or on the local computer in a workgroup.



**Important** If you overwrite or lose the EFS Recovery Agent's private key, you must designate a different EFS Recovery Agent for data recovery.

## Defining EFS Recovery Agents

Defining an EFS Recovery Agent involves two steps:

1. Obtain a certificate with the File Recovery application policy OID (or EKU if using Windows 2000).
2. Designate the certificate as the EFS Recovery Agent (in the domain or local group policy).

### Obtain an EFS Recovery Agent Certificate

The first step is to ensure that the user assigned the EFS Recovery Agent role acquires an EFS Recovery Agent certificate. An EFS Recovery Agent certificate includes the File Recovery application policy OID (1.3.6.1.4.1.311.10.3.4.1). There are four ways this type of certificate can be obtained:

- Request a certificate based on the EFS Recovery Agent certificate template. You must modify the default template permissions to assign Read and Enroll permissions.
- Request a certificate based on a custom version 2 certificate template based on the EFS Recovery Agent certificate template. The advantage of a version 2 certificate template is that you can require CA certificate manager approval before issuance.

- Use the **cipher /R:filename** command to generate a certificate file and a PKCS #12 file containing the private key on a Windows XP or Windows Server 2003 computer.
- In a Group Policy Object (GPO), right-click the *Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Encrypting File System* policy, and then click Create Data Recovery Agent.



**Note** The Create Data Recovery Agent option requires that the EFS Recovery Agent certificate template be available for enrollment at an enterprise CA in the forest, and that the user performing the procedure is assigned the Read and Enroll permissions for the EFS Recovery Agent certificate template.

### Designate the EFS Recovery Agent.

Once you issue the certificate with the File Recovery application policy OID, you must import the certificate, as follows:

- In a domain environment, you can import the EFS Recovery Agent's certificate into the *Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Encrypting File System* policy of a GPO. The GPO must be linked to the organizational unit (OU) where the user's computer account, not the user account, exists. The certificate can be imported from either a Base-64 or DER-encoded certificate file, or from Active Directory if the certificate template enables publication of the certificate file.
- In a workgroup environment, you can import the EFS Recovery Agent's certificate into the *Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Encrypting File System* policy (of the local computer). In this scenario, the EFS Recovery Agent certificate must be imported from a file.



**Note** If you generated the EFS Recovery Agent certificate by using the Create Data Recovery Agent option in Group Policy, you do not have to import the certificate. The EFS Recovery Agent certificate is automatically added to the GPO policy.



## Choosing EFS Recovery Agents

---

If you work for a large organization, you should provide the internal audit department with the private key associated with the EFS Recovery Agent certificate. Members of the Internal Audit department can then import the certificate and private key and open any file stored on the corporate network without intervention by network administrators when performing an audit. Removing control of the private key from the network administrator also prevents the network administrator from opening encrypted files.

Large organizations might also require more than one EFS recovery agent. In forests with multiple domains, an organization can implement a different EFS recovery agent per domain. Rather than having disjointed EFS recovery agents, consider implementing two EFS recovery agents at each domain: one EFS recovery agent that is unique to the domain and another that is common to all domains in the forest. The common EFS recovery agent provides the organization with centralized recovery and the unique EFS recovery agent provides decentralized recovery.

## Securing the Private Keys

Once you designate one or more EFS Recovery Agents, it is recommended that you remove the EFS Recovery Agent's private key from any user profile. This protects against an attacker attempting to log on as the EFS Recovery Agent and accessing the private key.

To remove the EFS Recovery Agent certificate and private key from the user's profile, you can export the certificate and private key and enable the options to *Delete the private key if export is successful* and *Enable strong private key protection*. These options ensure that the private key is removed from the user's profile and that the PKCS #12 export file is protected with a password.

## Are there any restrictions on EFS certificates?

---

There are two restrictions on EFS certificates:

- **You cannot store the EFS certificates on a smart card.** The EFS decryption and recovery processes are hard-coded to work only with software-based cryptographic service providers (CSPs) and will not access a private key that uses a smart card CSP. In addition, today's smart card CSPs do not support Rivest Shamir Adleman (RSA) encryption of symmetric key material generated outside of the CSP.

- **You cannot protect the EFS certificate with strong private key protection.** The EFS decryption and recovery processes are performed by the Local Security Authority (LSA) in Kernel mode. To input the password protecting the user certificate, the LSA must be exposed to the desktop, which is a security risk. Exposure of the LSA to the desktop is not allowed to prevent this security risk.

## Key Recovery

You can enable key recovery for EFS encryption certificates. This allows the recovery of a lost EFS encryption private key without the intervention of an EFS Recovery Agent. A certificate manager extracts the encrypted private key from the CA database and a key recovery agent decrypts the private key and distributes the resulting PKCS #12 file to the original user, allowing the original user to import the private key back into the user profile.



**Note** Enabling key recovery at an enterprise CA running on Windows Server 2003, Enterprise Edition, is covered in Chapter 14, “Archiving Encryption Keys.”

## Deploying EFS

The deployment scenario that follows assumes that you implement key recovery and data recovery for an organization’s EFS implementation. To deploy this solution, you must define the necessary certificate templates and plan how to deploy certificates to users.

### Enabling and Disabling EFS

An organization might not want to allow EFS encryption on all Windows 2000 or Windows XP network computers, preferring instead to enable EFS encryption for specific OUs or domains.

#### Enabling EFS

To enable EFS encryption on a Windows 2000 computer, you must ensure that an EFS recovery policy is implemented at the domain or OU containing the computer account that designates one or more EFS Recovery Agent certificates. Windows XP can implement EFS encryption without designating an EFS Recovery Agent.



**Note** In a Windows 2000 domain, EFS is enabled by default. The EFS Recovery Agent certificate's private key is stored in the first Administrator's profile on the first domain controller installed in the domain.

## Disabling EFS

To disable EFS encryption on a Windows 2000 computer, you must implement an empty EFS recovery policy, where an EFS recovery policy is designated with no EFS Recovery Agent certificates.



**Note** Enabling an empty EFS recovery policy is different than implementing no EFS recovery policy. If no EFS recovery policy is implemented, the client computer implements the EFS encryption settings defined in the local security policy.

To disable EFS encryption on a Windows XP computer, you must configure Group Policy to block EFS encryption. This is accomplished using the following procedure:

1. Link a new GPO to the OU where the Windows XP computer accounts exist.
2. Open the GPO in the Group Policy Editor.
3. In the console tree, navigate to *Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Encrypting File System*.
4. In the console tree, right-click Encrypting File System and click Properties.
5. In the Encrypting File System Properties dialog box, disable the Allow users to encrypt files using Encrypting File System (EFS) check box, and click OK.

## Certificate Templates for EFS Encryption

Three certificate template are required when deploying an EFS encryption solution with both data recovery and key recovery:

- An EFS Recovery Agent certificate template
- A Key Recovery Agent certificate template
- An EFS user certificate template

The sections that follow describe the specific configuration recommendations for each certificate template.

## EFS Recovery Agent Certificate Template

It is recommended that you create a version 2 certificate template based on the EFS Recovery Agent certificate template. The advantage of creating a version 2 certificate template is that you make the certificate request subject pending and require a certificate manager's approval to issue the certificate, increasing the assurance, or trust, of the EFS Recovery Agent certificate.

Table 16-1 shows the recommended settings for the version 2 EFS Recovery Agent certificate template.

**Table 16-1 EFS Recovery Agent Certificate Template Settings**

Tab	Actions
General	Template Display Name: <i>Company</i> EFS Recovery Agent Template Name: <i>Company</i> EFSRecoveryAgent Validity Period: Two years Publish certificate in Active Directory: Enabled
Request Handling	No modifications
Subject Name	No modifications
Issuance Requirements	CA certificate manager approval: Enabled
Superseded Templates	EFS Recovery Agent.
Extensions	No modifications
Security	Assign a custom universal or global group Read and Enroll permissions. Remove the assignment of the Enroll permission from any other security principals.



**Note** Publishing the certificate in Active Directory allows an administrator to select the certificate from Active Directory rather than having to import the EFS recovery agent's certificate from an export file.



**Note** If a user already has an EFS Recovery Agent certificate in their user certificate store, the enrollment attempt of a *Company* EFS Recovery Agent certificate will result in the EFS Recovery Agent certificate being archived in the user certificate store.

## Key Recovery Agent Certificate Template

The default version 2 certificate template implements all recommended settings for EFS key recovery. The only required modification for the Key Recovery Agent certificate template is to assign Read and Enroll permissions to a custom universal or global group. In addition, Read and Enroll permissions should be removed from the Administrators, *ForestRootDomain*\Domain Admins and *ForestRootDomain*\Enterprise Admins groups.

## EFS User Certificate Template

It is recommended that you create a custom version 2 certificate template based on the default Basic EFS certificate template. The custom certificate template allows an organization to implement both private key archival and autoenrollment of certificates for users with Windows XP client computers. Table 16-2 shows the recommended settings for the custom certificate template.

**Table 16-2 EFS User Certificate Template Settings**

Tab	Actions
General	Template Display Name: <i>Company</i> EFS Template Name: <i>CompanyEFS</i> Validity Period: Two years Publish certificate in Active Directory: Enabled
Request Handling	Purpose: Encryption Archive subject's encryption private key: Enabled Include symmetric algorithms allowed by the subject: Enabled Minimum Key Size: 1,024 bits Allow private key to be exported: Enabled Enroll subject without requiring any user input: Enabled
Subject Name	No modifications
Issuance Requirements	No modifications
Superseded Templates	Basic EFS
Extensions	In the Application Policies listing, in addition to the Encrypting File System OID (1.3.6.1.4.1.311.10.3.4), you can create a custom OID based on the organization's OID space. This custom OID can be used in CryptoAPICOM (CAPICOM) scripts to determine whether the certificate is a custom EFS certificate rather than a Basic EFS certificate or another default certificate template (such as the User certificate template that includes the Encrypting File System OID).
Security	The permissions assignment depends on who requires EFS encryption certificates. If all users require EFS encryption abilities, assign the Authenticated Users group Read, Enroll, and Auto-enroll permissions.

By deploying the certificate (based on this template) to all users, you then have an EFS certificate with key archival enabled before they start encrypting files.

## Certificate Enrollment

Once you design the three certificate templates, you must publish the certificate templates at one or more enterprise CAs in the forest. After the certificates are available for enrollment, the two methods that follow are recommended for issuing the certificates.

### EFS Recovery Agent and Key Recovery Agent Certificates

It is recommended that you deploy EFS Recovery Agent and Key Recovery Agent certificates by using the Certificate Services Web Enrollment pages. This procedure is covered in Chapter 14, “Archiving Encryption Keys.”



**Note** Once all designated EFS Recovery Agents or key recovery agents acquire their certificates, you can remove the two certificate templates from the enterprise CA. Removing the certificate ensures that no additional certificates are issued.

### EFS User Certificates

The method you use to distribute the EFS User certificates to user accounts depends on the operating system:

- For Windows XP clients, it is recommended that you deploy the EFS encryption certificates by using Autoenrollment Settings in Group Policy. This method triggers the users who have user accounts in the OU where the Autoenrollment Settings GPO is applied to acquire the certificates by using autoenrollment when the user logs on to the network.
- For Windows 2000 clients, users must manually enroll certificates through the Certificate Services Web Enrollment pages via the Advanced Certificate Request page. This page enables users to select the version 2 certificate template and enroll the certificate.



**Important** A user with a computer running Windows 2000 cannot use the Certificate Enrollment Wizard to enroll certificates based on a version 2 certificate template. The Certificates console, where the Certificate Enrollment Wizard is launched, only displays version 1 certificate templates on a Windows 2000 computer.



**Note** You can automate certificate enrollment by creating a custom enrollment script that uses the Certificate Enrollment Control. The custom script should use CAPICOM to determine whether the user already has a certificate with both the Encrypting File System application policy OID and the custom EFS application policy OID, as recommended in Table 16-2.

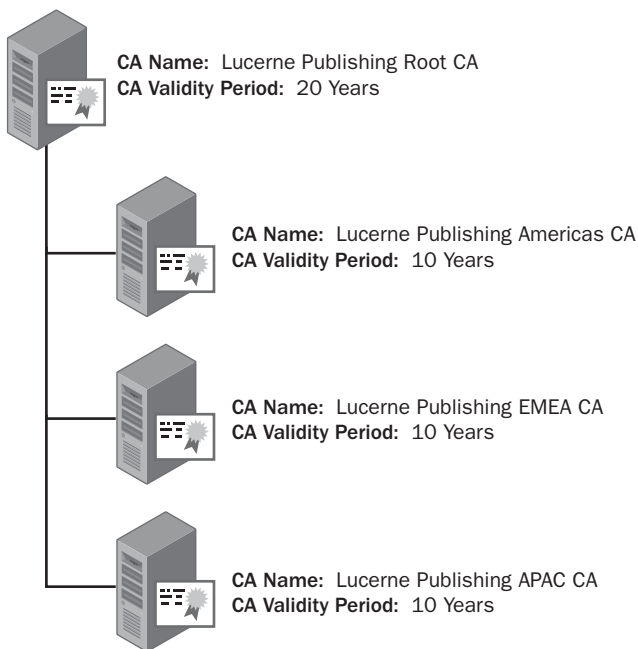
## Best Practices

- **When you deploy notebook computers, ensure that the notebooks are members of the organization's Active Directory.** Domain members are protected against disk attacks, such as the Nordahl attack, because the DRA's private key is not stored on the local disk medium of the notebook computer.
- **Enable the Store And Retrieve Archived Keys auditing option at a CA where key archival is enabled.** By enabling this auditing setting, you ensure that all key recovery operations are tracked in the CA's security event log.
- **Enforce role separation of certificate managers and key recovery agents.** If you implement role separation, you ensure that a minimum of two people are involved in any key recovery process.
- **If an encryption certificate's private key is compromised, revoke the certificate before performing the key recovery operation.** By revoking the certificate, you ensure that the private key of the certificate can be used only to decrypt EFS-encrypted files. The certificate cannot be used to encrypt new files.
- **If implementing key recovery, ensure that the EFS-enabled certificate with private key archival is distributed to workstations before EFS encryption is performed.** By deploying a certificate with the Encrypting File System application policy OID, you ensure that the EFS-enabled certificate with private key archival is used for all EFS-encrypted data.
- **Implement a central recovery workstation for EFS data recovery.** An EFS-encrypted file can be restored to the central recovery station by using a backup utility to back up encrypted files from the source workstation and then restoring those files to the central recovery machine. In this configuration, the DRA's private key can be stored on the recovery machine permanently or imported as required. This method prevents the DRA's private key from being exposed to the network from a typical workstation.

- **Implement Data Recovery Agent certificates from a CA.** Rather than using the default, self-signed EFS Recovery Agent certificate, implement a CA-issued certificate, which can be revoked or renewed and has a configurable expiration date.
- **Plan which folders on the workstation are enabled for encryption.** By encrypting common folders such as My Documents and temporary folders, you can ensure that any data saved in these folders is encrypted.
- **Store the Key Recovery Agent certificate and private key on a smart card or other hardware-based cryptographic service provider.** This ensures that the Key Recovery Agent's certificate is not susceptible to disk attacks.
- **Use syskey in mode 2 with a boot floppy or mode 3 with a boot password for nondomain member computers.** Setting the system key (syskey) to mode 2 or mode 3 prevents attacks that use an alternate operating system to access the EFS private key material stored on the local disk subsystem.

## Case Study: Lucerne Publishing

You manage the CAs for Lucerne Publishing, a global publishing company that has implemented a two-tier CA hierarchy, as shown in Figure 16-4.



**Figure 16-4** The Lucerne Publishing CA hierarchy



## Scenario

Last year, a Lucerne Publishing acquisitions editor's laptop was stolen. One of the files on the laptop was a listing of proposed book titles on computer security. Within six months of the theft, a rival publishing company released titles based on the same topics.

To prevent a similar incident, Lucerne Publishing wants to enable EFS encryption on all laptops to ensure that sensitive data is protected.

## Design Requirements

The following design requirements are provided to you:

- Only the Lucerne Publishing Americas CA is enabled for key archival. Three key recovery agents are defined at the CA: one from Europe, one from Asia, and one from the Americas. The Lucerne Publishing Americas CA uses all three Key Recovery Agent certificates when archiving a private key. The users acting as key recovery agents are members of the Enterprise Admins group.
- All notebook computers were recently upgraded to Windows XP Professional. The notebooks are all members of the lucernepublish.msft domain, and their computer accounts are in the organizational unit named OU=Notebooks,OU=Computer Accounts,DC=lucernpublish,DC=msft.
- Lucerne Publishing implements both Windows 2000 Professional and Windows XP Professional on the desktop computers.
- EFS encryption must be enabled for Windows XP notebook computers only. EFS encryption must be disabled on all other computers.
- The EFS encryption certificates must be deployed to all notebook users without user intervention. The private key of the EFS encryption certificate must be archived to allow key recovery operations.
- The internal audit department must be able to open any file stored on a Lucerne Publishing computer asset. If an EFS private key cannot be retrieved from the CA database, the internal audit performs data recovery to allow the user to regain access to the EFS-encrypted file.
- If a user's profile is deleted, the first attempt to regain access to the EFS certificates must use key recovery. Data recovery is implemented only if key recovery fails to regain access to an EFS-encrypted file.

## Proposed Solution

You assign Andy, a member of your department, the task of developing a solution that meets these design requirements. This is Andy's proposal

- The default EFS Recovery Agent and Key Recovery Agent certificate templates are used for the EFS project. The certificate templates are published only at the Lucerne Publishing Americas CA.
- Key recovery agents are defined at each issuing CA in the CA hierarchy. The key recovery agent for each region is designated as the only key recovery agent for that region's issuing CA.
- Permissions on the EFS Recovery Agent certificate template are modified to only allow members of the Internal Audit department Read and Enroll permissions. Three team members enroll the EFS Recovery Agent certificates, and the certificates are exported to Base-64 export files to allow definition of EFS Recovery Agents.
- A GPO named EFS Recovery is linked to the organization unit named OU=Notebooks,OU=Computer Accounts,DC=lucernepublish,DC=msft. The GPO designates the three EFS recovery certificates issued to the Internal Audit department as EFS Recovery Agents.
- The Default Domain Policy is modified to delete the existing Encrypting File System policy.
- A version 2 certificate template is created that enables the following settings.

<b>Tab</b>	<b>Actions</b>
General	Template Display Name: Lucerne Publishing EFS Template Name: LucerneEFS Validity Period: Two years Publish certificate in Active Directory: Enabled
Request Handling	Purpose: Encryption Archive subject's encryption private key: Enabled Include symmetric algorithms allowed by the subject: Enabled Minimum Key Size: 1,024 bits Allow private key to be exported: Enabled Enroll subject without requiring any user input: Enabled
Subject Name	No modifications
Issuance Requirements	No modifications
Superseded Templates	Basic EFS
Extensions	Application Policies: Encrypting File System
Security	LucernePublish\Domain Users: Read, Enroll, and Autoenroll

- A GPO named EFS Autoenrollment is linked to the OU named OU=Notebooks, OU=Computer Accounts,DC=lucernepublish,DC=msft. The GPO enables all autoenrollment settings for computer accounts.

## Case Study Questions

1. Does the default EFS Recovery Agent certificate template meet the design requirements for the Lucerne Publishing EFS project?
2. Does the default Key Recovery Agent certificate template meet the design requirements for the Lucerne Publishing EFS project?
3. Do the design requirements allow the EFS Recovery Agent and Key Recovery Agent certificate templates to be published only at the Lucerne Publishing Americas CA?
4. Does Andy's proposed solution meet the design requirements for designation of key recovery agents in the forest?
5. Is EFS encryption disabled for all Windows 2000 computers not in the OU named OU=Notebooks,OU=Computer Accounts,DC=lucernepublish,DC=msft?
6. Does Andy's proposed design disable EFS encryption for Windows XP computer accounts not in the OU named OU=Notebooks,OU=Computer Accounts,DC=lucernepublish,DC=msft?
7. Does the Lucerne Publishing EFS certificate template allow for autoenrollment by Windows XP users?
8. Does the proposed EFS Autoenrollment GPO enable autoenrollment of the Lucerne Publishing EFS certificate template by users with Windows XP computers?

## Additional Information

- Microsoft Official Curriculum, Course 2821: "Designing and Managing a Windows Public Key Infrastructure" ([www.microsoft.com/traincert/syllabi/2821afinal.asp](http://www.microsoft.com/traincert/syllabi/2821afinal.asp))
- "Key Archival and Management in Windows Server 2003" ([www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/kyacws03.msp](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/kyacws03.msp))
- "Encrypting File System in Windows XP and Windows Server 2003" ([www.microsoft.com/technet/prodtechnol/winxp/dep/encryptfs.msp](http://www.microsoft.com/technet/prodtechnol/winxp/dep/encryptfs.msp))

- “The Windows Server 2003 Family Encrypting File System” ([www.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/WinNETSrvr-EncryptedFileSystem.asp](http://www.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/WinNETSrvr-EncryptedFileSystem.asp)).
- Windows Data Protection (<http://msdn.microsoft.com/library/en-us/dnsecure/html/windataprotection-dpapi.asp>)
- Knowledge Base Article 298009: “Cipher.exe Security Tool for the Encrypting File System.”
- Knowledge Base Article 302093: “HOW TO: Prevent Files from Being Encrypted When Copied to a Server.”
- Knowledge Base Article 307877: “HOW TO: Encrypt a File in Windows XP.”
- Knowledge Base Article 308989: “HOW TO: Encrypt a Folder in Windows XP.”
- Knowledge Base Article 308991: “HOW TO: Share Access to an Encrypted File in Windows XP.”
- Knowledge Base Article 309408: “Troubleshooting the Data Protection API (DPAPI).”
- Knowledge Base Article 313365: “HOW TO: Configure a Domain EFS Recovery Policy in Windows 2000.”
- Knowledge Base Article 315672: “HOW TO: Use Cipher.exe to Overwrite Deleted Data in Windows.”
- Knowledge Base Article 320166: “HOW TO: Identify Encrypted Files in Windows XP.”
- Knowledge Base Article 324897: “HOW TO: Manage the Encrypting File System in Windows Server 2003.”
- Knowledge Base Article 329741: “EFS Files Appear Corrupted When You Open Them.”
- Knowledge Base Article 814599: “HOW TO: Use Cipher.exe to Overwrite Deleted Data in Windows Server 2003.”
- Knowledge Base Article 818200: “An Attacker with Physical Access to Your Computer May Be Able to Access Your Files and Other Data.”



**Note** Microsoft Knowledge Base articles can be found at <http://support.microsoft.com>. Enter the article number in the Search the Knowledge Base text box.

## Chapter 17

# Implementing SSL Encryption for Web Servers

Web browsing on the Internet or on local intranets is one of the most commonly used applications within an organization. By default, the Hypertext Transfer Protocol (HTTP) does not employ data encryption for transfers between the Web server and the Web client.

With a Web Server certificate installed at the Web server, however, the Web server can implement Secure Sockets Layer (SSL), an encryption protocol. SSL implementation at the Web server accomplishes two things:

- The client's Web browser validates the Web server's identity by performing certificate validation on the Web Server certificate.
- Data is encrypted as it is transferred between the Web server and the client's Web browser.

This chapter will discuss design decisions and details for implementing SSL at Web servers. Additional topics include using certificate-based authentication for Web clients and issuing Web Server certificates to third-party Web servers and Web accelerators.



**Note** Implementing SSL encryption for other protocols, such as Post Office Protocol version 3 (POP3) or Internet Mail Application Protocol version 4 (IMAP4) will be covered in Chapter 18, "Securing E-mail."

## How SSL Works

When a Web client connects to an SSL-secured Web server, the following process validates the Web server's identity and encrypts data. In basic terms:

1. An SSL connection is established when a user types or clicks a Uniform Resource Locator (URL) that begins with HTTPS (HTTP with SSL encryption).
2. When the connection is established, the Web server transmits its Web Server certificate to the Web browser.
3. To authenticate the Web server, the Web browser performs certificate validation (as described in Chapter 9, “Certificate Validation”) using the following tests:
  - Ensures that the Web Server certificate chains to a trusted root certification authority (CA).
  - Ensures that the Domain Name System (DNS) name in the certificate’s subject matches the DNS name in the HTTPS URL.
  - Ensures that the Web server certificate is time-valid.
  - Ensures that the Web server certificate has not been revoked.

## Enabling Strong Certificate Revocation List (CRL) Checking in Internet Explorer

The test for certificate revocation is performed only when CRL checking is enabled in the Web browser. For Internet Explorer, you can enable strong CRL checking using the following procedure:

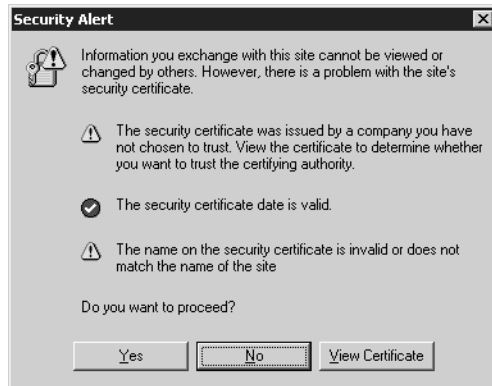
1. Open Internet Explorer.
2. From the Tools menu, click Internet Options.
3. In the Internet Options dialog box, on the Advanced tab, enable the Check for Server Certificate Revocation (Requires Restart) check box.
4. In the Internet Options dialog box, click OK.



**Warning** Enabling strong CRL checking can cause failures when connecting to SSL-protected Web sites if the CRLs cannot be downloaded in a timely manner. For example, if the user has a slow Internet connection, a large CRL might not download in a timely manner, resulting in a revocation checking error.

Alternatively, you can use the Internet Explorer Administration Kit (IEAK) when you deploy Internet Explorer to enable this option automatically. You must restart the computer for certificate revocation checking to take effect.

4. If the Web Server certificate fails any of these tests, the Web browser prompts the user to proceed. (See Figure 17-1.)



**Figure 17-1** The security alert presented when a Web server's certificate fails



**Note** In Figure 17-1, the Web Server certificate does not chain to a trusted root CA and the certificate's subject does not match the DNS name used by the Web client. Even though the validation tests fail, the user can still implement SSL encryption between the Web client and the Web server by clicking the Yes button.

5. If the Web Server certificate passes all tests, the Web browser extracts the certificate's associated public key.
6. The Web browser creates a pre-master secret, which is a string of randomly created bits whose length is determined by a negotiation between the Web browser and the Web server.
7. The Web browser encrypts the pre-master secret with the Web server's public key and sends the encrypted pre-master secret to the Web server.
8. The Web server decrypts the pre-master secret with its private key.
9. Depending on the cryptographic service provider (CSP) installed at the Web server, a Diffie-Hellman or a Rivest Shamir Adleman (RSA) negotiation allows the Web server and Web client to use the pre-master key to generate a symmetric session key using the same symmetric encryption algorithm.
10. The symmetric session key is used by the Web server and the Web client to encrypt data transmitted between the two. The session key is used until either the Web client or the Web server terminates the HTTPS session.



**Tip** When you are connected to a Web server using SSL, the Web browser displays a lock or key icon in the status bar, indicating that SSL is enabled for the session. You can view the properties of the Web server's certificate by double-clicking the lock or key icon.

## Certificate Requirements for SSL

When you implement SSL, you must identify the certificates that are required to enable SSL encryption between the Web client and the Web server. Two types of certificates can be used:

- **A Web Server certificate.** A Web Server certificate is mandatory when implementing SSL for a Web server. The Web Server certificate provides encryption of the pre-master secret when it is sent from the Web client to the Web server. In addition, the Web Server certificate allows the Web client to validate the Web server's identity, ensuring that the Web server is not an attacker's Web server impersonating the target Web server.
- **A Web client certificate.** When a Web site requires authentication to identify the actual user connecting to the Web site, the Web client can use certificate-based authentication. Certificate-based authentication is not required for SSL connections, but it does increase the security of the user's credentials.

## Choosing a Web Server Certificate Provider

When you implement SSL at a Web server, you must determine where you will obtain the Web Server certificate. The decision is most often based on whether the clients connecting to the Web server are internal or external. Internal clients are employees or partners of your organization who might or might not have computer accounts within your network. An external client is typically a customer that does business with you but does not have a user or computer account on your network.

An organization typically chooses to issue Web Server certificates from a private CA when:

- The organization must enforce its security policies and certificate policies. A certificate obtained from a commercial CA requires an organization to follow the guidelines defined in the commercial CA's certificate practice statement.
- The organization wants to reduce the costs associated with issuing certificates to intranet Web servers, which only accept connections from employees or



other trusted partners. In these circumstances, an organization can require employees or partners to trust the root CA of the organization's CA hierarchy. This eliminates the need to purchase Web Server certificates from a commercial organization only for internal use.

An organization typically chooses to acquire the Web Server certificates from a commercial CA when:

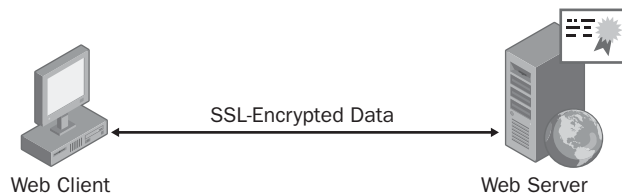
- The organization has not deployed an internal public key infrastructure (PKI). By outsourcing PKI management to a commercial CA, an organization eliminates the costs associated with designing, implementing, and managing CAs and certificates for the deployment of Web Server certificates.
- The organization uses the Web site to sell goods and services over the Internet, and the commercial CA can provide transaction liability insurance for commerce-based Web sites.
- A commercial CA is included in the Trusted Root Certification Authority store for most organizations.

## Placement of Web Server Certificates

When an organization implements SSL, the organization must choose where to deploy the Web Server certificates. The deployment location depends on the network configuration implemented by the organization. Certificate placement for common Web server deployment scenarios is discussed in the sections that follow.

### Single Web Server

When SSL is implemented for a single Web server, the Web Server certificate must be deployed at the Web server. (See Figure 17-2.)

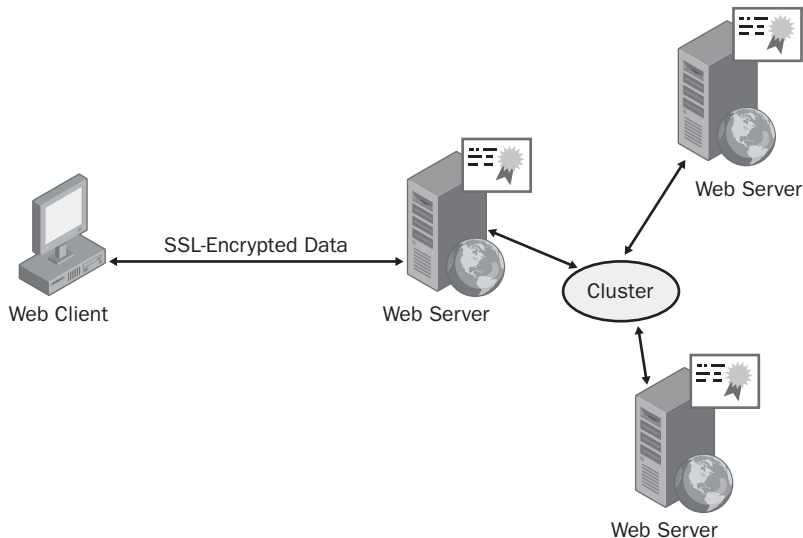


**Figure 17-2** Deploying a Web Server certificate to a single Web server

In this scenario, the Web Server certificate must be deployed at the Web server computer. This allows the client computer to validate the Web server's identity and use the Web Server certificate's public key to encrypt the pre-master secret key when sending it to the Web server.

## Clustered Web Servers

A common Web server deployment tactic is to arrange a Web site in a clustered configuration. In a clustered configuration, either a common disk exists between multiple servers or the servers host a common Web site through a Network Load Balancing (NLB) cluster. In either case, when users connect to a specific URL, they are redirected to any one of the cluster nodes. (See Figure 17-3.)



**Figure 17-3** Deploying a Web Server certificate to a clustered Web server

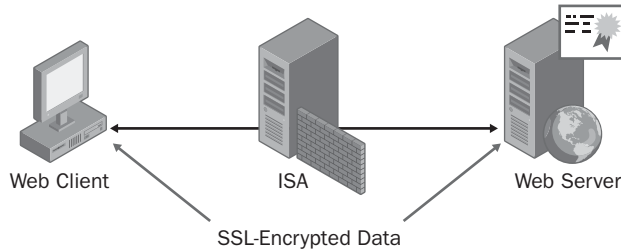
When you implement SSL in a clustered configuration, each Web server in the cluster must have its own Web Server certificate. The only requirement is that the Web Server certificate's subject name is the DNS name used by Web clients to connect to the Web site.



**Important** A common misconception is that the same certificate and private key pair must be deployed at each Web server in the cluster. Each node in the cluster does require its own certificate, but it is not necessary to deploy the same certificate and key pair at each node in the cluster. If a node in the cluster fails, all Web clients connected to that node must re-establish connections to another node in the cluster. Remember that this is a new SSL connection, requiring that a new symmetric session key be negotiated between the Web client and the Web server. In fact, if you purchase your Web Server certificates from a commercial organization, such as VeriSign or RSA, you might be required to purchase separate Web Server certificates for each node.

## Web Server Protected by ISA with Server Publishing

Microsoft Internet Security and Acceleration (ISA) Server with server publishing allows you to host a Web site behind a firewall. When you implement server publishing, all traffic that connects to the ISA Server's SSL listening port (TCP port 443) is redirected to the Web server protected by the ISA Server. (See Figure 17-4.)



**Figure 17-4** Deploying a Web Server certificate when using ISA server publishing

In this configuration, the Web Server certificate must be installed at the Web server. The DNS name in the certificate's subject must match the DNS name used by Web clients to connect to the ISA Server's external interface. In other words, the DNS name must resolve to an IP address bound to the ISA Server's external interface.



**Tip** You can also use this configuration with many industry-standard firewalls, such as Cisco PIX or Checkpoint Firewall-1, which implement port mapping to redirect inbound traffic to a server behind a firewall.

This configuration allows an organization to meet the technical requirement of implementing end-to-end encryption of data transmitted between the Web client and the Web server.

## Web Server Protected by ISA with Web Publishing

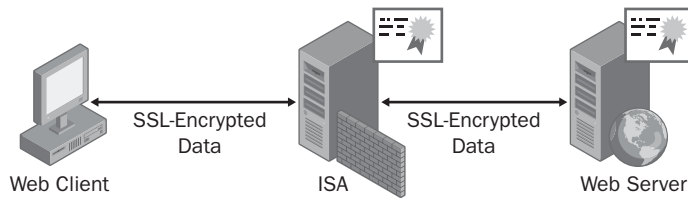
The ISA Server provides an alternate method of transmitting data to a Web server protected by a firewall. When you implement Web publishing, the data received by the ISA Server is decrypted and inspected by application filters. These application filters, such as URLScan, inspect Web traffic for worm attacks or other Web-based attacks against a Web server.

When you implement Web publishing, two certificate deployment scenarios are possible:

- Implementing end-to-end SSL
- Implementing SSL between the Web client and the ISA Server

## Implementing End-to-End SSL

In the first scenario, the ISA Server implements SSL between the Web client and the ISA Server, as well as between the ISA Server and the Web server. (See Figure 17-5.)



**Figure 17-5** Deploying Web Server certificates when using ISA Web publishing with SSL on all connections

In this configuration, Web Server certificates must be installed at both the ISA Server and at the Web server. Two separate SSL connections occur:

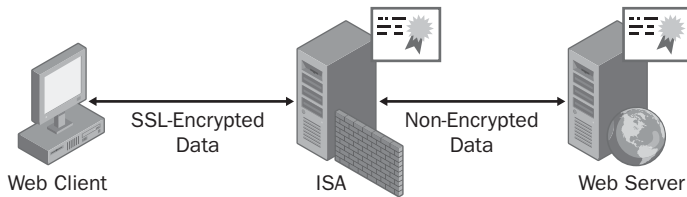
- The first SSL connection is between the Web client and the ISA Server. The subject of the Web Server certificate installed at the ISA Server must contain the DNS name used by the Web client to connect to the Web server, and the DNS name must resolve to the ISA Server's external IP address.
- The second SSL connection is between the ISA Server and the Web server. The subject of the Web Server certificate installed on the Web Server must contain the DNS name or IP address indicated in the Web publishing rule at the ISA Server.



**Note** If your company has an SLA for performance, such as servicing 1,000 transactions per second, you can consider implementing SSL acceleration cards at the Web server and the ISA Server. Otherwise, any acceleration gains made by connecting to the ISA Server are lost when data is re-encrypted and transmitted to the back-end Web server.

## Implementing SSL Between the Web Client and the ISA Server

In the second scenario, SSL is implemented only between the Web client and the ISA Server. (See Figure 17-6.)



**Figure 17-6** Deploying Web Server certificates when using ISA Web publishing with SSL only between the Web client and the ISA Server

In this configuration, a Web Server certificate must be installed only on the ISA Server. Once the ISA Server's application filter inspects the incoming HTTPS stream, the data is redirected as HTTP to the back-end Web server.



**Note** This scenario allows network intrusion detection systems such as Snort to inspect all data as it is transmitted to the Web server's network.

In this scenario, the subject of the Web Server certificate installed at the ISA Server must contain the DNS name used by the Web client to connect to the Web server, and the DNS name must resolve to the ISA Server's external IP address.

## Choosing a Certificate Template

If your organization chooses to proceed with deploying Web Server certificates to internal Web servers, the default Web Server certificate template meets the needs of most companies. Typically, the only change that must be performed is to modify certificate template permissions to enable Read and Enroll permissions at a custom universal or global group that contains Web server administration user accounts.



**Important** Although you can create a version 2 certificate template based on the Web Server certificate template to enable modification of application policies or certificate policies, this prevents use of the Internet Information Services (IIS) Web Server Certificate Wizard. This wizard, discussed in more detail later in the chapter, is hard-coded to use the Web Server certificate template display name and does not allow use of a custom version 2 certificate template.

## Issuing Web Server Certificates

The process of requesting and issuing a Web Server certificate varies according to the type of device on which the certificate request is generated. When issuing certificates from an enterprise CA, options include:

- Issuing certificates to Web servers running IIS on forest member computers.
- Issuing certificates to Web servers running IIS on non-forest member computers.
- Issuing certificates to third-party Web servers or hardware-based Web acceleration devices.

### Issuing Web Server Certificates to Forest Members

When you issue a Web Server certificate to a forest member using the Web Server Certificate Wizard, the certificate request is submitted in the security context of the user using the Web Server Certificate Wizard. The user running the wizard must belong to a group assigned Read and Enroll permissions for the Web Server certificate template. In addition, the user must be a member of the local Administrators group on the Web server to allow him or her to write certificate information into the computer's local store.

Installation of the Web Server certificate in a forest environment is a two-step process:

1. Request and install the Web Server certificate at the Web server.
2. Configure the Web server to enable SSL encryption for a Web site or virtual server.

### Requesting and Installing the Web Server Certificate

The Web Server Certificate Wizard is launched from the Internet Services Manager console in Windows 2000 and the Internet Information Services (IIS) Manager console in Windows Server 2003. The following process installs a Web Server certificate:

1. From the Start menu, point to Programs, point to Administrative Tools, and click Internet Services Manager if you are using Windows 2000 or Internet Information Services (IIS) Manager if you are using Windows Server 2003.
2. In the console tree, expand *ServerName* and click Default Web Site.
3. Right-click Default Web Site and click Properties.
4. In the Default Web Site Properties dialog box, click the Directory Security tab.
5. On the Directory Security tab, in the Secure Communications section, click Server Certificate.

6. In the Web Server Certificate Wizard, click Next.
7. On the Server Certificate page, click Create a New Certificate and click Next.
8. On the Delayed or Immediate Request page, click Send the Request Immediately to an Online Certification Authority and click Next.



**Note** By sending the request to an online CA, the enterprise CA decides whether to issue or deny the certificate request based on the permissions assigned to the Web Server certificate template.

9. On the Name and Security Settings page, in the Name box, type a description of the Web server, set the Bit Length to 1024, and click Next.



**Note** In Windows Server 2003, you can choose which SChannel CSP to use for the Web Server certificate on the Name and Security Settings page.

10. If you are running Windows Server 2003 and you want to choose the CSP on the Available Providers page, select the CSP you want to implement and click Next.



**Note** The default providers for Web Server certificates include the Microsoft RSA/SChannel Cryptographic Provider and the Microsoft Diffie-Hellman/Schannel Cryptographic Provider.

11. On the Organization Information page, enter the organization and department name, and click Next.
12. On the Your Site's Common Name page, in the Common Name box, type the **DNSName** of the Web site (where *DNSName* is the full DNS name of the Web site as typed by a Web client), and click Next.



**Note** For example, use **www.example.com** rather than **webserver**, the NetBIOS name of the computer, when providing the common name for the certificate request.

13. On the Geographical Information page, enter the country, state, and city information and then click Next.
14. If you are using IIS 6.0, on the SSL page, accept the default port of 443, and click Next.
15. On the Choose a Certification Authority page, in the Certification Authorities drop-down list, select an available enterprise CA, and click Next.
16. On the Certificate Request Submission page, verify the settings and click Next.
17. On the Completing the Web Server Certificate Wizard page, click Finish.

As you can see, there are only minute differences between the Web Server Certificate Wizard in Windows 2000 and Windows Server 2003. At the completion of this procedure, the Web Server certificate is installed in the Local Machine store and available for use by IIS.

### Enabling SSL at the IIS Web Server

Once you install the Web Server certificate, you can enable SSL protection for an entire Web site or for a virtual folder within a Web site. The following procedure describes the steps involved:

1. In the Internet Services Manager or Internet Information Services (IIS) Manager console tree, right-click the Web site or virtual directory where you want to enable SSL and click Properties.
2. In the Properties dialog box, click the Directory Security tab.
3. On the Directory Security tab, in the Secure Communications section, click the Edit button.
4. In the Secure Communications dialog box, enable the Require Secure Channel (SSL) check box, enable the Require 128-bit Encryption check box, and click OK.



**Note** Enabling the 128-bit encryption check box is subject to international export laws. For example, the United States prohibits the export of strong encryption to embargoed countries. For details on U.S. export law changes, see “Revisions to Encryption Items,” available at [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2000\\_register&docid=fr19oc00-5](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2000_register&docid=fr19oc00-5).

5. In the Properties dialog box, click OK.
6. Close the Internet Services Manager or Internet Information Services (IIS) Manager console.





**Note** After you enable SSL, you should ensure that the Web site implements SSL, as required. To verify encryption, open the Web site using the URL *https://WebServerDNSName/vdir*. For example, open *https://www.example.com/secure*. If 128-bit encryption is enabled, you can verify the encryption level in Internet Explorer by hovering the mouse over the lock icon on the window's bottom right corner. If you have enabled 128-bit encryption, the words SSL Secured (128 bit) appear.

## Issuing Web Server Certificates to Non-Forest Members

When you issue a Web Server certificate to a non-forest member, the certificate request cannot be submitted to the Windows Server 2003 CA directly. Instead, the certificate request must be saved to a PKCS #10 request file and then submitted to the CA by a member of the managing organization.



**Note** This process is the same as when you submit a Web Server certificate request to a commercial CA organization, such as VeriSign or RSA. The only difference is in the certificate issuance, which varies depending on the type of CA used by the commercial CA.

The installation of the Web Server certificate to a non-forest member is a four-step process:

1. Generate a Web Server certificate request at the Web server.
2. Submit the Web Server certificate request to the CA.
3. Install the issued Web Server certificate at the Web server.
4. Configure the Web server to enable SSL encryption for a Web site or virtual directory.



**Note** There is no difference in enabling SSL encryption at an IIS Web server when the certificate is installed on a forest member versus a non-forest member. For details on how to enable and verify SSL encryption, see the section "Enabling SSL at the IIS Web Server" earlier in this chapter.

## Generating the Web Server Certificate Request

The Web Server Certificate Wizard is launched from the Internet Services Manager console in Windows 2000 and the Internet Information Services (IIS) Manager console in Windows Server 2003. The following process generates a Web Server certificate request file:

1. From the Start menu, point to Programs, point to Administrative Tools, and click Internet Services Manager if you are using Windows 2000 or Internet Information Services (IIS) Manager if you are using Windows Server 2003.
2. In the console tree, expand *ServerName* and click Default Web Site.
3. Right-click Default Web Site and click Properties.
4. In the Default Web Site Properties dialog box, click the Directory Security tab.
5. On the Directory Security tab, in the Secure Communications section, click Server Certificate.
6. In the Web Server Certificate Wizard, click Next.
7. On the Server Certificate page, click Create a New Certificate and click Next.
8. On the Delayed or Immediate Request page, click Prepare the Request Now, But Send It Later and click Next.



**Note** By generating the certificate request, you can submit the request to any CA, whether it is a Microsoft enterprise CA, a Microsoft standalone CA, or a commercial CA. The PKCS #10 request format file is interoperable with any (standards compliant) CA.

9. On the Name and Security Settings page, in the Name box, type a description of the Web server, set the Bit Length to 1024, and click Next.



**Note** In Windows Server 2003, you can choose the SChannel CSP for the Web Server certificate on the Name and Security Settings page.

10. If you are running Windows Server 2003 and you want to choose the CSP on the Available Providers page, select the CSP you want to implement and click Next.

11. On the Organization Information page, enter the organization and department name, and click Next.
12. On the Your Site's Common Name page, in the Common Name box, type the ***DNSName*** of the Web site (where *DNSName* is the full DNS name of the Web site as typed by a Web client), and click Next.
13. On the Geographical Information page, enter the country, state, and city names, and click Next.
14. On the Certificate Request File Name page, in the File name box, type a file path and name for the PKCS #10 request file, and click Next.
15. On the Request File Summary page, verify the settings and click Next.
16. On the Completing the Web Server Certificate Wizard page, click Finish.

### **Submitting the Request File at the Windows Server 2003 CA**

The previous procedure results in a request file, which file can be e-mailed to a commercial provider or submitted through a form on the provider's Web site for certificate issuance. If the certificate is to be issued by a Windows Server 2003 enterprise CA, the following procedure issues and verifies the certificate:

1. Retrieve the request file generated in the previous procedure.
2. Log on at a Windows computer as a user assigned Read and Enroll permissions for the Web Server certificate template.
3. Open Internet Explorer.
4. In Internet Explorer, open the URL *http://CADNSName/certsrv* (where *CADNSName* is the DNS name of the CA computer).
5. On the Welcome page, click the Request a Certificate link.
6. On the Request a Certificate page, click the Advanced Certificate Request link.
7. On the Advanced Certificate Request page, click the Submit a Certificate Request By Using a Base 64-Encoded CMC or PKCS #10 File, Or Submit A Renewal Request By Using a Base 64-Encoded PKCS #7 File link.
8. On the Submit a Certificate Request or Renewal Request page, provide the following information:
  - Saved Request: Paste the request file's contents into the Base 64-encoded certificate request box.



**Note** You can open the request file in Notepad, select all the file's contents by pressing CONTROL+A, and copy it to the clipboard by pressing CONTROL+C. The contents of the file can be copied into the Base 64–encoded certificate request by clicking in the box and pressing CONTROL+V.

- Certificate Template: Web Server.
  - Additional Attributes: No input is required.
9. On the Submit a Certificate Request or Renewal Request page, click Submit.
  10. On the Certificate Issued page, select Base 64–encoded and click Download Certificate Chain.



**Note** The Download Certificate Chain link downloads the certificate chain for the Web Server certificate, including the root CA certificate and any intermediate CA certificates in the certificate chain. These certificates are required to add the root CA as a trusted root CA at the Web server and to install any intermediate CA certificates and the issuing CA certificate into the Intermediate Certification Authorities store.

11. Close Internet Explorer.

This procedure varies slightly if the certificate request is submitted to a standalone CA, which does not implement certificate templates. A standalone CA eliminates the need to designate the certificate template when submitting the certificate request file because the standalone CA does not implement certificate templates.



**Tip** If you have not installed IIS at the standalone CA, you can submit the certificate request by using the Certification Authority console. You cannot use this method at an enterprise CA, as the interface does not allow you to designate the certificate template to use for the request.

## Installing the Web Server Certificate at the Web Server

Once you download the Web Server certificate chain, you must complete the installation of the certificate *and chain* at the Web Server, as follows:

1. From the Start menu, point to Programs, point to Administrative Tools, and click Internet Services Manger if you are using Windows 2000 or Internet Information Services (IIS) Manager if you are using Windows Server 2003.
2. In the console tree, expand *ServerName* and click Default Web Site.
3. Right-click Default Web Site and click Properties.
4. In the Default Web Site Properties dialog box, click the Directory Security tab.
5. On the Directory Security tab, in the Secure Communications section, click Server Certificate.
6. In the Web Server Certificate Wizard, click Next.
7. On the Pending Certificate Request page, click Process the Pending Request and Install the Certificate, and click Next.
8. On the Process a Pending Request page, in the Path and File Name box, type the path and file name to the CA certificate chain file (\*.p7b), and click Next.
9. If you are using IIS 6.0, on the SSL Port page, in the SSL Port this Web Site Should Use box, type **443**, and click Next.
10. On the Certificate Summary page, review the details of the certificate and click Next.
11. On the Completing the Web Server Certificate Wizard page, click Finish.



**Tip** By changing the defaults to designate the PKCS #7 file containing the Web server's certificate chain, you complete two steps in one. You install the Web Server certificate at the Web server and you install all certificates in the certificate chain to the Local Machine store, allowing the Web Server to trust the root CA certificate.

At this point, you can enable the Web site or a virtual directory within the Web site for SSL protection, as discussed earlier in the chapter.

## Issuing Web Server Certificates to Third-Party Web Servers and Web Acceleration Devices

In many organizations, Web servers other than IIS are used for Web applications. Although the Web servers are not Microsoft Web servers, there is nothing preventing the Web servers from receiving their Web Server certificate from a Windows Server 2003 CA.

When a Web Server certificate is required on a third-party Web server or a Web acceleration appliance, the same process is required to enable SSL at the Web server or appliance as for a non-forest member IIS server. To implement SSL at the Web server or appliance, you must:

1. Generate a key pair and Web Server certificate request at the third-party Web server or device using the tools provided by the third-party Web server or device.
2. Submit the Web Server certificate request to the Windows Server 2003 CA.
3. Install the issued Web Server certificate at the third-party Web server or device.
4. Enable SSL at the third-party Web server or device.



**Note** For detailed information on the procedure for your Web server or network appliance, review the documentation for the server or appliance, focusing on generating certificate requests and installing certificates at the server or device.

## Certificate-Based Authentication

In addition to implementing SSL encryption, a Web server can implement certificate-based authentication. Rather than typing credentials or simply being connected to a Web site anonymously, users select a certificate from their certificate store with the Client Authentication Enhanced Key Usage (EKU) for authentication. The certificate is associated to a user account in IIS's available account databases through a process known as *mapping*. There are two types of mappings:

- **Explicit mapping.** The certificate is mapped directly in the properties of a user's Active Directory account; in a database of mappings in IIS; or in an application, such as Netegrity Siteminder.
- **Implicit mapping.** The certificate is mapped to a user account based on the information included in either the Subject or the Subject Alternate Name extension. For example, if Active Directory mapping is implemented, the Subject Alternate Name must include the User Principal Name (UPN) name form.



**Note** Implicit mappings require that the certificate of the CA that issues the user's certificate be included in the NTAuth object in Active Directory.

Whatever mapping method is used to associate the presented certificate with a user account, the user presenting the certificate must have access to the certificate's private key to prove his or her identity. Just having the access to the certificate is insufficient because the certificate is a public document. Possession of the private key proves that the user is the certificate's subject.

## Defining Certificate Mappings

When you define certificate mapping, you can choose to implement either one-to-one mappings, where each certificate is directly mapped to a single user account, or many-to-one mappings, where a group of certificates with common attributes is mapped to a single user account.

### One-to-One Mappings

In a one-to-one certificate mapping, you are defining a direct relationship between a certificate and an account in the directory used by the Web server—Active Directory or the local account database of the Web server. Once the Web server validates the presented certificate, the certificate's private key holder is identified as a user account mapped to the certificate. The user is granted any rights or permissions assigned to the associated account.

### Many-to-One Mappings

In many-to-one mappings, multiple certificates are mapped to a single user account by rules defined in Active Directory or in IIS. If the certificate matches the rule set defined in Active Directory and a user holds the private key associated with the certificate, he or she is assigned the rights and permissions defined for the associated account.

For example, your organization might have a partnership with Fabrikam Industries. All users who require access to your organization's extranet Web site have received a client authentication certificate with a subject in the form OU=Employees, DC=Fabrikam,DC=com. When you define the many-to-one relationship, you define that any certificate that has CN=\*,OU=Employees,DC=Fabrikam,DC=com as its subject maps to a user account in your directory named Fabrikam User.



**Note** When you define a many-to-one mapping, you cannot differentiate individual users connecting to your Web site. Auditing only shows access by the user accounts defined in the many-to-one mapping. If you require auditing of each person's access to a Web site, you must define one-to-one mappings.

## Combining One-to-One and Many-to-One Mappings

If you define both one-to-one and many-to-one mappings, a one-to-one mapping takes precedence. This allows you to define one-to-one mappings for specific users you want to track when they connect to your Web site, yet grants universal access to other users whose certificate matches a many-to-one mapping definition.

For example, if you define a one-to-one mapping for Andy Ruth (CN=Andy Ruth,OU=Employees,DC=fabrikam,DC=com) and a many-to-one mapping for anyone with a certificate issued by the CA whose subject is CN=Fabrikam Employees CA,OU=Employees,DC=fabrikam,DC=com, Andy's one-to-one mapping takes precedence, even though his certificate is a match for both mapping rules.

## Choosing Where to Perform Certificate Mappings

Once you determine the type of mapping you want to perform, you must choose how to perform the mapping. In a Windows environment, you can choose from two methods:

- **Active Directory.** If you define certificate mapping in Active Directory, the certificate mapping definition is available at any IIS server that is a member of the forest. This reduces the work and effort in defining and using certificate mappings. As long as the IIS server is configured to enable certificate mapping and enables the Windows directory service mapper, all defined certificate mappings are available for use.
- **IIS.** If you define certificate mappings in IIS, the certificate mapping definition is only available on that IIS server. In some cases, this is the only choice. For example, if the IIS server is not a member of the forest or is installed on a network where Active Directory is not used, IIS certificate mapping is the only solution (unless you implement a third-party product).



**Note** There are several third-party methods for certificate mapping that enable you to use certificate-based authentication with Web servers other than IIS. For example, Netegrity Siteminder installs an agent at both the client computers and the Web servers so that Siteminder can authenticate the user based on the certificate presented during authentication. In addition to allowing certificate-based authentication on non-Windows platform computers, Siteminder allows you to use alternate directories, such as a corporate Lightweight Directory Access Protocol (LDAP) directory, a SQL database, or a Novell Directory Services (NDS) directory as the directory source for the certificate mapping.



# Performing Certificate-Based Authentication

In a Windows environment, certificate mappings can be defined in both Active Directory and in IIS. This section discusses how to define certificate mappings in both.

## Configure IIS to Use Active Directory Mappings

IIS can use Active Directory as its mapping directory. As mentioned earlier, the advantage of using Active Directory is that the mapping is available on multiple Web servers (as long as they are members of the forest) and can be used by applications other than Web browsers.

Use the following steps to enable IIS to use Active Directory mappings:

1. Create a certificate template for user authentication.
2. Define the mappings in Active Directory.
3. Enable IIS to use certificate mappings.
4. Enable the directory service mapper.

## Creating a Certificate Template

The first step in defining a certificate mapping in Active Directory is to design a certificate template that allows a user to authenticate in a Web browser. The user certificate must meet the following requirements:

- The certificate must be a signing certificate that implements the Digital Signature key usage.
- The certificate must include the Client Authentication (1.3.6.1.5.5.7.3.2) object identifier (OID).



**Note** The default User Signature Only meets these requirements without providing additional capabilities other than signing e-mail. If you want to remove the e-mail signing capability, it is recommended that you duplicate the User Signature Only certificate template and remove the Secure Email (1.3.6.1.5.5.7.3.4) OID. Alternatively, if you want to use a smart card for authentication, the Smart Card Login certificate template meets these requirements.

## Defining the Mapping in Active Directory

You might have to define certificate mappings in Active Directory. The decision on whether to define a mapping in Active Directory is often based on the answers to the following questions:

- **Is the certificate issued by an enterprise CA in your forest?** If so, the certificate contains the user's UPN in the Subject Alternative Name extension and the CA's certificate is included in the NTAAuth store of Active Directory. This enables the ability to use implicit mappings.
- **Is the certificate issued by a foreign CA?** If the CA is not from your forest, you must define an explicit mapping to enable certificate-based authentication. In addition, you must add the foreign CA's certificate to the NTAAuth store and ensure that the certificate's Subject or Subject Alternative Name contains the user's User Principal Name (UPN).

### Enabling Implicit Certificate Mappings

If you intend to use a certificate based on the User Signature Only or Smart Card Login certificate templates, you can implement implicit certificate mappings. For an implicit certificate mapping, you only have to ensure that the issuing CA is in the NTAAuth store. You can verify this using the following procedure:

1. Ensure that the Windows Server 2003 Resource Kit Tools are installed.



**Note** The Resource Kit Tools are available for download at [www.microsoft.com/downloads/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cffd&displaylang=en](http://www.microsoft.com/downloads/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cffd&displaylang=en).

2. Open the PKI Health Tool (Pkiview.msc).
3. In the PKI Health Tool, in the console tree, right-click Enterprise PKI and click Manage AD Containers.
4. In the Manage AD Containers dialog box, on the NTAAuthCertificates dialog box, ensure that the issuing CA's certificate appears. If the CA certificate does not appear, click Add.
5. In the Open dialog box, in the File Name box, type the file location of the issuing CA certificate and click Open.
6. In the Manage AD Containers dialog box, click OK.
7. Close the PKI Health Tool.

## Enabling Explicit Mappings

To enable an explicit mapping in Active Directory, the user holding the private key associated with a client authentication certificate must provide you with access to the certificate. He or she can do this by simply e-mailing the certificate to you or by copying the certificate to a removable device and providing access to you.

An implicit mapping takes precedence and is tried first by SChannel before trying explicit mapping when validating a client certificate.



**Note** Even if you define an explicit mapping for a certificate, SChannel will attempt to perform an implicit mapping based on the certificate's subject before determining whether an explicit mapping exists.

Once you obtain the certificate, you can define the explicit mapping in Active Directory, as follows:

1. Log on as a user who is delegated the permissions to modify the target user account.
2. Open Active Directory Users and Computers.
3. From the View menu, click Advanced Features.
4. In the console tree, navigate to the container or OU in which the user account you want to associate with the certificate exists. You might have to create this user account.
5. In the details pane, right-click the user account and click Name Mappings.
6. In the Security Identity Mapping dialog box, on the X.509 Certificates tab, click Add.
7. In the Add Certificate dialog box, in the File Name box, type the path and file name of the user's certificate file, and click Open.
8. In the Add Certificate dialog box, verify the subject and issuer information. In this dialog box, you can choose whether to implement a one-to-one or a many-to-one mapping:
  - If you enable the Use Subject for Alternate Security Identity check box, you are enabling a one-to-one mapping. The certificate must contain the designated subject information for the mapping to occur.
  - If you clear the Use Subject for Alternate Security Identity check box, you are enabling a many-to-one mapping. The certificate must contain the designated issuer information for the mapping to occur.



**Note** If you choose to implement a many-to-one mapping, a dialog box appears warning you that you cannot switch the mapping back to a one-to-one mapping without redefining the mapping. The subject information is lost once you disable the Use subject for alternate security identity check box.

9. In the Security Identity Mapping dialog box, click OK.



**Important** Explicit mappings cannot be used for smart card logon. Smart card logon only uses an implicit mapping by mapping the UPN in the Subject Alternative Name of the certificate to the UPN of a user account in Active Directory. Explicit mappings can be used for Web authentication, wireless authentication, and VPN authentication.

## Enabling IIS to Use Certificate Mappings

After defining all of the required certificate mappings, you must enable the IIS server to enable certificate-based authentication. Use the following procedure:

1. Open the Internet Services Manager (in Windows 2000) or the Internet Information Services (IIS) Manager (in Windows Server 2003).
2. In the console tree, navigate to the Web site or virtual directory where you want to enable certificate-based authentication.
3. In the Properties dialog box, on the Directory Security tab, in the Secure Communications section, click Edit.
4. In the Secure Communications dialog box, ensure that the following settings are enabled to enforce certificate-based authentication:
  - **Require secure channel (SSL): Enabled.** Certificate-based authentication is a mutual authentication between the client and the server. You must have SSL enabled to enable server authentication.
  - **Require client certificates: Selected.** This option enforces certificate-based authentication. If you want to provide alternate methods of authentication, such as Windows Integrated Authentication, you can choose Accept Client Certificates instead.
  - **Enable client certificate mapping: Enabled.** This option enables the Web site to perform certificate mapping.

5. In the Secure Communications dialog box, click OK
6. In the Properties dialog box, click OK.

## Preventing Other Forms of Authentication

You can further restrict the Web site to disallow other forms of authentication. This is accomplished by disabling all other authentication methods for the Web site or virtual directory, as follows:

1. Open the Internet Services Manager (in Windows 2000) or the Internet Information Services (IIS) Manager (in Windows Server 2003).
2. In the console tree, navigate to the Web site or virtual directory where you want to enable certificate mapping.
3. In the Properties dialog box, on the Directory Security tab, in the Anonymous access and authentication control section, click Edit.
4. In the Authentication Methods dialog box, clear all check boxes and click OK.



**Note** This configuration disables all other forms of authentication. If certificate-based authentication fails, the user is no longer provided with an alternative authentication method.

5. In the Properties dialog box, click OK.

In addition, you must configure the NTFS permissions on the folder where the Web content exists to limit access to groups in which there are authorized users. The permissions assigned must allow the user to perform the tasks required by the Web site.

## Enabling the Directory Service Mapper

Once you enable certificate mappings for the Web site or virtual directory, you must enable the Windows directory service mapper. To do this, perform the following steps:

1. Open the Internet Information Services Manager (in Windows Server 2003).
2. In the console tree, right-click Web Sites and click Properties.

3. In the Web Sites Properties dialog box, on the Directory Security tab, click Enable the Windows Directory Service Mapper, and click OK.
4. Close Internet Information Services (IIS) Manager.

The process is different if you are using Windows 2000:

1. Open the Internet Services Manager.
2. In the console tree, right-click *ServerName* (where *ServerName* is the name of the IIS Server) and click Properties.
3. In the *ServerName* Properties dialog box, on the Internet Information Services tab, in the Master Properties drop-down list, select WWW Service, and click Edit.
4. In the WWW Service Master Properties dialog box, on the Directory Security tab, click Enable the Windows Directory Service Mapper, and click OK.
5. In the *ServerName* Properties dialog box, click OK.

## Configure IIS to Use IIS Certificate Mappings

The procedure is similar when you perform certificate mappings in IIS rather than Active Directory. The only difference is that you must define the mapping between the certificate and the user account within IIS rather than enable the Windows directory service mapper.

To enable IIS Certificate Mapping, use the following procedure:

1. Create a certificate template for user authentication.
2. Enable IIS to use certificate mapping.
3. Define the mappings in IIS.

### Creating a Certificate Template for User Authentication

When you implement certificate-based authentication, the Web browser does not change its behavior based on the type of mappings configured at the Web server. The same certificates used for Active Directory mapping are used for IIS mapping. As long as the certificate includes the Client Authentication (1.3.6.1.5.5.7.3.2) OID and chains to a trusted root authority, Internet Explorer can use the certificate for Web authentication.

## Enabling IIS to Use Certificate Based Authentication

The same process enables certificate-based authentication in IIS when you implement IIS Certificate mapping, rather than Active Directory certificate mapping. You still must:

- Enable SSL at the Web site.
- Configure whether certificates are optional or required for authentication.
- Enable certificate-based authentication.

You can also disable all other forms of authentication.

## Defining the Mappings in IIS

The final configuration steps for certificate-based authentication differ greatly when you enable IIS certificate mapping, rather than Active Directory mapping.

The first thing you must do is ensure that the Windows directory service mapper is disabled. Otherwise, if the Windows directory service mapper is enabled, the IIS server continues to use Active Directory mapping even if you define mappings in IIS.

Once you disable Windows directory service mapper, you can define IIS Certificate Mapping using the following procedure:

1. Open the Internet Services Manager (in Windows 2000) or the Internet Information Services (IIS) Manager (in Windows Server 2003).
2. In the console tree, navigate to the Web site or virtual directory where you want to enable certificate mapping.
3. In the Properties dialog box, on the Directory Security tab, in the Secure Communications section, click Edit.
4. In the Secure Communications dialog box, ensure that Enable Client Certificate Mapping is enabled and click Edit.
5. In the Account Mappings dialog box, you can choose whether to define a one-to-one mapping by clicking the 1-to-1 tab or a many-to-one mapping by clicking the Many-to-1 tab.

The following procedure performs one-to-one mapping:

1. In the Account Mappings dialog box, click Add.
2. In the Open dialog box, select the path and file name of the certificate file and click Open.

3. In the Map to Account tab, enable the Enable This Mapping check box and enter the following information:
  - Map name: A logical name for the name mapping definition.
  - Account: The user account from the local SAM database or from Active Directory that you want to associate with the certificate.
  - Password: The password for the selected user account.



**Important** The password is stored in IIS, requiring that you either update the password when it changes in IIS or allow the password to not expire.

4. In the Map to Account tab, click OK.
5. In the Confirm Password dialog box, re-enter the password and click OK.
6. In the Account Mappings dialog box, click OK.
7. In the Secure Communications dialog box, click OK.
8. In the Properties dialog box, click OK.

If the account mapping is many-to-one, you must define the matching rules used by IIS to determine which certificates are mapped to the designated user account. The interface and selections vary depending on the version of IIS and the certificate matching rules your organization requires.



**More Info** For more information on defining the client certificate mapping rules, search for “Mapping Client Certificate Many-to-One” in the IIS Help files.

## Best Practices

- **Implement Web Server certificates from a private CA if the Web server is an intranet server.** An intranet server is only accessed by computers and users within your organization. It is possible to deploy the trusted root certificate to an organization’s computers through enterprise policy, Group Policy, or CAPICOM scripts.



- **Implement Web Server certificates from a commercial CA when:**
  - The Web server is on the Internet or on an extranet. If the Web server is accessed by non-organization-managed computers or users, you increase trust in your Web site by deploying a Web Server certificate from a commercial CA.
  - The Web server is selling goods or services on the Internet. A commercial CA certificate can provide liability insurance for e-commerce transactions on the Web server.
- **Enable SSL for only those Web sites that require enhanced security.** There is extra performance overhead involved in connecting to a Web server implementing SSL. Only implement SSL in cases where you must prove the Web server's identity or provide encryption to data transmitted between the Web server and the Web client.
- **Ensure that all Web clients trust the root CA certificate of the Web Server's certificate chain.** If the Web Server certificate chains to a non-trusted root CA, users are warned that the certificate is not trusted, which can prevent them from connecting to the Web site.
- **Ensure that the Web Server certificate's subject matches the Web server's DNS name.** If the subject name does not match the Web site's DNS name, the user is warned.
- **Define certificate mappings in IIS if you have the following requirements:**
  - Define a mapping in a non-Active Directory environment. IIS is the only way to perform certificate mapping in a non-Active Directory environment without purchasing third-party products or developing custom solutions.
  - Require complex many-to-one mappings. The IIS interface for certificate mapping allows more complex definitions than Active Directory mapping. In Active Directory, you can only define a many-to-one mapping based on the issuing CA. In IIS, you can base information on the actual subject of the certificate.
- **Define certificate mappings in Active Directory if you have the following requirements:**
  - Requires usage at more than one IIS server. An Active Directory mapping can be used by any IIS server that is a member of the forest.
  - Requires strong protection of the user's password. An Active Directory mapping does not require input of the user's password. This allows for password changes without reconfiguring certificate mapping.

If you implement certificate mapping, the user certificate and server certificate must chain to root CAs trusted by both the Web client and the Web server. If the Web client's certificate was issued by a foreign CA hierarchy, you can either add its root CA to the Trusted Root Store or perform qualified subordination to only trust certificates with the Client Authentication application policy OID. In addition, you can define basic constraints and specific namespaces for the qualified subordination conditions.

## Case Study: The Phone Company

You manage the IIS Server for The Phone Company, a large telephone company with major offices in Toronto, Amsterdam, and Dallas. The Phone Company has a two-tier CA hierarchy with an offline root CA, named The Phone Company Root CA, at the Dallas office and three second-tier issuing CAs at the Toronto, Amsterdam, and Dallas offices. The CAs are named:

- The Phone Company Canadian Issuing CA
- The Phone Company American Issuing CA
- The Phone Company Dutch Issuing CA

The offline root CA is a standalone root CA owned and managed by The Phone Company, and the issuing CAs are members of the `thephonecompany.com` forest and are configured as enterprise subordinate CAs.

### Scenario

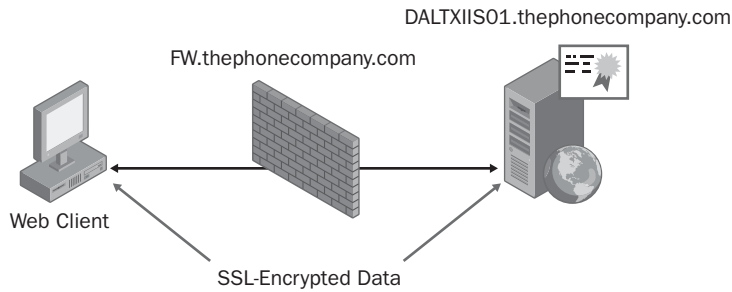
The Phone Company has two new Web-based applications you must deploy in the next month, and SSL is identified as a requirement for both Web-based applications.

#### The Customer Billing System

The first Web-based application is a customer bill reporting system that must be available to all customers by viewing `www.thephonecompany.com/billing`.

When customers connect to the Web page, they must enter their telephone number and assigned PIN in a Web-based form to authenticate with the application. Once authenticated, customers can view their phone records for the past six months, as well as make changes to their calling plans.

The computer that hosts the customer billing system Web site is at the Dallas office and is assigned the NetBIOS name `DALTXIIS01`. The `DALTXIIS01` Web server is protected by a Cisco PIX. (See Figure 17-7.) All traffic received on TCP port 443, the SSL port, is redirected to the `DALTXIIS01` server with no content inspection by the Cisco PIX firewall.

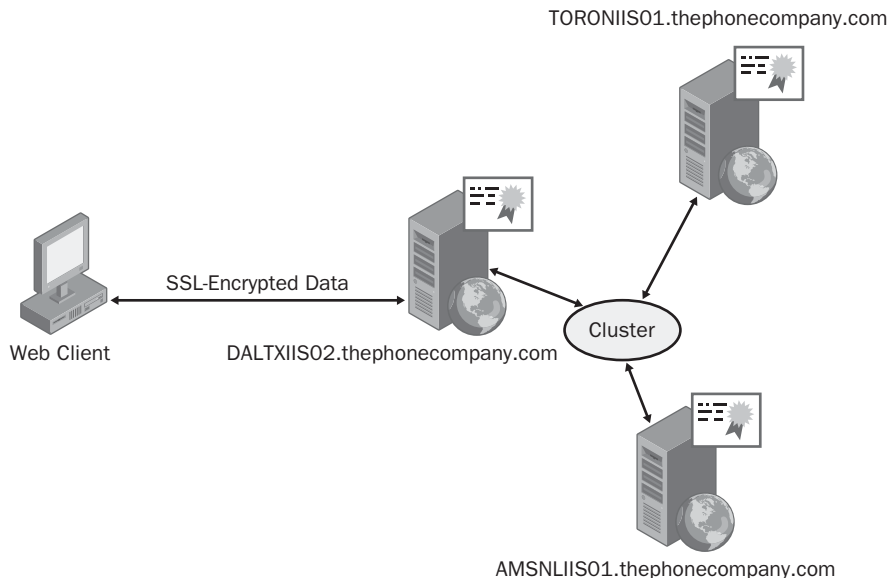


**Figure 17-7** The customer billing application Web server network infrastructure

## The Benefits Web Application

The second Web-based application is an internal application that allows The Phone Company's employees to review and modify their benefits.

To allow high-availability, the benefits Web site, <https://benefits.thephonecompany.com>, is deployed using an NLB cluster with the three Web servers—DALTXIIS02, AMSNLIIS01, and TORONIIS01—located at the Dallas, Amsterdam, and Toronto offices. (See Figure 17-8.) The three Web servers are members of Thephonecompany.com domain.



**Figure 17-8** The employee benefits application Web server network infrastructure

Only The Phone Company employees can access the benefits Web site. To provide enhanced password security, employees can only access the Web site using their smart card certificate. Employees use their existing The Phone Company smart cards, based on the Smart Card User certificate template.

## Case Study Questions

1. Which CA should issue the Web Server certificate for the customer billing system Web site?
2. Which CA should issue the Web Server certificate for the employee benefits Web site?
3. Where should the Web server certificate(s) be deployed for the customer billing system Web site?
4. Where should the Web Server certificate(s) be deployed for the employee benefits Web site?
5. How do you implement certificate mapping for the customer billing Web site?
6. If you perform an implicit certificate mapping, what form of name must be included in the Subject or the Subject Alternative Name extension of the user certificate? Does the Smart Card User certificate template meet this condition?
7. What subject is required for the Web Server certificate for the customer billing system Web site?
8. What subjects are required for the Web Server certificate for the employee benefits Web site?

## Additional Information

- Microsoft Official Curriculum, Course 2821: “Designing and Managing a Windows Public Key Infrastructure” ([www.microsoft.com/traincert/syllabi/2821afinal.asp](http://www.microsoft.com/traincert/syllabi/2821afinal.asp))
- “Step by Step Guide to Certificate Mapping” ([www.microsoft.com/windows2000/techinfo/planning/security/mappingcerts.asp](http://www.microsoft.com/windows2000/techinfo/planning/security/mappingcerts.asp))
- *Windows Security Resource Kit* by Ben Smith and Brian Komar ([www.microsoft.com/MSPress/books/6418.asp](http://www.microsoft.com/MSPress/books/6418.asp))
- “SSL Diagnostics Version 1.0” ([www.microsoft.com/downloads/details.aspx?FamilyId=CABEA1D0-5A10-41BC-83D4-06C814265282&displaylang=en](http://www.microsoft.com/downloads/details.aspx?FamilyId=CABEA1D0-5A10-41BC-83D4-06C814265282&displaylang=en))
- “Windows Server 2003 Resource Kit Tools” ([www.microsoft.com/downloads/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cffd&displaylang=en](http://www.microsoft.com/downloads/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cffd&displaylang=en))

- “Configuring Server Certificates for SSL” ([www.microsoft.com/resources/documentation/windows/2003/all/deployguide/en-us/iisdg\\_mea\\_nfmd.asp](http://www.microsoft.com/resources/documentation/windows/2003/all/deployguide/en-us/iisdg_mea_nfmd.asp))
- Knowledge Base Article 308160: “HOW TO: Configure Internet Information Services Web Authentication in Windows Server 2003”
- Knowledge Base Article 313070: “HOW TO: Configure Client Certificate Mappings in Internet Information Service 5.0”
- Knowledge Base Article 324069: “HOW TO: Set Up an HTTPS Service in IIS”
- Knowledge Base Article 324276: “HOW TO: Configure Internet Information Services Web Authentication in Windows Server 2003”
- Knowledge Base Article 330211: “ActiveX Error Messages Using Certificate Enrollment Web Pages to Enroll a Smart Card in Internet Explorer”
- Knowledge Base Article 310178: “HOW TO: Install Imported Certificates on a Web Server in Windows Server 2003”
- Knowledge Base Article 332077: “IIS 6.0: Computer Must Trust All Certification Authorities Trusted by Individual Sites”
- Knowledge Base Article 813618: “Security Alert: The Name of the Security Certificate Is Invalid or Does Not Match the Name of the Site”
- Knowledge Base Article 816794: “HOW TO: Install Imported Certificates on a Web Server in Windows Server 2003”



**Note** Microsoft Knowledge Base articles can be found at <http://support.microsoft.com>. Enter the article number in the Search the Knowledge Base text box.



# Chapter 18

## Secure E-Mail

Many organizations use e-mail as a method of communication between employees and external customers. By default, Internet e-mail is sent without any encryption, exposing the e-mail content to any users that are able to capture the packets as they traverse the network.

This chapter looks at the public key infrastructure (PKI) requirements for protecting e-mail with cryptographic measures.

### Securing E-Mail

Two different methods can be implemented to secure e-mail:

- **Securing the content of e-mail messages.** The content of e-mail messages is secured by implementing Secure/Multipurpose Internet Mail Extensions (S/MIME).



**Note** The design details of S/MIME version 3 are defined in RFC 2633, “S/MIME Version 3 Message Specification,” referenced in the “Additional Information” section of this chapter.

- **Securing data as it is transmitted between the mail client and the mail server.** The data stream is protected by implementing Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to provide validation of the mail server’s identity and encryption of the data transmitted between the mail server and the mail client.

The sections that follow provide more specific information on how the two methods work to protect e-mail messaging.

## Secure/Multipurpose Internet Mail Extensions (S/MIME)

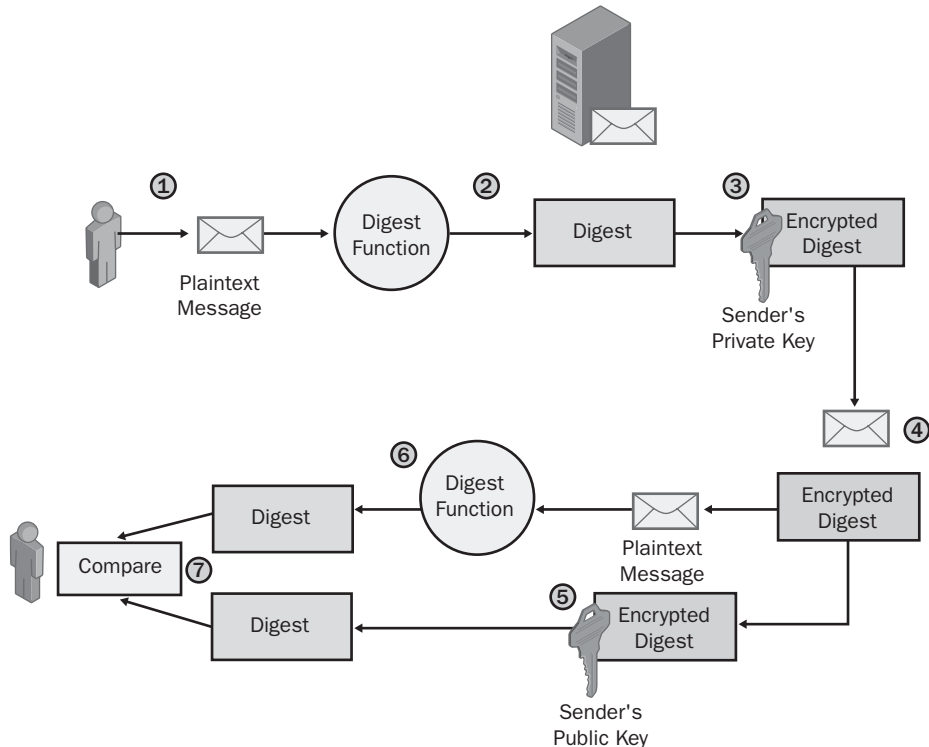
S/MIME allows e-mail programs to provide both digital signing and encryption services for e-mail delivery. S/MIME is an extension to MIME that allows digital data to be sent using text-based e-mail.

### E-Mail Digital Signing Process

E-mail digital signing uses the key pair of the sender so that the recipient can verify the authenticity of the message. (See Figure 18-1.) The process for e-mail signing is the same process used for general digital signing, except that the original text is the e-mail message.



**Note** The use of MIME extensions allows the digital signing of e-mail messages. MIME converts binary attachments to text-based extensions in the e-mail message. The S/MIME encryption is represented as an additional MIME in the e-mail message.



**Figure 18-1** The S/MIME e-mail signing process



1. The sender creates an e-mail message.
2. The sender's e-mail client runs a hash algorithm against the plaintext message to create a message digest.
3. The digest is encrypted using the sender's e-mail signing private key.
4. The plaintext e-mail message and the encrypted digest are sent to the recipient.



**Note** When using digital signing, no encryption is applied to the plaintext e-mail message. The e-mail message can be modified in transit, but modification invalidates the encrypted digest sent with the message.

5. The recipient decrypts the encrypted digest by using the sender's e-mail signing public key. Usually, the signing certificate, which contains the sender's public key, is included with the signed data.

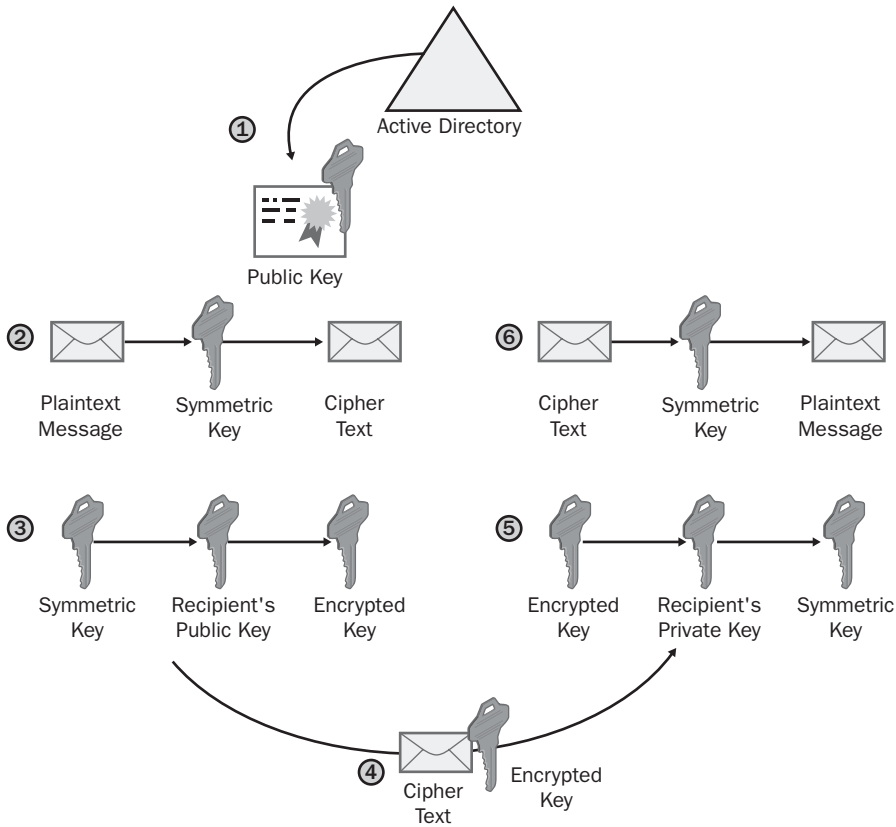


**Note** If the sender has an e-mail encryption certificate, the e-mail encryption and e-mail signing certificates are included in the sent message.

6. The recipient runs the same hash algorithm used by the sender to create a personal digest of the e-mail message. This digest is created against the plaintext e-mail message received from the originator.
7. The two digests are compared. If they differ, either the message or the digest has been modified during transmission.

## E-Mail Encryption Process

E-mail encryption uses the e-mail encryption key pair of the recipient of the e-mail message. When e-mail encryption is performed, the process shown in Figure 18-2 takes place.



**Figure 18-2** E-mail encryption process

1. The sender retrieves the recipient's e-mail encryption public key from Active Directory or another directory such as an e-mail contact list, and extracts the public key from the certificate.
2. The sender generates a symmetric key and uses this key to encrypt the original plaintext e-mail message.
3. The symmetric key is encrypted with the recipient's public key to prevent the symmetric key from being intercepted during transmission.
4. The encrypted symmetric key and encrypted e-mail message are sent to the intended recipient.
5. The recipient uses his or her private key to decrypt the encrypted symmetric key.
6. The encrypted e-mail message is decrypted with the symmetric key, which results in the recipient viewing the original plaintext e-mail message.

## SSL for Internet Protocols

In addition to digitally signing and encrypting e-mail messages, you can increase the security of authentication and data transmission for several Request for Comment (RFC) e-mail protocols. RFC-based protocols include:

- **Post Office Protocol 3 (POP3).** Used to retrieve e-mail messages from the user's Inbox on an e-mail server.
- **Internet Message Access Protocol 4 (IMAP4).** Used to retrieve any messages stored on an e-mail server. This includes messages in the user's Inbox and other message boxes on the e-mail server, including Drafts, Sent Items, and Public Folders.
- **Simple Mail Transfer Protocol (SMTP).** Used to send e-mail messages to e-mail recipients.
- **Network News Transfer Protocol (NNTP).** NNTP is used to download and post newsgroup messages from newsgroup servers.



**More Info** RFCs related to implementing Transport Layer Security (TLS) with these RFC-based protocols are listed in the “Additional Information” section of this chapter.



**Important** Although the RFCs reference TLS rather than SSL, the TLS RFCs describe compatibility between TLS and SSL version 3. It is an RFC-based client decision whether to refer to the security mechanism as TLS or SSL.

All of these RFC-based protocols use plaintext when transmitting data between the RFC-based client and the back-end server. If an attacker were to capture the data stream with a network sniffer, the attacker could read all contents of the data exchanged between the client and the server.

By implementing SSL, you can protect the RFC-based protocols that are used to send and receive e-mail from a server running Exchange 2000 or Exchange Server 2003. SSL encrypts the data between the e-mail client and the server. When SSL is implemented, the server accepts connections on the SSL port rather than on the standard port.

Table 18-1 shows the protocols that SSL can protect and lists the default and SSL-protected ports.

**Table 18-1 SSL Ports for E-Mail Protocols**

Protocol	Default port	SSL port
POP3	TCP 110	TCP 995
IMAP4	TCP 143	TCP 993
SMTP	TCP 25	TCP 25 or TCP 465
NNTP	TCP 119	TCP 563

To enable SSL at an Exchange Server, the Exchange Server must have a certificate installed that includes the Server Authentication Enhanced Key Usage (EKU) object identifier (OID), such as a certificate based on the Web Server certificate template. Only a single Web Server certificate is required for the Exchange server, the same Web Server certificate is used for each of the protocols, so long as the subject of the certificate matches the Domain Name System (DNS) name used by e-mail clients to connect to the server.

### Installing the Web Server Certificate

1. Log on to the Exchange 2000 or Exchange 2003 Server as an Exchange administrator.
2. From the Start menu, point to All Programs, point to Microsoft Exchange, and then click System Manager.
3. In the console tree, expand Servers, expand *ComputerName* (where *ComputerName* is the name of the Exchange Server), expand Protocols, expand *RFCProtocol* (where *RFCProtocol* is the name of the RFC-based protocol such as IMAP4 or POP3), right-click Default *RFCProtocol* Virtual Server, and then click Properties.
4. In the Default *RFCProtocol* Virtual Server Properties dialog box, on the Access tab, click Certificate.
5. In the Web Server Certificate Wizard, click Next.
6. On the Server Certificate page, click Create a New Certificate, and then click Next.



**Note** If you already have a Web Server certificate installed on the Web server, you can choose the Assign an Existing Certificate option.

7. On the Delayed or Immediate Request page, click Send the Request Immediately to an Online Certification Authority, and then click Next.



**Note** This assumes that you are requesting the certificate from an enterprise certification authority (CA) and not from a standalone CA. If you are submitting the request to a standalone or commercial CA, you must save the request to a request file.

8. On the Name and Security Settings page, accept the default name and bit length, and then click Next.
9. On the Organization page, enter the organization name and organizational unit, and then click Next.
10. On the Your Site's Common Name page, type the DNS name used to connect to the e-mail server, and then click Next.
11. On the Geographical Information page, enter the Country, State/Province, and City/Locality for the e-mail server, and then click Next.
12. On the Choose a Certification Authority page, select an available enterprise certification authority (CA) from the drop-down list, and then click Next.
13. On the Certificate Request Submission page, verify the details of the certificate request, and then click Next.
14. On the Completing the Web Server Certificate Wizard, click Finish.

### Enabling SSL for an RFC-Based Protocol

Once the Web server certificate is installed, the following procedure will enable SSL for an RFC-based protocol:

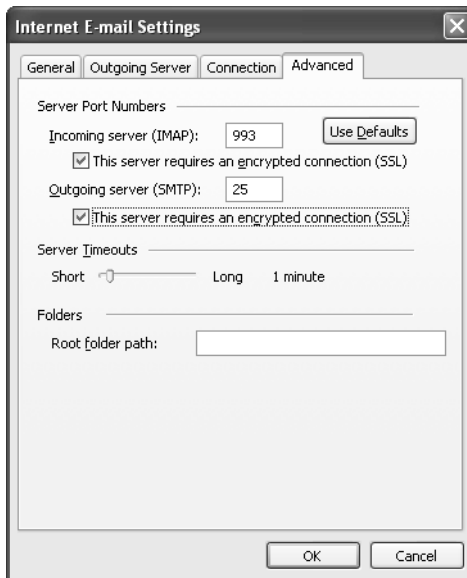
1. Ensure that you are still viewing the Default *RFCTProtocol* Virtual Server Properties dialog box.
2. In the Default *RFCTProtocol* Virtual Server Properties dialog box, on the Access tab, click Communication.
3. In the Security dialog box, enable the Require Secure Channel check box, enable the Require 128-Bit Encryption check box, and then click OK.
4. In the Default *RFCTProtocol* Virtual Server Properties dialog box, click OK.



**Warning** The enabling of SSL at an Exchange Server will likely require modification of the organization's firewall to allow communications to the Exchange Server from the Internet to the SSL listening ports. In addition, the firewall can close or deny access to the non-SSL ports for the RFC-based protocols.

## Enabling SSL in the E-mail Applications

Once you have enabled SSL on the Exchange Server, you must enable SSL in your organization's e-mail client software. The e-mail client software must be modified to use the SSL ports rather than the non-SSL ports. For example, Figure 18-3 shows how Microsoft Outlook 2003 is configured to enable SSL for both IMAP4 and SMTP.



**Figure 18-3** Enabling SSL for IMAP4 and SMTP in Outlook 2003



**Note** The actual configuration steps to enable SSL depend on the specific e-mail application software used by your organization. For details on how to enable SSL, review the Help files and documentation provided with the e-mail application.

## Another Alternative for Secure E-Mail

RFC-based protocols are often used to connect to the corporate mail server from an employee's a home computer or while on the road. When combined with SSL, RFC-based protocols can provide a secure method for remote users to access their mailboxes hosted on a Microsoft Exchange Server. Rather than implementing SSL for RFC-based protocols, two other alternatives exist to allow users to securely connect to the corporate mail server:

- **Outlook Web Access (OWA).** Outlook Web Access provides Active Server Pages (ASP) connectivity to the Microsoft Exchange Server. ASPs allow a user full access to a personal mail store, including the ability to use S/MIME when using Exchange Server 2003.

**Important** RPC over HTTP is only supported by Exchange Server 2003 with Outlook 2003 clients installed on Microsoft Windows XP Service Pack 1 and later.

- **RPC over HTTP.** RPC over HTTP allows the remote procedure call (RPC) commands to be encapsulated in an HTTP header.

## Choosing Certification Authorities

When your organization chooses to implement secure e-mail using S/MIME, the first decision that must be made is where to acquire the S/MIME certificates. Your organization can choose to acquire the certificates from a commercial CA or issue the certificates from a private CA.

### Choosing Commercial CAs

An organization will choose to obtain a user's S/MIME certificates from a commercial CA when the user sends the majority of the S/MIME-protected e-mail messages to people outside the organization. Using a certificate issued by a commercial provider, such as VeriSign, that is trusted by most organizations increases the probability that a user outside the organization will trust a digital signature created with the certificate issued by the commercial CA. The drawback is that the organization must purchase each S/MIME certificate issued to its employees.



**Note** Alternatively, an organization can choose to purchase a subordinate CA certificate from a commercial organization. The commercial organization will then appear as the root CA in the CA hierarchy when an e-mail certificate is validated by another organization. One example of this type of service is beTrusted's Omniroot program ([www.betrusted.com/products/omniroot/chaining.asp](http://www.betrusted.com/products/omniroot/chaining.asp)). If you choose to create a subordinate CA below a commercial root CA, you must ensure that the Authority Information Access (AIA) and CRL Distribution Point (CDP) URLs included in the certificates issued by the subordinate CA are available on the Internet for certificate validation purposes.

## Choosing Private CAs

An organization will choose to issue certificates from a private CA when the majority of the e-mail secured with S/MIME is exchanged between users of the organization. Because all the users exchanging S/MIME e-mail trust the same trusted root CA, all digital signing and encryption operations are trusted. There are no additional costs for issuing the private S/MIME certificates to an organization's employees because the certificate infrastructure is owned and managed by the organization. In addition, methods such as autoenrollment can be implemented to aid in the distribution of the S/MIME certificates.

### Using Multiple Profiles

---

There are cases where a user can acquire two different sets of S/MIME certificates: one set for internal use and one set for external use. If the user is using Outlook, the user can create two separate profiles for sending e-mail:

- The first profile designates that the internally issued certificates be used for all digital signing and encryption options.
- The second profile designates that the commercially issued certificate be used for all digital signing and encryption options.

Both profiles access the same Microsoft Exchange Server mailbox, but each designates a different certificate combination for S/MIME transactions.



## Choosing Certificate Templates

If your organization chooses to deploy its own certificates for secure e-mail, the first decision that the organization must make is whether to use the same certificate for both signing and encryption operations, or to issue two separate certificates: one for digital signing and one for encryption.

The advantage of a single certificate is that the user only has to manage a single certificate for all e-mail operations. The disadvantage is that if your organization implements key archival of the e-mail certificate, it is possible that another person could gain access to the signing private key associated with the e-mail certificate.



**Note** For details on enabling key archival at a CA and the security issues of archiving private keys used for digital signing, review Chapter 14, “Archiving Encryption Keys.”

The advantage of issuing separate certificates for signing and encryption operations is that by delegating encryption operations to one certificate, you can safely archive the encryption certificate without fear of signing impersonations. The private key associated with the e-mail signing certificate is not archived; only the private key for encryption is archived.

### A Combined Signing and Encryption Template

If you implement a single certificate for e-mail, it is recommended that you create a version 2 certificate template based on either the Exchange User or Exchange Signature Only certificate template.

Use these recommendations for each tab when you create the custom version 2 certificate template:

- **General.** Ensure that you publish the certificate in Active Directory to allow other users to send encrypted e-mail to the user referenced in the certificate. You can use your organization’s naming conventions for the certificate template and define the validity period and renewal period based on the technical requirements of the organization.

- **Request Handling.** Change the Purpose of the certificate to Signature and Encryption to allow both digital signing and encryption. Alternatively, you can enable the following options based on the requirements of your organization:
  - **Key archival.** Key archival stores an encrypted copy of the e-mail certificate's private key in the CA database.
  - **Private key protection.** Enabling the option to Prompt the user during enrollment and require user input when the private key is used ensures that the user can assign a password, separate from the logon password, that protects the user's private key.
- **Subject name.** Enable populating the subject from information stored in Active Directory. For S/MIME purposes, the certificate's subject must include the user's e-mail address in either the Subject field or the Subject Alternative Name extension.



**Important** If the user account associated with the user requesting the certificate does not have a value in the E-mail-Addresses attribute, the certificate request will fail. The requesting user accounts must have the E-mail-Addresses attribute populated.

- **Security.** A custom universal or global group that contains all users that will perform S/MIME digital signing and encryption must be assigned the Read, Enroll, and Autoenroll permissions. This permission combination will allow deployment of the certificate to users with Windows XP computers by using autoenrollment.



**Note** No modifications are required for the Issuance Requirements, Superseded Templates, and Extensions tabs.

## Dual Certificates for E-Mail

Due to the risks of archiving the private key associated with a S/MIME signing certificate, many organizations choose to implement separate certificates for e-mail signing and encryption. Deploying separate certificates ensures that only the private key associated with the e-mail encryption certificate is archived.

## E-Mail Signing Certificate Template

If you implement a separate certificate template for e-mail signing, it is recommended that you duplicate the Exchange Signature Only certificate template. When you separate the e-mail signing and e-mail encryption certificates, you can choose to deploy the signing certificate on a smart card. If you choose this option, when you duplicate the Exchange Signature Only certificate template you must make the same changes recommended for the combination e-mail signing and e-mail encryption certificate. The only differences in the settings are on the General and Request Handling tabs.

### General Tab

On the General tab, it is recommended that you *not* enable the Publish Certificate in Active Directory check box. A user does not have to retrieve the user's certificate to verify the signature on an e-mail message because the certificate is included in the message payload.

### Request Handling Tab

On the Request Handling tab, the recommended settings when you deploy the certificate on a smart card are:

- Purpose: Signature and Smart Card Logon
- Prompt the user during enrollment: Enabled
- CSP: Microsoft Enhanced Cryptographic Provider v1.0

If you choose to deploy the e-mail signing certificate as a certificate stored in the user's profile, the following settings are recommended for the Request Handling tab:

- Purpose: Signature
- Allow Private key to be exported: Enable this option if your organization allows export of the e-mail signing private key. Disable this option if your organization does not allow export of the e-mail signing private key.
- Prompt the user during enrollment and require user input when the private key is used: Enabled
- CSP: The smart card CSP associated with your organization's selected smart card vendor.

## Strong Private Key Protection

---

When you enable strong private key protection, the user is prompted during the enrollment process to enable medium or high security on the certificate's private key.

- If the user selects *medium*, then the user is prompted each and every time the private key associated with the certificate is accessed. The user must click an OK button to acknowledge that the private key is being accessed.
- If the user selects *high*, then the user is prompted to input a password each and every time the private key associated with the certificate is accessed. The user must type the password in order to access the private key.

**Warning** If the user forgets the password required to access the private key, all access to the private key is lost. Unless the private key is archived at the CA, there is no method of recovering the existing private key.

Although it is possible to enforce that the user select high protection for all private keys by enabling the *System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing* policy setting, this Group Policy Object (GPO) or local policy setting cannot be enabled if the organization deploys applications such as Encrypting File System (EFS) or wireless authentication. Applications such as EFS and wireless authentication do not expose an interface for the user to provide the password protecting the private key, causing the applications to silently fail.

## E-Mail Encryption Certificate Template

When you implement a separate certificate for e-mail encryption, it is recommended that you duplicate the Exchange User certificate template. The separate e-mail encryption certificate allows you to enable key archival for the encryption certificate. As key archival is not supported for smart card certificates, you must store the certificate in the user's personal store.

When you duplicate the Exchange User certificate template, you must make the same changes recommended for the combination e-mail signing and e-mail

encryption certificate. The only differences are the settings on the General tab and the Request Handling tab.

On the General tab, ensure that you enable the Publish Certificate in Active Directory check box so that other users can retrieve the user's certificate from the global catalog when sending encrypted e-mail to the user.

On the Request Handling tab, ensure that the following settings are defined:

- Purpose: Encryption
- Archive subject's encryption private key: Enabled
- Include symmetric algorithms allowed by the subject: Enabled
- Allow private key to be exported: Enabled



**Note** You only have to allow the export of the private key if a user has Windows 2000 or earlier. This check box does not have to be enabled if only Windows XP or Windows 2003 clients are deployed, as key archival can take place without enabling the export option.

- Prompt the user during enrollment and require user input when the private key is used: Enabled
- CSP: Microsoft Enhanced Cryptographic Provider v1.0

## Choosing Deployment Methods

Whether you choose to deploy a single e-mail certificate or to implement separate e-mail signing and e-mail encryption certificates, it is recommended that you enable autoenrollment for the deployed certificate template(s).

Autoenrollment allows the automated enrollment of the e-mail certificates to all users that have a Windows XP computer that is a member of the domain.



**Important** Automated enrollment requires the user's input if you enable a smart card for the signing certificate or implement strong private key protection for the certificates.

If your network includes Windows 2000 or earlier clients, you cannot use the Windows Server 2003 native autoenrollment methods. Instead, you must choose from the following methods to deploy the custom certificates:

- **Web Enrollment.** A user with membership in a global or universal group assigned the Read and Enroll permissions can enroll both version 2 certificates by using the Certificate Services Web Enrollment pages.
- **Scripted enrollment of the e-mail encryption certificate.** A user can run the `EmailwithKeyArchive.vbs` script provided on the accompanying CD to automate the request of the e-mail encryption certificate. To run the script, the user must either double-click the script or type **`cscript EmailwithKeyArchive.vbs`** from a command line. This script must be edited to fit your organization's environment before execution, as follows:
  - Line 77 must be modified to reflect the DNS name and logical name of an enterprise CA on your network. For example, if the DNS name of the CA computer is `issuingca.example.com` and the logical name of the CA is Example Corporation Issuing CA, you must modify the line to read `Const StrCAConfig = "issuingca.example.com\Example Corporation Issuing CA"`.
  - Line 89 must be modified to reflect the name of the certificate template used by your organization. The line is currently set to request a certificate template named "EmailEncrypt".
- **Scripted enrollment of the e-mail signing certificate.** A user can run the `enroll.vbs` script provided on the accompanying CD to automate the request of the e-mail signing certificate. The user must run the script from a command line using the following syntax:

```
cscript enroll.vbs /ca "issuingca.example.com\Example Corporation Issuing CA"
/certype EmailSign /keyl 1024 /csp enhanced
```



**Note** This command line assumes that the name of the CA to which you are submitting the request is named "issuingca.example.com\Example Corporation Issuing CA" and the certificate template is named EmailSign.

## Enabling Secure E-Mail

Once you have successfully deployed the certificates to the users, each user must configure his or her e-mail application to use the e-mail certificates for S/MIME protection. The following sections detail how to enable S/MIME security in:

- Outlook
- Outlook Express
- Outlook Web Access (OWA)



**Note** S/MIME is only available in the OWA provided with Exchange Server 2003. Previous versions of OWA do not provide support for S/MIME protection.

## Enabling Outlook

Both Outlook 2002 and Outlook 2003 automatically use available e-mail signing and e-mail encryption certificates if the certificates exist in the user's profile.

You can verify the existence of the certificates, and define the encryption and signing algorithms using the following procedure:

1. Open Outlook.
2. On the Tools menu, click Options.
3. In the Options dialog box, on the Security tab, click Settings.
4. In the Change Security Settings dialog box (see Figure 18-4), ensure that the following settings are defined:



**Figure 18-4** Defining S/MIME Settings in Outlook 2003

- Cryptography Format: S/MIME.
- Default Security Settings for this cryptographic message format: Enabled.
- Default Security Settings for all cryptographic messages: Enabled.
- Hash Algorithm: SHA1 or MD5—but SHA1 is recommended.

- Encryption Algorithm: 3DES, RC2 (128-bit), RC2 (64-bit), DES, RC2 (40-bit)—but 3DES is recommended.
- Send these certificates with signed messages.



**Note** For a review of the strengths and weaknesses of each hash and encryption algorithm, see Chapter 1, “Basics of Cryptography.”

5. In the Change Security Settings dialog box, click OK.
6. In the Options dialog box, click OK.

## Enabling OWA

To allow S/MIME usage in OWA, you must install the S/MIME ActiveX control at the client computer. The S/MIME ActiveX control enables using S/MIME for signing and encrypting e-mail messages.



**Important** Only a local administrator or member of the local Power Users group can install the ActiveX control. Once the control is installed, all users can use it. In addition, the ActiveX control requires Internet Explorer version 6.0 or later running on Windows 2000 or later.

To install the S/MIME ActiveX control:

1. Log on to the computer as a member of the local Administrators or Power Users group.
2. Open Internet Explorer.
3. In Internet Explorer, open the URL *http://ExchangeServer/exchange* (where *ExchangeServer* is the DNS name of the Exchange 2003 Server hosting the user’s mailbox).
4. When prompted, type the user name and password for accessing your mailbox.
5. In Outlook Web Access, in the Navigation Pane, click Options.
6. On the Options page, under E-Mail Security, click Download.
7. In the File Download dialog box, click Open.
8. If any security warnings appear, click Yes to install the ActiveX control.



## Enabling Outlook Express

Outlook Express does not automatically assign certificates for S/MIME usage. You must modify the properties of your existing POP3 or IMAP e-mail account to select the certificates for secure e-mail.

The following procedure designates the e-mail signing and e-mail encryption certificates:

1. Click Start, point to All Programs, and click Outlook Express.
2. If prompted to set Outlook Express as your default e-mail client, click No.
3. On the Tools menu, click Accounts.
4. In the Internet Accounts dialog, on the Mail tab, select your POP3 or IMAP mail account, and then click Properties.
5. In the Mail Account Properties dialog box, on the Security tab, in the Signing Certificate section of the dialog box, click Select.
6. In the Select Default Account Digital ID dialog box, select the S/MIME signing certificate, and then click OK.



**Tip** By assigning a friendly name to the e-mail signing certificate during the enrollment process, you can easily identify the correct certificate if multiple certificates are displayed. The only time that you cannot assign a friendly name to the e-mail signing certificate is when the certificate is deployed using autoenrollment settings.

7. In the Mail account Properties dialog box, on the Security tab, in the Encrypting Preferences section of the dialog box, click Select.
8. In the Select Default Account Digital ID dialog box, select the S/MIME encryption certificate, and then click OK.
9. In the Algorithm drop-down list, select the encryption algorithm used by your organization, and then click OK.



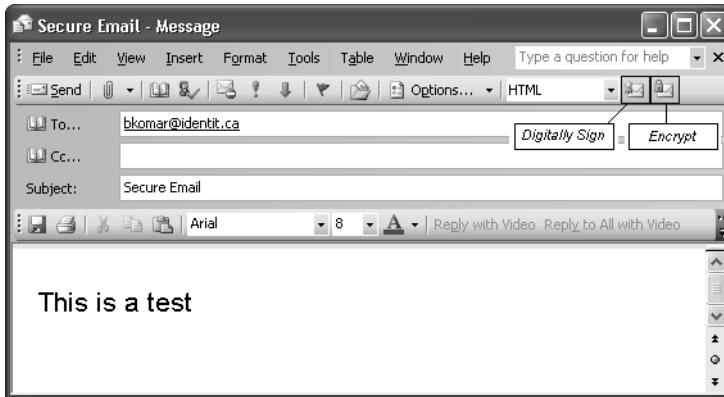
**Note** To ensure the strongest encryption method for S/MIME e-mail messages, it is recommended that you use 3DES encryption.

10. In the Internet Accounts dialog box, click OK.

## Sending Secure E-Mail

Once you have enabled S/MIME in the e-mail package, the decision to send secure e-mail is made for every message sent by the e-mail participant.

For example, Figure 18-5 shows a message window in Outlook 2003 that is enabled for both digital signing and e-mail encryption.



**Figure 18-5** Defining S/MIME Settings in Outlook 2003

By enabling the Digital Signing button and the Encryption button, the sender can decide whether to implement signing, encryption, or both encryption and signing for the outbound e-mail message. In addition, the user can select what defaults to enable within the e-mail client for S/MIME e-mail.



**Note** Although Figure 18-5 shows the Outlook 2003 client, similar buttons for enabling digital signing and encryption exist in Outlook Express and OWA.



**Important** To send encrypted e-mail to a recipient, the sender must have access to the recipient's public key. In an Active Directory environment, the sender retrieves the certificate from the global catalog. The certificate is added to the *userCertificate* attribute of the user account during the enrollment process by enabling the Publish certificate in Active Directory check box in the e-mail encryption certificate template. The *userCertificate* attribute is replicated to the global catalog. For nondomain members, the users can exchange encryption certificates by sending signed e-mail messages, and then creating a contact object for the other user. The properties of the contact object include the signing and encryption certificates.

# Migrating from Previous Exchange Server Versions

Previous versions of Microsoft Exchange Server implemented the Key Management Service (KMS) to provide recovery of encryption private keys associated with S/MIME. In these Microsoft Exchange environments, the KMS requested the S/MIME encryption certificates on behalf of the e-mail user, allowing the KMS to archive the e-mail encryption certificate's private key.

With the Windows Server 2003 enterprise CA, it is possible to have all encryption certificates archived in the same location, rather than using an application-specific solution, such as the Exchange KMS. To allow a smooth migration from Exchange KMS, it is possible to import the KMS database into the Windows Server 2003 enterprise CA.



**Note** There are version dependencies for the migration process. The Exchange Server must be running Exchange Server 2000, and the enterprise CA must be running Windows Server 2003, Enterprise Edition, or Windows Server 2003, Datacenter Edition.

The following process is required to migrate an existing Exchange 2000 KMS Server database to a Windows Server 2003 Certificate Authority database:

1. If running Exchange 5.5 KMS, upgrade to Exchange 2000.
2. Enable key archival at the Windows Server 2003 enterprise CA.
3. Install an encryption certificate at the issuing CA.
4. If necessary, enable foreign certificate import at the enterprise CA.
5. Export the Exchange KMS database at the Microsoft Exchange server.
6. Import the Exchange database into the enterprise CA database.

The sections that follow provide more details on each step in the process.

## Upgrade to Exchange 2000

Export of the Exchange KMS database is only possible in Microsoft Exchange Server 2000. If your organization is still using Microsoft Exchange 5.5 or earlier, you must first upgrade to Microsoft Exchange Server 2003 before migrating the KMS database to a Windows Server 2003 enterprise CA.



**Note** In addition to upgrading to Microsoft Exchange 2000, you also should apply the latest Microsoft Exchange 2000 service pack and security updates.

## Enable Key Archival at the Windows Server 2003 Enterprise CA

The migration of the Exchange Server KMS database requires a Windows Server 2003 enterprise CA that is enabled for key archival. As discussed in Chapter 14, “Archiving Encryption Keys,” you must designate one or more Key Recovery Agent certificates at the enterprise CA to enable key archival. Once Certificate Services is restarted, the enterprise CA is enabled for key archival.

## Install an Encryption Certificate at the Enterprise CA

The KMS migration process requires the enterprise CA to provide an encryption certificate to the person performing the KMS database export. The public key from the CA’s encryption certificate is used to encrypt the KMS database export so that the KMS database can only be imported into the database of the CA that holds the private key associated with the certificate.



**Note** For the purpose of KMS database import, you can use a Web Server certificate, a Computer certificate, or any other certificate that enables the Key Usage option to Allow Key Exchange Only With Key Encryption. The certificate must be issued to the enterprise CA.

## Enable Foreign Certificate Import at the Enterprise CA

You must enable foreign certificate import at the enterprise CA if you are importing certificates from the KMS database that were not issued by that specific enterprise CA. Foreign certificate import is required if the certificates are X.509 version 1 certificates generated by the KMS or if the KMS service requested the certificates on behalf of a user from another Windows CA.



**Note** The KMS service in Exchange 5.5 and Exchange 2000 could be configured to request certificates from a Windows CA: a standalone CA was required for Exchange 5.5 and an enterprise CA for Exchange 2000. If the CA used by the KMS service is upgraded to a Windows Server 2003, there is no need to enable foreign certificate import.

To enable foreign certificate import at an enterprise CA, a local administrator must type the following command at a command prompt:

```
certutil -setreg ca\KRAFlags +KRAF_ENABLEFOREIGN
```

In addition, Certificate Services must be restarted after running this certutil command to ensure that Certificate Services is aware of the setting change.



**Note** It is also possible to import individual PKCS #12 files into an enterprise CA database. To import an individual PKCS #12 file you must enable foreign certificate import.

## Export the Exchange KMS Database

Once you have enabled the enterprise CA for foreign certificate import, you can start the export process:



**Warning** The export of data from the KMS database is a destructive process that removes the certificate and private keys from the KMS database. To protect against accidental loss of data, ensure that you perform and verify a backup of the KMS server before starting the export process.

1. If the KMS is configured to request certificates from an existing enterprise or standalone CA, stop Certificate Services on that CA.



**Important** If the CA used by the KMS server is online during the export process, the KMS server will attempt to revoke every X.509 version 3 certificate that is exported from the KMS server

2. Log on as an Exchange administrator.
3. Start the Exchange System Manager.
4. In the console tree, expand Administrative Groups, expand *AdminGroup* (where *AdminGroup* is the name of the administrative group), and then click Advanced Security.
5. In the details pane, right-click Key Manager, point to All Tasks, and then click Export Users.

6. In the Key Management Service Logon dialog box, type the Key Management Service password, and then click OK.
7. In the Exchange KMS Key Export Wizard, click Next.
8. On the Encryption Certificate page, in the Path box, type the full path of the CA's encryption certificate, and then click Next.
9. In the Windows Explorer, open the CA's encryption certificate, and click the Details tab.
10. In the Certificate dialog box, on the Details tab, select the Thumbprint field so that the value of the thumbprint is displayed.
11. On the Certificate Thumbprint Verification page, in the Thumbprint box, type the first eight characters of the Thumbprint field, as displayed in the Certificate dialog box, and then click Next.
12. On the Export Filename page, in the Export File box, type the name of the export file, and then click Next.



**Important** Do not include any path information when typing the file name. The export file is automatically created in the C:\program files\exchsrvr\KMSDATA folder, assuming that Exchange Server is installed in the default location without a file extension.

13. On the User View Selection page, click Display Mailbox Stores, Exchange Servers, and Administrative Groups of Eligible Users, and then click Next.



**Note** Alternatively, you could select to display an alphabetical list of users and select mailboxes on a user-by-user basis.

14. On the User Container Selection page, select the mailbox store, Exchange Server, or administrative group to export, and then click Next.
15. On the Ready to Export page, click Next.



**Note** The export will process roughly 100 records per minute.

16. On the Completing the Export Advanced Security Users Wizard page, click Finish.



**Note** If a large number of certificates and private keys are exported, the export wizard will generate multiple export files. If multiple export files are generated, all export files must be imported at the target enterprise CA.

17. Copy the C:\program files\exchsrvr\KMSDATA\KMSExportFile(s) to the file system of the target enterprise CA.

## Import the Exchange KMS Database into Enterprise CA Database

Once the export file or export files are copied to the file system of the target enterprise CA, you can import the export file(s) into the enterprise CA database. Use the following procedure to import the certificates and private keys from the KMS export file(s).

1. Open a command prompt.
2. Make the folder that contains the export file(s) the current directory.
3. At the command prompt, type **certutil.exe -f -importkms *ExportFile*** for each *ExportFile* in the current directory.
4. Ensure that the output of the certutil command indicates that the import was successful.



**Important** The export file can only be opened by the CA that holds the private key associated with the encryption certificate used during the KMS export process. If the import is attempted at another enterprise CA, the import will fail because the CA will be unable to decrypt the export file.

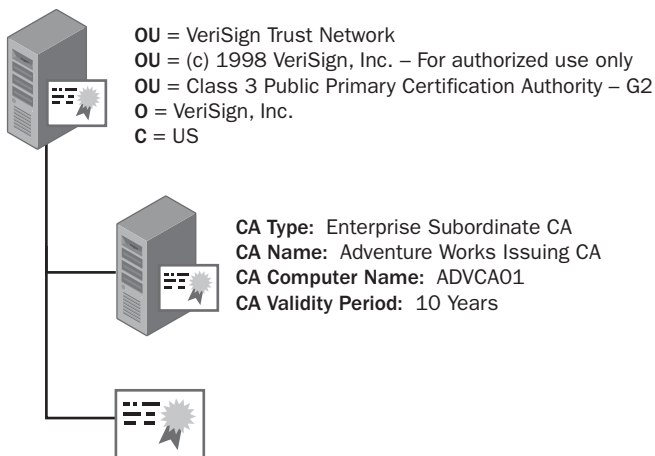
## Best Practices

- **Issue separate certificates for e-mail signing and encryption.** Using separate certificates allows your organization to archive the private keys of e-mail encryption certificates, yet not archive the private keys for e-mail signing certificates. If you use a single certificate for both signing and encryption, there is a greater possibility of identity theft. Finally, implementing separate signing and encryption e-mail certificates allows an organization to restrict a user to performing e-mail encryption or e-mail signing. If the organization only wants to implement e-mail signing, it can issue a certificate that only enables e-mail signing.

- **Use strong private key protection for e-mail signing and encryption certificates.** Strong private key protection provides additional security for certificates stored in a user's profile. Every time the private key of the certificate is accessed, the user must provide a password. This strong private key protection prevents an administrator who resets the user's password from gaining access to the e-mail certificate private keys.
- **Provide key archival for e-mail encryption certificates.** Key archival allows the user's private key to be recovered in the event that the private key is deleted or corrupted. Retrieving the private key allows the user to gain access to e-mail previously encrypted with the public key of the key pair.
- **Use autoenrollment or scripted enrollment to distribute e-mail certificates to users.** Automated enrollment ensures that each user obtains the required certificates for e-mail with minimal user actions. If you enable strong private key protection, the user will be prompted to provide the password used to protect the private key.
- **Ensure that AIA and CDP URLs are accessible from both the private network and the Internet.** If you send signed e-mail or receive encrypted e-mail, you must ensure that at least one AIA and one CDP URL are accessible from the private network or from the Internet to allow certificate validation to succeed.

## Case Study: Adventure Works

You manage the network for Adventure Works, a travel agency in New York that specializes in radical vacation trips. The organization implements the CA hierarchy shown in Figure 18-6.



**Figure 18-6** The Adventure Works CA hierarchy

To provide increased trust of the certificates issued by the Adventure Works Issuing CA, Adventure Works has purchased a subordinate CA certificate from Veri-



Sign. The VeriSign root CA certificate is included in the packaged list of trusted root CAs distributed by Microsoft with the Windows operating system, increasing the trust in the certificates issued by the Adventure Works Issuing CA.

## Scenario

Adventure Works implements Exchange Server 2003 in a single domain forest named `adventureworks.com`. The Exchange Server, `ADVEXCH01`, provides e-mail services to all employees of Adventure Works and is also used to send and receive e-mail over the Internet. All client computers use Outlook 2003 to connect to the mail server.

All servers on the network are running Windows Server 2003, Enterprise Edition, and the client computers are running Windows XP. The latest service packs are installed and security updates are applied to all client computers on a weekly basis.

Recently, the IT, human resources, and legal departments drafted security policies for the Adventure Works network. The following security policies are related to e-mail:

- Any e-mail messages containing proposed or confirmed flight itineraries to customers must be signed to provide confidence to the customers that the contents are valid and did originate from the Adventure Works travel consultant.
- Any e-mail messages containing customer confidential information such as passport numbers, credit card numbers, and bank account information must be encrypted. In addition, any e-mail messages containing classified data must be encrypted when sent to employees.
- The private keys associated with encryption certificates must be archived at the issuing CA to allow recovery of the private key in the event of computer failure, computer rebuild, profile deletion, or corruption of the private key. All key recovery must require the participation of at least two employees to prevent unauthorized access to a user's encryption key.
- The private keys associated with signing certificates must never be archived in order to ensure that two users do not have access to the same signing certificate.
- E-mail signing and encryption private keys must be protected by a password. The password must be typed each and every time the private key is accessed.

In addition to enforcing the security policies defined for Adventure Works, the secure e-mail project must meet the following design requirements:

- Several of the agents participate in a job-sharing program. When an agent comes into the office, there is no guarantee that he or she will sit at the same computer, so e-mail certificates must be portable.
- Some of the agents have laptop computers and connect to the mail server, `ADVEXCH01`, from remote locations. Secure access to their e-mail must be provided, as well as the ability to use S/MIME for signing and encrypting e-mail.

## Case Study Questions

1. Based on the security policies related to e-mail usage, how many e-mail certificates must be distributed to each user?
2. What certificate(s) must be published to Active Directory to enable the sending of encrypted e-mail between employees of Adventure Works?
3. Will the current CA infrastructure allow the e-mail signing and e-mail encryption certificates to be recognized by the customers of Adventure Works?
4. What method would you use to deploy the e-mail certificate(s) to the Adventure Works users? What certificate template settings are required to allow this method of enrollment?
5. One of the travel agents is able to open his encrypted e-mail at only one of the available agent computers. When he attempts to open his encrypted e-mail at the other computers, the attempt fails. What can you do to ensure that the travel agent can open the encrypted e-mail at any of the travel agent computers?
6. How do you propose to enforce the security policy that two or more people must be involved in the recovery?
7. How do you enforce that users must provide a password to access the private keys associated with the e-mail signing and e-mail encryption certificates?
8. What must a travel agent do to allow a customer to send an encrypted e-mail message?
9. What solution can be used to allow remote travel agents to securely access their e-mail and use S/MIME to protect the e-mail messages without enabling an additional e-mail client?
10. One of the travel agents has forgotten the password used to protect the e-mail encryption certificate and can no longer read encrypted e-mail. What must you do to allow the travel agent to access the encrypted e-mail?
11. When performing the proof of concept test of your e-mail solution, you are told that customers are complaining that their e-mail applications are reporting that the digital signatures are failing. You look at the certificate and find the following URLs in the CDP extension:
  - *LDAP:///CN=Adventure Works Issuing CA,CN=ADVCA01,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=travelworks,DC=com*
  - *http://advca01/certenroll/Adventure%%20Works%%20%%20Issuing%%20CA.crl*

What is causing the certificate validation to fail? What must you do to fix the problem?

## Additional Information

- Microsoft Official Curriculum, Course 2821: “Designing and Managing a Windows Public Key Infrastructure” ([www.microsoft.com/traincert/syllabi/2821afinal.asp](http://www.microsoft.com/traincert/syllabi/2821afinal.asp))
- “Key Archival and Management in Windows Server 2003” ([www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/kyacws03.mspix](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/kyacws03.mspix))
- “Exchange Server 2003 Message Security Guide” ([www.microsoft.com/technet/prodtechnol/exchange/2003/library/exmessec.mspix](http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/exmessec.mspix))
- “Exchange 2000 Deployment Guide: Chapter 9—Ensuring Messaging Security” ([www.microsoft.com/technet/prodtechnol/exchange/2000/deploy/upgrademigrate/series/planningguide/p\\_09\\_tt1.mspix](http://www.microsoft.com/technet/prodtechnol/exchange/2000/deploy/upgrademigrate/series/planningguide/p_09_tt1.mspix))
- “Windows 2000 Server and Key Management Server Interoperability” ([http://support.microsoft.com/support/exchange/content/whitepapers/win2k\\_kms.doc](http://support.microsoft.com/support/exchange/content/whitepapers/win2k_kms.doc))
- “Overview of Cryptography in Outlook 2003” (<http://go.microsoft.com/fwlink/?LinkId=17808>)
- “Quick Start Guide for S/MIME in Exchange Server 2003” ([www.microsoft.com/downloads/details.aspx?FamilyId=F2D49F68-9E36-414B-906B-13C7C075E1B1&displaylang=en](http://www.microsoft.com/downloads/details.aspx?FamilyId=F2D49F68-9E36-414B-906B-13C7C075E1B1&displaylang=en))
- “Configuring ISA Server 2000 to Support Outlook 2003 RPC over HTTP—Part 1: Preparing the Infrastructure and Configuring the Front-End Exchange Server” ([www.msexchange.org/articles/rpchttppart1.html](http://www.msexchange.org/articles/rpchttppart1.html))
- RFC 2595, “Using TLS with IMAP, POP3 and ACAP” ([www.ietf.org/rfc/rfc2595.txt](http://www.ietf.org/rfc/rfc2595.txt))
- RFC 2633, “S/MIME Version 3 Message Specification” ([www.ietf.org/rfc/rfc2633.txt](http://www.ietf.org/rfc/rfc2633.txt))
- RFC 3207, “SMTP Service Extension for Secure SMTP over Transport Layer Security” ([www.ietf.org/rfc/rfc3207.txt](http://www.ietf.org/rfc/rfc3207.txt))
- Knowledge Base Article 812594: “XADM: Key Management Server Concepts in Exchange 2000”
- Knowledge Base Article 816787: “OL2000: E-Mail Is Sent with 40-Bit Encryption Instead of 128-Bit”
- Knowledge Base Article 823503: “How To: Import and Export Certificates So That You Can Use S/MIME in Outlook Web Access on Multiple Computers”
- Knowledge Base Article 823568: “HOW TO: Configure Exchange Server 2003 OWA to Use S/MIME”



**Note** Microsoft Knowledge Base articles can be found at <http://support.microsoft.com>. Enter the article number in the Search the Knowledge Base text box.

# Chapter 19

# Virtual Private Networking

Virtual private networking allows users to connect to corporate resources from off-site locations, such as a home office or hotel room. This chapter discusses the certificate deployment required to implement client-to-gateway virtual private network (VPN) solutions.



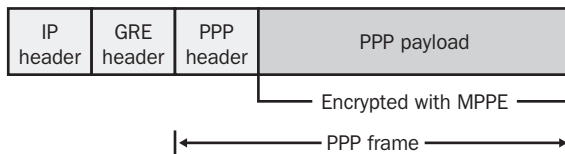
**Note** It is also possible to deploy gateway-to-gateway VPN solutions that join two offices over a public network such as the Internet. The certificates required for these connections are similar to the client-to-gateway scenarios and are not discussed in this chapter. Resources for more information on deploying gateway-to-gateway solutions are listed in the “Additional Information” section of this chapter.

## Certificate Deployment for VPN

When planning certificate deployment for VPN solutions, the main criteria in determining certificate requirements are the tunneling protocol and the user authentication protocol used with the tunneling protocol.

### Point-to-Point Tunneling Protocol (PPTP)

Point-to-Point Tunneling Protocol (PPTP) encapsulates the Point-to-Point Protocol (PPP) datagrams in a modified version of Generic Routing Encapsulation (GRE). (See Figure 19-1.)



**Figure 19-1** PPTP packet structure

In addition to encapsulating the PPP data within a GRE header, PPTP also maintains a TCP connection between the client and the server where the client connects to

TCP port 1723 at the VPN server for management of the tunnel. To protect the data transmitted in the PPTP packets, Microsoft Point-to-Point Encryption (MPPE) is used to encrypt the PPTP data.

PPTP does not require any certificates for the VPN client computer and the VPN server that the VPN client computer connects to. MPPE does not use certificates for the encryption of the data exchanged between the two computers.

## VPN Authentication Options

When a user connects to the network through a VPN connection, the user must provide his credential information to the VPN server to authenticate with the network. The following protocols are available for user authentication when you implement a VPN solution:

- **Password Authentication Protocol (PAP).** Transmits user credentials to the remote access server as plaintext, offering no protection against interception of the user's account and password.
- **Challenge Handshake Authentication Protocol (CHAP).** Provides a stronger form of authentication by sending the password and a challenge to the server after passing the two items through the Message Digest 5 (MD5) hashing algorithm. When the authentication server receives the authentication attempt, the authentication server retrieves the user's password from Active Directory, and then performs the same MD5 hash against the challenge and password. If the results match, the user is authenticated. The use of the server's challenge protects the authentication attempt against replay attacks.

**Warning** CHAP authentication requires that the user's password be stored in a reversibly encrypted format in Active Directory. This weakens password security and requires stronger physical security of the domain controller.

- **Microsoft Challenge Handshake Authentication Protocol (MS-CHAP).** MS-CHAP differs from CHAP in that it creates the challenge response by passing the challenge and the user's password through the Message Digest v4 (MD4) hashing algorithm. MS-CHAP then uses MPPE to encrypt all data transmitted between the remote access client and the remote access server. MS-CHAP does not require the user's password to be stored in reversible encryption in Active Directory.

- **Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2).** Requires the authentication of both the remote access client and the remote access server for a successful authentication attempt. In addition, MS-CHAPv2 implements stronger data encryption keys and uses different encryption keys for sending data than the encryption keys used for receiving data.
- **Extensible Authentication Protocol (EAP).** Provides extensions to PPP connection authentication. These extensions allow advanced authentication methods, such as two-factor authentication. EAP uses Transport Layer Security (TLS) to secure the authentication process. EAP provides mutual authentication, encryption-method negotiation, and secured key exchange between the remote access server and the remote access client.

Although a VPN connection can use any of the authentication protocols listed here, it is recommended to only use MS-CHAPv2 or EAP/TLS authentication when allowing VPN connectivity to your network. Only these authentication methods provide strong protection of the credentials and mutual authentication of both the remote client and the authentication server.

PPTP only requires certificates if EAP/TLS authentication is enforced for VPN connections. When EAP/TLS authentication is required, two certificates are required:

- **User certificate.** Used at the VPN server to authenticate the user account. The certificate must:
  - Be issued by a CA whose certificate is included in the NTAAuth object in Active Directory.
  - Be issued by a CA that chains to a root CA certificate trusted by both the VPN client computers and the authenticating server.
  - Include the Client Authentication Enhanced Key Usage (EKU) object identifier (OID).
  - Pass all certificate validity checks including a revocation check.
  - Include the User Principal Name (UPN) of the user in the subject alternative name extension or be explicitly mapped to a user account in Active Directory.

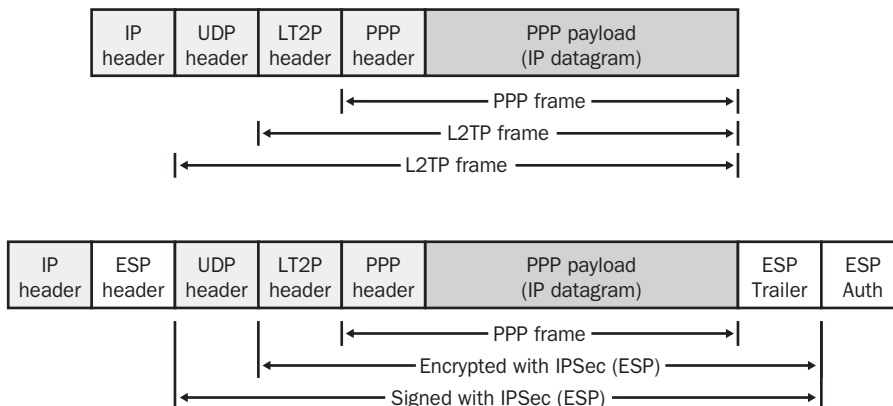


**Note** Optionally, a custom application policy OID can be added to the user certificate to indicate that the certificate is used for the organization's VPN solution. By including the custom application policy OID, an organization can implement a remote access policy profile that requires the custom application policy OID in the presented certificate.

- **Authenticating server certificate.** Used at the authenticating server. If the VPN server implements Windows authentication, the computer certificate must be installed at the VPN server. If the VPN server implements Remote Authentication Dial-In User Service (RADIUS) authentication, the computer certificate must be installed at the RADIUS server. The certificate must:
  - Be issued by a CA that chains to a root CA certificate trusted by both the VPN client computers and the authenticating server.
  - Include the Server Authentication application policy OID.

## Layer Two Tunneling Protocol (L2TP) with IP Security

Layer Two Tunneling Protocol (L2TP) combines the strengths of PPTP and Cisco's Layer Two Forwarding (L2F). When using L2TP, the original PPP data is encapsulated in an L2TP header, and then the combined PPP data and L2TP header is encapsulated in a User Datagram Protocol (UDP) header connecting to UDP port 1701 at both the client and the server. (See Figure 19-2.)



**Figure 19-2** L2TP packet structure

L2TP does not have a built-in encryption mechanism like PPTP. To provide encryption for L2TP communications, Internet Protocol Security (IPSec) with Encapsulating Security Payload (ESP) is used. As shown in Figure 19-2, IPSec provides both signing and encryption protection to the encapsulated L2TP data.





**More Info** The specifics of how L2TP uses IPSec to protect L2TP data are described in RFC 3193, “Securing L2TP Using IPSec” referenced in the “Additional Information” section at the end of this chapter. The combination of L2TP and IPSec is known as L2TP/IPSec.

When you implement L2TP/IPSec for a VPN solution, you require a minimum of two certificates for IPSec endpoint authentication:

- **VPN Server certificate.** Used at the VPN computer to provide authentication for the IPSec security association established between the VPN server and the VPN client computer. The certificate must:
  - Be issued by a CA that chains to the same trusted root as the certificate issued to the client computer.
  - Include the VPN server’s Domain Name System (DNS) name in the certificate’s subject or subject alternative name.
  - Optionally include the IP Security IKE Intermediate application policy OID. If the IP Security IKE Intermediate application policy OID is not included, then the certificate *must* include the Client Authentication application policy OID.
- **Client Computer certificate.** Used at the VPN computer to provide authentication for the IPSec security association established between the VPN server and the VPN client computer. The certificate must:
  - Be issued by a CA that chains to the same trusted root as the certificate issued to the client computer.
  - Include the IP Security IKE Intermediate policy OID.
  - Include the client computer’s DNS name in the certificate’s subject or subject alternative name.



**Note** Only Windows 2000, Windows XP, and Windows Server 2003 include native L2TP/IPSec VPN capabilities. Windows 98, Windows ME, and Windows NT 4.0 Professional clients must install the Microsoft L2TP/IPSec VPN Client for Windows 98, Windows Millennium Edition, and Windows NT 4.0 Workstation. Resources for more information on this add-on client are listed in the “Additional Information” section of this chapter.



**Caution** It is possible to deploy L2TP/IPSec without using VPN server and client computer certificates. Microsoft Knowledge Base Articles 324258 and 281555, titled “HOW TO: Configure a Preshared Key for Use with Layer 2 Tunneling Protocol Connections in Windows XP” and “HOW TO: Configure a Preshared Key for Use with Layer 2 Tunneling Protocol Connections in Windows Server 2003,” respectively, describe how to deploy L2TP/IPSec without certificates. Although it is possible to use a shared secret for IPSec, deployment in this manner is not recommended. When deploying a client to VPN server solution, the compromise of a single client computer would require changing the shared secret pass phrase at every client computer connecting to the network and at every VPN server.

You also require certificates for the authenticating server and the VPN user if you implement EAP/TLS authentication. The same authentication certificates are required for L2TP/IPSec as for PPTP.

## Certificate Template Design

The number of certificate templates that you design for VPN access will depend on the tunneling protocol and authentication protocols used in your solution. The sections that follow detail the certificate template requirements for each component of the VPN solution.

### User Authentication

The user authentication certificate must include the Client Authentication OID in the EKU. For the VPN user authentication, you implement either a private key and certificate stored in the user’s profile or a certificate stored on a smart card.

If you choose to deploy a certificate on a smart card certificate for VPN authentication, consider duplicating the version 1 Smart Card Login certificate template. Make the following modifications to the new version 2 certificate template:

- Modify the certificate template to use the specific smart card cryptographic service provider (CSP) required by your organization’s smart cards.
- Add a custom application policy to the certificate template named *Organization* VPN User. When you define the application policy, ensure that you assign the application policy an OID from your organization’s assigned OID arc.



**Note** You can increase the VPN connection's security by requiring that the user certificate include the *Organization* VPN User application policy OID, in addition to the required Client Authentication OID. This prevents users from using other certificates that have the Client Authentication application policy OID and restricting VPN access to the custom certificate.

- Assign Read, Enroll, and Autoenroll permissions to a custom universal or global group that contains all user accounts that will connect to the network through a VPN. This allows autoenrollment to automate distribution of certificates to users.

If users have Windows 2000 computers, they can still enroll the certificate by using the Certificate Services Web Enrollment pages or a custom enrollment script.

If you choose to deploy a user authentication certificate in the user's profile, consider duplicating the Authenticated Session certificate template. Make the following modifications to the new version 2 certificate template:

- Assign Read, Enroll, and Autoenroll permissions to a custom universal or global group that contains all user accounts that will connect to the network through a VPN. This allows autoenrollment to automate distribution of certificates to users. If users have Windows 2000 computers, they can still enroll the certificate by using the Certificate Services Web Enrollment pages or a custom enrollment script.
- Optionally, add a custom application policy to the certificate template named *Organization* VPN User. When you define the application policy, ensure that you assign it an OID from your organization's assigned OID arc.

## Server Authentication

For server authentication, it is recommended to deploy the default RAS and IAS Server certificate template. This certificate template implements the required Server Authentication application policy OID and is intended for deployment at remote access and RADIUS servers.



**Note** Remember that the decision of where to deploy the RAS and IAS Server certificate depends on the authentication method implemented at the VPN server. If you implement Windows authentication, the RAS and IAS Server certificate must be issued to the VPN Server. If you implement RADIUS authentication, then the RAS and IAS Server certificate must be issued to the RADIUS server.

The default RAS and IAS Server certificate template is recommended for RADIUS servers. This certificate template implements the required Server Authentication application policy OID and is intended for deployment at remote access and RADIUS servers.

The only modification required for the RAS and IAS Server certificate template is to assign the RAS and IAS Servers domain local group Read, Enroll, and Autoenroll permissions. If multiple domains exist in the forest, you must create a custom global group in each and assign each domain's custom global group Read, Enroll, and Autoenroll permissions.



**Note** You must also ensure that all RADIUS server computer accounts are added to the RAS and IAS Servers global group.

## IPSec Endpoint Authentication

For IPSec endpoint authentication, the certificate template that you deploy depends on whether the computer is a member of the forest. If it is a member of the forest, you can use the IPSec certificate template. This certificate template can be deployed using Automatic Certificate Request Settings in group policy to all domain member computers, including domain controllers.

Because the subject information for a computer certificate is based on the computer account information stored in Active Directory, this certificate template cannot be deployed to nonforest members. If a computer is a member of another forest, or is a member of a workgroup, you can deploy the IPSec (offline request) certificate template. The only difference between the IPSec and the IPSec (offline request) certificate templates is that the IPSec (offline request) certificate template allows the certificate requestor to provide the subject information in the certificate request. This allows a VPN user to provide the DNS name of their home computer in the certificate request.

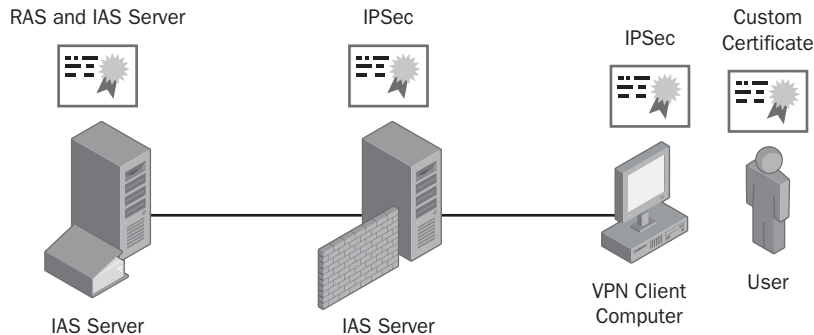
The permissions of the IPsec (offline request) certificate template must be modified to allow a custom universal or global group the Read and Enroll permissions. The custom group must contain all VPN user accounts. The only way to deploy the certificate to non-domain-joined machines is through the Certificate Services Web Enrollment pages or through custom scripting solutions.



**Important** If the home computer does not have access to the corporate network without the IPsec (offline request) certificate being installed, the user might have to request the certificate from an office computer, export the certificate and private key to a floppy disk, and install the certificate and private key at the home computer. The export file must contain the entire certificate chain.

## Deploying a VPN Solution

The procedure for deploying a VPN solution documented in the following sections is based on the network architecture shown in Figure 19-3.



**Figure 19-3** VPN certificate deployment

This network architecture assumes that the VPN client will connect to the network with an L2TP/IPsec tunnel and use EAP/TLS for user authentication. This requires that the following certificates be deployed before you start the actual network configuration:

- RADIUS server: A RAS and IAS Server certificate
- VPN Server: An IPsec certificate
- VPN Client Computer: An IPsec or an IPsec (offline request) certificate
- User: A custom version 2 certificate template with the Client Authentication and the *Organization* VPN User application policy OIDs

## IAS Server Configuration

The Internet Authentication Service (IAS) provides RADIUS services. To implement the strongest form of security, the Windows Server 2003 IAS service should be used. The Windows Server 2003 IAS allows inspection of the presented user certificate for a specific EKU or certificate policy OID.



**Note** The ability to designate required application policy OIDs is not available on the Windows 2000 Server IAS solution.

The configuration of IAS is composed of four steps:

- Install IAS
- Define RADIUS clients
- Define the VPN Access Policy
- Enable Logging at the IAS Server



**Note** Deploying IAS on a domain controller, rather than on a member server, is recommended because it ensures that all communications between IAS and the domain controller are local procedure calls and not communications transmitted over the network.

### Install Internet Authentication Service (IAS)

To install IAS on the Windows Server 2003 server, use the following procedure:

1. Log on as a member of the local Administrators group.
2. From the Start menu, point to Control Panel and then click Add or Remove Programs.
3. In the Add or Remove Programs dialog box, click Add/Remove Windows Components.
4. On the Windows Components page, select the words Networking Services, and then click Details.
5. In the Networking Services dialog box, enable Internet Authentication Services, and then click OK.
6. On the Windows Components page, click Next.

7. If prompted, insert the Windows Server 2003, Standard Edition, or Enterprise Edition, compact disc in the CD-ROM drive and choose the i386 folder.
8. On the Completing the Windows Components Wizard page, click Finish.
9. Close the Add or Remove Programs dialog box.

## Define RADIUS clients

To define the RADIUS clients, the VPN server's IP address must be known and added as a RADIUS client at the IAS server.

1. From Administrative Tools, open Internet Authentication Service.
2. In the console tree, right-click RADIUS Clients, and then click New RADIUS Client.
3. On the Name and Address page, in the Friendly Name box, type a descriptor for the VPN server, in the Client address (IP or DNS) box, type the IP address of the VPN Server, and then click Next.
4. On the Additional Information page, enter the following information:
  - Client-Vendor drop-down list: Select RADIUS Standard
  - Shared Secret: A complex password
  - Confirm shared secret: The same complex password



**Warning** Do *not* enable the Request Must Contain the Message Authenticator attribute. It causes the RADIUS authentication message to fail when using IAS as a RADIUS server.

5. Click Finish.



**Note** Repeat this process for every VPN Server that will use the IAS server for RADIUS authentication.

## Define the VPN Access Policy

Once you define the RADIUS clients, you must define the remote access policy for VPN Access. This remote access policy will allow smart card users to authenticate with the network.

The following process creates and configures the remote access policy:

1. Ensure that you are in the Internet Authentication Service console.
2. In the console tree, select Remote Access Policies.
3. In the details pane, delete any default remote access policies.
4. In the console tree, right-click Remote Access Policies, and then click New Remote Access Policy.
5. In the New Remote Access Policy Wizard, click Next.
6. On the Policy Configuration Method page, click Use the Wizard to Set Up a Typical Policy for a Common Scenario, name the policy VPN Authentication, and then click Next.
7. On the Access Method page, click VPN, and then click Next.
8. On the User or Group Access page, click Group, and then click Add.
9. In the Select Groups dialog box, type **Domain\Domain Users**, and then click OK.
10. On the User or Group Access page, click Next.
11. On the Authentication methods page, select only the Extensible Authentication Protocol (EAP) check box, select Smart Card or Other Certificate from the Type drop-down list, and then click Configure.
12. In the Smart Card or other Certificate Properties dialog box, select the RAS and IAS Server certificate issued to the IAS server, and then click OK.



**Note** The RAS and IAS Server certificate allows the VPN client to authenticate the IAS server during the VPN authentication process.

13. On the Authentication Methods page, click Next.
14. On the Policy Encryption Level page, only select the Strongest Encryption (IPSec Triple DES or MPPE 128-bit) check box, and then click Next.
15. On the Completing the New Remote Access Policy Wizard page, click Finish.
16. In the details pane, double-click VPN Authentication.
17. On the Settings tab, click Add.
18. In the Select Attribute dialog box, select Tunnel-Type, and then click Add.



19. In the Tunnel-Type dialog box, in the Available Types list, select Layer Two Tunneling Protocol (L2TP), click Add, and then click OK.



**Note** If you wish to enable PPTP, you can add Point-to-Point Tunneling Protocol in the Tunnel-Type dialog box.

20. On the Settings tab, click Edit Profile.
21. In the Edit Dial-in Profile dialog box, on the Advanced tab, click Add.
22. In the Add Attribute dialog box, in the Attribute list, select Allowed-Certificate-OID, and then click Add.
23. In the Multivalued Attribute Information dialog box, click Add.
24. In the Attribute Information dialog box, in the Attribute Value box, type **CustomOID** (where *CustomOID* is the custom *Organization* VPN User application policy OID defined by your organization to identify approved VPN users), and then click OK.



**Tip** You can copy the application OID by viewing the object identifiers in the Certificate Templates console (certtmpl.msc).

25. In the Multivalued Attribute Information dialog box, click OK.
26. In the Add Attribute dialog box, click Close.
27. In the Edit Dial-in Profile dialog box, click OK.
28. In the VPN Authentication Properties dialog box, click OK.

### Enable Logging at the IAS Server

The last procedure required in the Internet Authentication Services console is to enable logging for all RADIUS authentication and accounting events. Logging enables you to audit all authentication attempts submitted to the RADIUS server. Use the following procedure:

1. In the console tree, click Remote Access Logging.
2. In the details pane, double-click Local File.

3. In the Settings tab, enable logging for:
  - Accounting requests
  - Authentication requests
  - Periodic Status
4. In the Settings tab, click Apply.
5. In the Local File Properties dialog box, on the Log File tab, enable the following options:
  - Format: IAS
  - Create a new log file: Daily
  - When disk is full delete older log files: Enabled
6. In the Local File Properties dialog box, click OK.
7. Close the Internet Authentication Service dialog box.



**Note** Alternatively, you can configure IAS to log all information into a SQL database. For details on enabling logging to a SQL server database, view the Help files in the Internet Authentication Service console.

## VPN Server Configuration

Once the RADIUS server is installed and configured, you can install the VPN servers. Each VPN server requires installation of the Routing and Remote Access Service. The proposed VPN server configuration will only allow VPN connectivity to the network to provide the highest level of security.

Use the following procedure to install Routing and Remote Access:

1. From the Start menu, click Administrative Tools, and then click Routing and Remote Access.
2. In the console tree, right-click *ComputerName* (local), and then click Configure and Enable Routing and Remote Access.
3. In the Routing and Remote Access Server Setup Wizard, click Next.
4. On the Configuration page, click Remote Access (dial-up or VPN), and then click Next.
5. On the Remote Access page, click VPN, and then click Next.

6. On the VPN Connection page, in the Network Interfaces list, select the network interface connected to the Internet, ensure that the Enable Security on the Selected Interface by Setting Up Static Packet Filters check box is enabled, and then click Next.
7. On the IP Address Assignment page, click Automatically, and then click Next.



**Note** This procedure assumes that a Dynamic Host Configuration Protocol (DHCP) server exists on the private network for the assignment of IP addresses to VPN clients.

8. On the Managing Multiple Remote Access Servers page, click Yes, Set Up this Server to Work with a RADIUS Server, and then click Next.
9. On the RADIUS Server Selection page, provide the following information, and then click Next.
  - Primary RADIUS Server: The *DNSName* or *IP address* of the RADIUS server
  - Alternate RADIUS Server: The *DNSName* or *IP address* of a second RADIUS server
  - Shared secret: The shared secret defined at the RADIUS server for the RADIUS client
10. On the Completing the Routing and Remote Access Server Setup Wizard, click Finish.
11. In the Routing and Remote Access dialog box, click OK to accept that you must configure the DHCP Relay Agent at the VPN server with the IP address of the DHCP server.
12. In the console tree, expand *ComputerName* (local), expand IP Routing, right-click DHCP Relay Agent, and then click Properties.
13. In the DHCP Relay Agent Properties dialog box, in the Server Address box, type the IP address of the DHCP server on the internal network, click Add, and then click OK.



**Note** If there are multiple DHCP servers, add the IP address of each DHCP server in the DHCP Relay Agent Properties dialog box.



**Note** The Routing and Remote Access server uses Windows 2000 Server or Windows Server 2003. The preceding procedure describes the configuration process for Windows Server 2003, and requires minor modification when using Windows 2000 Server.

## Create a VPN Connection Object

Once the back-end infrastructure is established, the user can create a VPN connection object at the client computer. This book will only show how to manually create the VPN connection object, although it is highly recommended to use the Connection Manager Administration Kit (CMAK) that is included with Windows Server 2003.

The Connection Manager is a custom dialer that integrates with Windows operating systems from Windows 98 and later. The Connection Manager can be configured to manage all aspects of dial-up and VPN connections in a corporate environment, reducing the configuration required at the VPN client computers.



**More Info** For details on creating CMAK packages, see the “Step-by-Step Guide for Creating and Testing Connection Manager Profiles in a Test Lab” white paper referenced in the “Additional Information” section of this chapter.

### Creating a Connection Object in Windows 2000

To create a connection object in Windows 2000, you must define a new dial-up and network connection:

1. From the Start menu, point to Settings, point to Network and Dial-up Connections, and then click Make New Connection.
2. In the Network Connection Wizard, click Next.
3. On the Network Connection Type page, click Connect to a Private Network Through the Internet, and then click Next.
4. On the Destination Address page, in the Host name or IP address box, type the DNS name or IP address of the VPN Server’s external interface, and then click Next.
5. On the Connection Availability page, click For all users, and then click Next.



**Note** By defining the connection object for all users, the network connection can be used when initialing logging on to the computer from the Windows Security dialog box. Only connection objects assigned to anyone are available when no user is logged on at the computer. You must be a member of the local Administrators group to create a connection object for anyone's use.

6. On the Completing the Network Connection Wizard page, type a name for the connection object, click Add a Shortcut to My Desktop, and then click Finish.
7. In the Connect Virtual Private Network Connection dialog box, click Properties.
8. In the Virtual Private Connection dialog box, on the Options tab, select Include Windows Logon Domain if you are using MS-CHAPv2 authentication.
9. In the Virtual Private Connection dialog box, on the Security tab in the Validate My Identity as Follows drop-down list:
  - Select Use Smart Card for Smart Card-Based Authentication.



**Warning** You must have a smart card reader and associated CSP installed to use the smart card option.

- Select Advanced (custom settings) if you are using certificate-based authentication with a certificate in the user's local store. You must also define that the certificate is a certificate on the computer rather than on the smart card.
- Select Require Secured Password for MS-CHAP or MS-CHAPv2 authentication.



**Note** You must define Advanced (custom settings) to restrict authentication to MS-CHAPv2.

10. In the Virtual Private Connection dialog box, on the Networking tab, in the Type of VPN Server I Am Calling drop-down list, select:
  - Automatic: First attempt L2TP/IPSec, and then attempt PPTP.
  - Point to Point Tunneling Protocol (PPTP). Only use PPTP.
  - Layer-2 Tunneling Protocol (L2TP). Only use L2TP/IPsec.



**Tip** Only use Automatic if your network supports both L2TP/IPSec and PPTP VPNs. You will establish a faster connection to the network if you specifically choose PPTP or L2TP/IPSec if your network only supports one of the VPN protocols.

11. In the Virtual Private Connection dialog box, click OK.

## Creating a Connection Object in Windows XP

To create a connection object in Windows XP, you must define the new VPN connection object in the Network Connections window.

1. From the Start menu, point to Control Panel, right-click Network Connections, and then click Open.
2. In the Network Connections window, click Create a New Connection.
3. In the New Connection Wizard, click Next.
4. On the Network Connection Type page, click Connect to the Network at My Workplace, and then click Next.
5. On the Network Connection page, click Virtual Private Network Connection, and then click Next.
6. On the Connection Name page, in the Company Name box, type the name of your company, and then click Next.
7. On the Public Network page, click Do Not Dial the Initial Connection if you are on a network attached to the Internet or click Automatically Dial this Initial Connection if you dial an initial Internet connection such as a dial-up connection, and then click Next.
8. On the VPN Server Selection page, type the DNS name or IP address of the VPN Server's external interface, and then click Next.
9. On the Smart Card page, click Use My Smart Card if you are using a smart card for authentication, otherwise click Do Not Use My Smart Card, and then click Next.

10. On the Connection Availability page, click Anyone's Use, and then click Next.
11. On the Completing the New Connection Wizard page, click Add a Shortcut to This Connection to my Desktop, and then click Finish.

## Connecting to the VPN

Once you have created the VPN connection object, you can then connect to the network using the VPN connection. The user interface presented to the user will depend on whether you are using EAP/TLS authentication or MS-CHAPv2 authentication. If you are using a smart card for authentication, you must type the personal identification number (PIN) for the smart card to authenticate. If you are using MS-CHAPv2 authentication, you must type your user account, password, and domain to connect to the network.

## Best Practices

- **Allow only MS-CHAPv2 or EAP/TLS authentication for remote access clients.** Only MS-CHAPv2 and EAP/TLS allow mutual authentication between VPN client and authentication server. In addition, MS-CHAPv2 and EAP/TLS provide the strongest protection for a user's credential information.
- **Allow only strong encryption for remote access clients.** Ensure that the remote access policy enforces the strongest form of encryption to ensure that connections use 128 bit MPPE for PPTP connections and 3DES for L2TP/IPSec connections for encryption.
- **Create separate remote access policies for VPN access.** Do not try and create an all-in-one remote access policy for VPN and dial-up connections. Create separate remote access policies for each application, and ensure that the policy conditions do not overlap.



**Important** If the policy conditions overlap, you must order the remote access policies so that the desired policy is applied to the correct users. For example, if you have one remote access policy applied to Domain Admins and another applied to Domain Users, you must place the remote access policy applied to Domain Admins higher in the remote access policy listing. This ensures that an administrator, who is a member of both Domain Admins and Domain Users, has the Domain Admins policy applied to his or her connection.

- **Deploy IPsec certificates to all VPN servers and clients.** Create a version 2 certificate template based on the IPsec certificate template to enable autoenrollment of the certificates to Windows XP and Windows Server 2003 computers. For Windows 2000 computers, you can use scripted enrollment or the Web enrollment pages by deploying the IPsec (offline request) certificate template.
- **Implement RADIUS for all remote access authentication and accounting.** RADIUS allows centralized administration of all remote access policy and collection of VPN connection activity logs. Also, configure both primary and secondary RADIUS servers for all VPN devices so that VPN connectivity still succeeds if a single RADIUS server fails.
- **Deploy RAS and IAS Server certificates to all RADIUS servers.** If you use Windows Server 2003 IAS servers, you can deploy the RAS and IAS Server certificates by using autoenrollment. This server certificate is required for EAP/TLS mutual authentication.
- **Do not use preshared keys for IPsec authentication, only use certificate-based authentication.** Although it is possible to configure L2TP/IPsec to use preshared keys for authentication, the risks are high. If a single laptop is compromised, an attacker could gain access to the preshared key, and use the preshared key from other computers to connect to the corporate network.
- **Use smart cards for user certificate-based authentication to provide the strongest protection of user credentials.** A smart card provides additional security by applying two-factor protection. An attacker must gain access to both the smart card and the PIN to access the network.
- **Implement a custom application policy OID in the user authentication certificates and require the existence of the application policy OID in the remote access policy.** The implementation of a custom application policy OID increases security by requiring the authentication certificate to contain the application policy OID. Use of a custom application policy OID limits authentication only to the designated certificate.
- **Use the CMAK to create Connection Manager profiles.** A Connection Manager profile ensures that the correct settings are created and defined for all remote access clients. In addition, the Connection Manager profile can be distributed to Windows 98, Windows ME, Windows NT 4.0, Windows 2000, Windows XP, and Windows Server 2003 client computers.

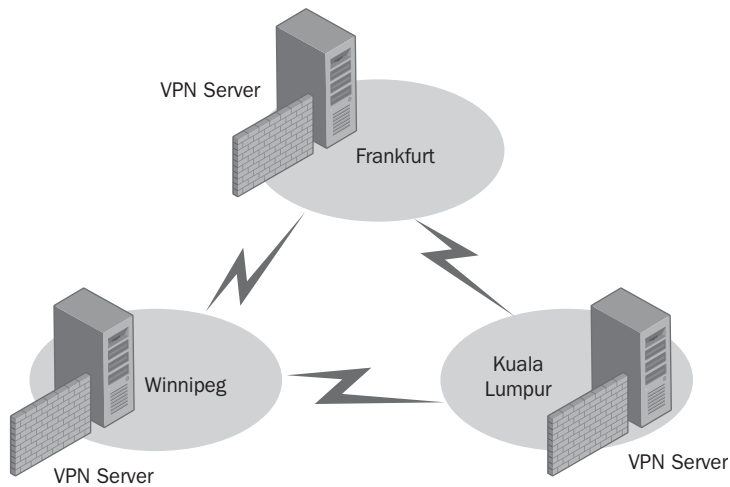
## Case Study: Lucerne Publishing

You are the network manager for Lucerne Publishing. Lucerne Publishing has several acquisition editors who work remotely from their home offices and require access to resources on the corporate network.



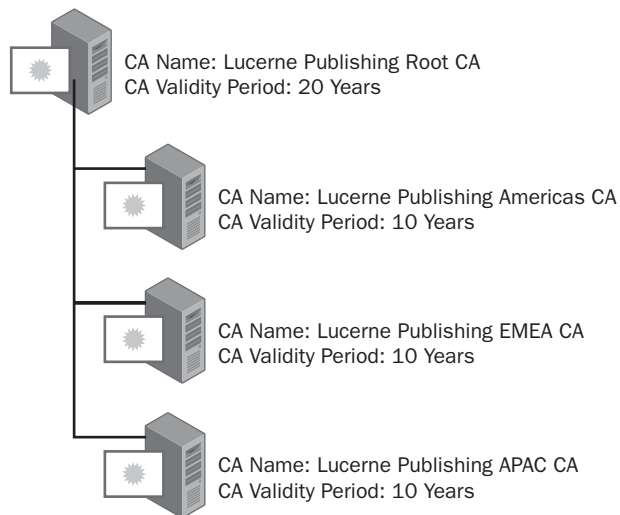
## Scenario

To allow VPN access, you propose implementing a VPN server, running Windows Server 2003, Enterprise Edition, at each of the major offices, as shown in Figure 19-4.



**Figure 19-4** VPN Server Placement for Lucerne Publishing

To facilitate the issuance of certificates, Lucerne Publishing has implemented a two-tier CA hierarchy, as shown in Figure 19-5.



**Figure 19-5** The Lucerne Publishing CA hierarchy

The following design requirements have been identified for VPN deployment:

- The VPN servers are configured with two network interfaces, one attached to the corporate network and one attached to the Internet, allowing connections to the VPN server. The VPN servers are configured so that the servers will only accept L2TP/IPSec connections from the VPN clients. Any attempts to communicate with the VPN servers with protocols other than L2TP/IPSec will fail.
- Lucerne Publishing employees will use a mix of Windows 98, Windows 2000, and Windows XP computers when they connect to the corporate network.
- Lucerne Publishing plans to use L2TP/IPSec for all VPN communications between the remote employees and the corporate network.
- In addition, all authentication initially will be performed by the users typing their user account and password. In the future, Lucerne Publishing plans to change the authentication to require smart cards.
- All connections between the VPN clients and the VPN servers must enforce mutual authentication.
- To prevent access to the network if a virus attack occurs, management wants the ability to immediately shut down all VPN access to the network at any given time.
- Many of the acquisition editors' computers are not members of the forest. Methods must be developed to provide certificates for the VPN connection to these editors.

## Case Study Questions

1. What authentication protocol must be enforced for VPN communications to meet the initial authentication requirements?
2. What certificates are required for the initial VPN solution? Provide your answers in the following table.

Principal	Certificate
VPN User	
VPN Client Computer	
RADIUS Server	
VPN Server	

3. What authentication protocol must be enforced for VPN communications to meet the modified authentication requirements to enforce smart card authentication?

4. What certificates are required for the modified VPN solution that uses smart cards? Provide your answers in the following table.

Principal	Certificate
VPN User	
VPN Client Computer	
RADIUS Server	
VPN Server	

5. How can Lucerne Publishing implement the ability to immediately shut down all VPN access?
6. What certificate template(s) are required for the L2TP/IPSec tunnel? What CA should you publish the certificates at?
7. What method could you use to deploy the IPSec certificates to forest member computers?
8. What method could you use to deploy the IPSec certificates to nonforest member computers?
9. When Lucerne Publishing switches to using Smart Card certificates, how can the Smart Card certificate template be modified to further restrict VPN access to the network?
10. What certificate(s) would you deploy at the VPN server when using RADIUS authentication?
11. What application would you use to configure the client computers to ensure that the VPN client software is correctly configured?
12. What additional VPN software is required for some of the home computers?

## Additional Information

- “Deploying Virtual Private Networks with Microsoft Windows Server 2003” ([www.microsoft.com/mspress/books/5519.asp](http://www.microsoft.com/mspress/books/5519.asp))
- “Virtual Private Networking with Windows Server 2003: Overview” ([www.microsoft.com/windowsserver2003/techinfo/overview/vpnover.mspx](http://www.microsoft.com/windowsserver2003/techinfo/overview/vpnover.mspx))
- “Virtual Private Networking with Windows Server 2003: Deploying Remote Access VPNs” ([www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/deploy/confeat/vpndeplr.asp](http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/deploy/confeat/vpndeplr.asp))

- “Virtual Private Networking with Windows Server 2003: Deploying Site-to-Site VPNs” ([www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/deploy/confeat/vpndpls2.asp](http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/deploy/confeat/vpndpls2.asp))
- “Microsoft’s Virtual Private Networks for Windows Server 2003 Web Portal” ([www.microsoft.com/windowsserver2003/technologies/networking/vpn/default.aspx](http://www.microsoft.com/windowsserver2003/technologies/networking/vpn/default.aspx))
- “Virtual Private Networking with Windows Server 2003: An Example Deployment” ([www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/deploy/confeat/vpnexamp.asp](http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/deploy/confeat/vpnexamp.asp))
- “Step-by-Step Guide for Setting Up VPN-based Remote Access in a Test Lab” ([www.microsoft.com/technet/prodtechnol/windowsserver2003/deploy/confeat/rmotevpn.asp?frame=true](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/deploy/confeat/rmotevpn.asp?frame=true))
- “Step-by-Step Guide for Creating and Testing Connection Manager Profiles in a Test Lab” ([www.microsoft.com/downloads/details.aspx?FamilyID=93fd20e7-e73a-43f6-96ec-7bcc7527709b&DisplayLang=en](http://www.microsoft.com/downloads/details.aspx?FamilyID=93fd20e7-e73a-43f6-96ec-7bcc7527709b&DisplayLang=en))
- “Microsoft L2TP/IPSec VPN Client for Windows 98, Windows Millennium Edition, and Windows NT 4.0 Workstation” ([www.microsoft.com/windows2000/server/evaluation/news/bulletins/l2tpclient.asp](http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/l2tpclient.asp))
- “Microsoft Internet Authentication Services Web Portal” ([www.microsoft.com/windowsserver2003/technologies/ias/default.aspx](http://www.microsoft.com/windowsserver2003/technologies/ias/default.aspx))
- RFC 2637: “Point-to-Point Tunneling Protocol (PPTP)” ([www.ietf.org/rfc/rfc2637.txt](http://www.ietf.org/rfc/rfc2637.txt))
- RFC 2661: “Layer Two Tunneling Protocol “L2TP”” ([www.ietf.org/rfc/rfc2661.txt](http://www.ietf.org/rfc/rfc2661.txt))
- RFC 3193: “Securing L2TP Using IPsec” ([www.ietf.org/rfc/rfc3193.txt](http://www.ietf.org/rfc/rfc3193.txt))
- Knowledge Base Article 248711: “Mutual Authentication Methods Supported for L2TP/IPSec”
- Knowledge Base Article 248750: “Description of the IPsec Policy Created for L2TP/IPSec”
- Knowledge Base Article 254442: “Windows 2000 L2TP/IPSec Interoperation with Third-Party Manufacturers”
- Knowledge Base Article 255784: “Increasing Security on Windows 2000 VPN Server”
- Knowledge Base Article 259335: “Basic L2TP/IPSec Troubleshooting in Windows 2000”
- Knowledge Base Article 314831: “Basic L2TP/IPSec Troubleshooting in Windows XP”

- Knowledge Base Article 281555: “HOW TO: Configure a Preshared Key for Use with Layer Two Tunneling Protocol Connections in Windows XP”
- Knowledge Base Article 324258: “HOW TO: Configure a Preshared Key for Use with Layer 2 Tunneling Protocol Connections in Windows Server 2003”
- Knowledge Base Article 324915: “Description of the Microsoft L2TP/IPSec Virtual Private Networking”
- Knowledge Base Article 325032: “Using the Microsoft L2TP/IPSec VPN Client with Windows 98, Windows Millennium Edition, and Windows NT 4.0”
- Knowledge Base Article 816573: “HOW TO: Configure a VPN Server to Act as a Router in Windows Server 2003”



**Note** Microsoft Knowledge Base articles can be found at <http://support.microsoft.com>. Enter the article number in the Search the Knowledge Base text box.



## Chapter 20

# Wireless Networking

Many organizations are investigating wireless networking. Wireless networking allows users to easily move around the office or between desks or meeting rooms while still maintaining network connectivity.

Although wireless networking makes it easy for employees to connect to the corporate network, it also provides an access for an attacker to connect to the network if proper security is not implemented.

This chapter will look at how a public key infrastructure (PKI) can increase your wireless network's security by requiring certificate-based authentication for access.

## Threats Introduced by Wireless Networking

When an organization implements a wireless network, several threats are introduced that do not exist in a wired environment, including:

- **Accidental connections to the wireless network.** People might not realize that their computers automatically connect to the organization's wireless network. This can make the computers a target for attackers when they are connected to the network without appropriate security measures, such as the Internet Connection Firewall or a host-based intrusion detection system. These visiting computers can be used as launch points to attack the network.



**Note** The default behavior for Microsoft Windows XP is to connect automatically to any available wireless network that is detected.

- **Inspection of data.** As data is sent from the computer over the wireless network, it might be possible for user credentials or other confidential data to be viewed by an unauthorized person connected to the wireless network.
- **Data modification.** If attackers can gain access to the wireless network, it might be possible for them to implement a man-in-the-middle attack where legitimate packets are intercepted and modified as they are transmitted from

source to destination. Likewise, false packets can be transmitted from attackers who impersonate valid users.

- **Rogue Wireless Access Points (WAPs).** Windows XP's default behavior is to automatically connect to any detectable wireless network. Users can easily connect a WAP to the network and start using the WAP to connect to the corporate network, and the rogue WAP can prevent users from connecting to an authorized WAP.
- **Unauthorized network connections.** With a wireless network, an attacker can gain access to the network without entering the physical premises. You cannot stop the transmission of packets beyond the walls of your building. The distance the transmissions reach depends on the strength of the WAPs you deploy.

## Protecting for Wireless Communications

When you implement a wireless network, you must develop a plan for securing the network to reduce the likelihood of threats. Some of the more common methods of protecting a wireless network are mentioned in the sections that follow.

### MAC Filtering

One of the most basic ways of protecting a wireless network is to implement media access control (MAC) filtering. At the WAP, you can configure which MAC addresses (the low-level firmware address of a wireless card) are allowed to connect to the WAP. Although this sounds like an ideal, easy way to secure a wireless network, consider the following issues:

- **It is easy to spoof an approved MAC address.** Software, such as SMAC, allows you to manually modify your wireless card's MAC to an approved MAC address.



**Note** You can learn more information about SMAC at [www.klccconsulting.net/smac/default.htm?v=readme11](http://www.klccconsulting.net/smac/default.htm?v=readme11).

- **MAC filtering is hard to manage.** If you have several wireless computers, each MAC address must be managed manually at the WAP.
- **MAC filtering authenticates only the computer, not the user.** If attackers steal a laptop or use a laptop included in the approved MAC listing, they can access the network.
- **The size of the approved MAC list is limited.** In large environments, you might not be able to input all approved MAC addresses.



## Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) is one method of providing encryption services to wireless networking. When a wireless connection enables WEP, the wireless network interface card (NIC) encrypts each data packet transmitted on the network using the RC4 stream cipher algorithm. The WAP then decrypts the data packets on receipt.



**Warning** Wireless encryption only encrypts data between the wireless client and the WAP. Once the data is on the wired network, no encryption is applied, unless the wireless client applies other encryption technologies, such as virtual private networking or Internet Protocol Security (IPSec).

WEP requires that both the wireless client and WAP share a 40-bit or a 64-bit symmetric encryption key. When WEP is implemented alone, the wireless client and WAP must configure the encryption key manually. If 802.1x authentication (as described later in this chapter) is implemented, the encryption key is configured only at the WAP and securely transmitted to the wireless client.



**Note** Some hardware vendors also provide support for a 128-bit WEP key.

The symmetric encryption key is concatenated to a randomly generated 24-bit initialization vector (IV). The IV lengthens the lifetime of the symmetric key due to the random generation of the IV. A new IV is used for each frame transmitted between the wireless client and the WAP.

The problem with WEP is that a brute force attack can be executed successfully in a short period of time. The weakness in WEP's implementation is two-fold.

- **The symmetric encryption key is rarely changed.** Once an organization inputs a WEP key, it typically does not change. This is especially true if both the wireless client and the WAP must input the key manually.
- **The IV is only 24 bits and is re-used over time.** When WEP is deployed on a large network, an IV is re-used about every hour. An application such as AirSnort can capture frames over a period of time and determine what the WEP key is based on by identifying frames that use the same IV.



**Note** For a detailed analysis of WEP weaknesses, see the article, “Security of the WEP Algorithm,” referenced in the “Additional Information” section of this chapter.

## Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) is an encryption method produced by the Wi-Fi Alliance to address the security issues found in WEP. The following major enhancements are included in WPA:

- **Increased data encryption.** WPA implements Temporal Key Integrity Protocol (TKIP), which uses a per-packet key mixing function; a message integrity check (MIC), known as *Michael*; and an extended IV with rules on sequencing. In addition, WPA implements a re-keying mechanism so that the same key is not used for long periods of time.
- **Dependency on 802.1x authentication.** The use of 802.1x authentication is optional for WEP encryption only. WPA requires 802.1x authentication to ensure that only authorized users or computers are allowed connectivity to the wireless network. 802.1x authentication also ensures mutual authentication so that a wireless client does not connect to a rogue network, rather than the corporate network.



**Note** A future proposal for wireless security is the IEEE 802.11i security specification. The current WPA definition includes forward compatibility with the new 802.11i security specification. 802.11i adds secure fast handoffs, secure de-authentication, and secure disassociation with WAPs. 802.11i also implements strong forms of authentication from the Advanced Encryption Standard (AES).

## 802.1x Authentication Types

A Microsoft Windows Server 2003 PKI provides the necessary certificates for 802.1x authentication for wireless and wired networks. When a user or computer performs 802.1x authentication, the following two authentication types are available:

- Extensible Authentication Protocol with Transport Layer Security (EAP/TLS)
- Protected Extensible Authentication Protocol (PEAP).



**Note** There are several WLAN security solutions similar to PEAP and EAP/TLS. For example, Cisco's Light EAP (LEAP) and Funk Software's Tunneled Transport Layer Security (EAP-TTLS) provide security comparable to PEAP or EAP/TLS, but they lock your organization into vendor-specific solutions.

## EAP/TLS Authentication

EAP/TLS is a certificate-based authentication method that provides mutual authentication between the user or computer and the Remote Authentication Dial-In User Service (RADIUS) server when implemented for a wireless networking solution. To implement EAP/TLS authentication, the following certificates are required:

- **Client Computer or User.** The client end of the wireless connection must have a certificate with the Client Authentication EKU object identifier (OID). This certificate proves the identity of the client computer or the user account.
- **Server.** The server end of the wireless connection must have a certificate with the Server Authentication EKU OID. This certificate proves the RADIUS server's identity to all connecting wireless clients.



**Note** No certificate is required for the WAP when implementing 802.1x authentication. The role of the WAP is to translate EAP messages sent from the client to the WAP into RADIUS messages sent from the WAP to the RADIUS server, and vice versa.

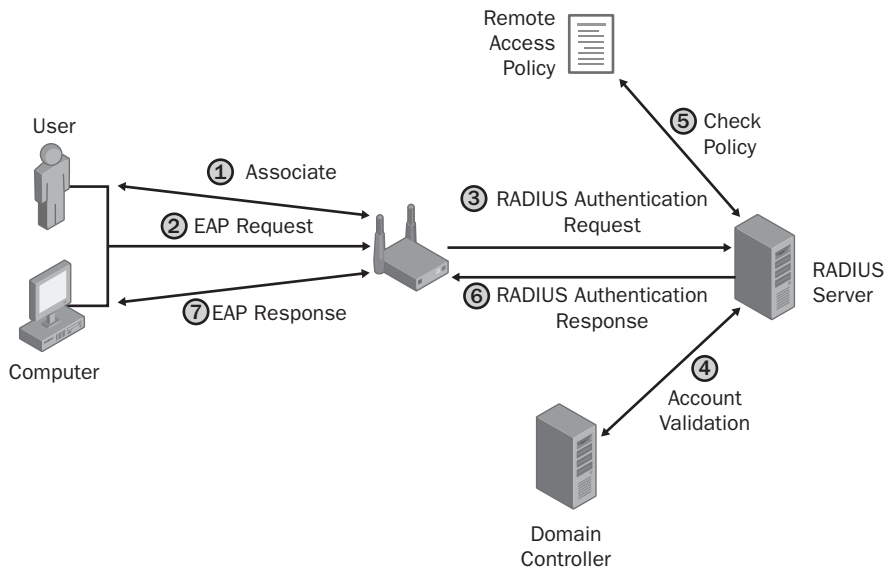
## PEAP Authentication

PEAP authentication allows the transmission of other EAP types within a TLS-secured channel. When PEAP is used, the user must type in a user account and a password that is sent to the RADIUS server. The user's identity is proven through knowledge of a user account and password, which are protected by using Microsoft Challenge Authentication Protocol version 2 (MS-CHAPv2). The RADIUS server still requires a certificate with the Server Authentication EKU OID to prove its identity and to protect the user's password as it is transmitted to the server, but no certificate is required for the user.

## How 802.1x Authentication Works

802.1x authentication allows an organization to require users and computers to authenticate with the network before they are allowed full network access. The process

includes enforcing mutual authentication of the client computer or user account with a RADIUS server. The process takes place when a wireless client attempts to connect to a wireless network requiring 802.1x authentication. (See Figure 20-1.)



**Figure 20-1** The 802.1x authentication process

1. The computer attempts to associate with the WAP, which responds that the user or computer must provide EAP authentication.
2. The computer or user passes its credentials to the WAP.
  - If using EAP/TLS authentication, a signed request is submitted to the WAP, proving that the user or computer has access to the private key associated with the Client Authentication certificate.
  - If using PEAP authentication, users must type their user account and password combination in an authentication dialog box.
3. The WAP translates EAP authentication packets into RADIUS authentication packets and forwards the authentication packets to the RADIUS server.



**Note** The WAP is simply an intermediary for the authentication process, translating EAP request messages into RADIUS request messages and RADIUS response messages into EAP response messages.

4. The RADIUS server contacts a domain controller to either validate the user account and the password combination or use the User Principal Name (UPN) in the certificate's Subject Alternative Name to map the certificate to a user account in Active Directory.
5. The RADIUS server determines whether the identified user or computer is granted access to the network based on the RADIUS server's configured remote access policies.
6. The RADIUS server sends a RADIUS authentication success or failure message to the WAP.
7. The WAP sends an EAP success or failure message to the wireless client.

If the client is authorized, the user or computer exchanges encryption keys with the WAP. The encryption keys are used by the client and the WAP, allowing the client internal network connectivity. If the client is not authorized, then no network connectivity is allowed.

## Planning Certificates for 802.1x Authentication

To use 802.1x authentication, you must deploy to the RADIUS server, at minimum, a certificate with the Server Authentication EKU OID. If you are implementing EAP/TLS authentication, you also must deploy a computer certificate or a user certificate, or both.

### Computer Certificates for RADIUS Servers

For RADIUS servers, it is recommended to deploy the default RAS and IAS Server certificate template. This certificate template implements the required Server Authentication EKU OID and is intended for deployment at remote access and RADIUS servers.

The only modification required for the RAS and IAS Server certificate template is to assign the RAS and IAS Servers domain local group Read, Enroll, and Autoenroll permissions. If multiple domains exist in the forest, you must create a custom global group in each domain and assign each domain's custom global group Read, Enroll, and Autoenroll permissions.



**Note** You also must ensure that all RADIUS server computer accounts are added to the RAS and IAS Servers global group.

## User Certificates for Clients

If EAP/TLS authentication is implemented, a user must provide a certificate for authentication. To enhance the wireless network's security, you should implement a custom version 2 certificate template based on the User Signature certificate template.

Only two modifications are recommended for the custom certificate template:

- **Add a custom application policy to the certificate template named *Organization Wireless User*.** When you define the application policy, ensure that you assign the application policy an OID from your organization's assigned OID arc.



**Note** You can increase the wireless connection's security by requiring that the user certificate include the *Organization Wireless User* application policy OID, in addition to the required Client Authentication OID. This prevents users from using other certificates that have the Client Authentication application policy OID and restricts access to the custom certificate.

- **Assign Read, Enroll, and Autoenroll permissions to a custom universal or global group that contains all user accounts that connect to the wireless network.** This allows autoenrollment to automate distribution of certificates to users. If users have Windows 2000 computers, they can still enroll the certificate by using the Certificates MMC or the Certificate Services Web Enrollment pages.

## Computer Certificates for Clients

If a computer account is a member of the forest, installing a computer certificate allows the computer to connect to the network before a user logs on to the computer. This enables application of the following:

- Computer Group Policy Objects (GPOs)
- User GPOs
- Logon scripts configured within a user-assigned GPO

If the computer is not issued a certificate, users log on to the computer with cached credentials. Only after the logon process is complete do users gain access to their Client Authentication certificates, permitting them to connect to the corporate network.

The Workstation Authentication or Computer certificate template can be used to provide the client computer a certificate with the Client Authentication application policy OID. A universal or global group containing the computer account must be assigned Read, Enroll, and Autoenroll permissions for the Workstation Authentication certificate or Read and Enroll permissions for the Computer certificate.

## Deploying Certificates to Users and Computers

The sections that follow provide recommendations for deploying the necessary certificates for 802.1x authentication for wireless networks.

### RADIUS Server

When implementing 802.1x authentication, it is recommended that you use Windows Server 2003 IAS as the RADIUS server. The implementation of a Windows Server 2003 computer allows you to restrict certificate-based authentication to certificates with a designated OID in the certificate, such as a custom application policy OID.

To enable autoenrollment of the RAS and IAS Server certificates:

- Ensure that the RADIUS server's computer account has membership in a group assigned Read, Enroll, and Autoenroll permissions for the RAS and IAS Servers certificate template.
- Ensure that the RAS and IAS Server certificate template does not require user input for autoenrollment.
- Ensure that the RAS and IAS Server certificate template is available for enrollment on one or more Windows Server 2003, Enterprise Edition, enterprise certification authorities (CAs).
- Ensure that the RADIUS server's computer account is in an organizational unit (OU) where the Autoenrollment Settings Group Policy setting for computers is applied.



**Note** Alternatively, a user assigned Read and Enroll permissions who is a member of the local Administrators group at the RADIUS server can manually enroll a RAS and IAS Server certificate.

## Client Computers

Client computers only require a certificate for 802.1x authentication if the computer is a member of the forest. If not, a computer certificate does not associate with any computer account in Active Directory.

The method used to deploy the computer certificate depends on whether you are deploying the Computer version 1 certificate template or the Workstation Authentication version 2 certificate template.

If you are deploying to Windows 2000 computers, you can deploy the Computer version 1 certificate template by adding the Computer certificate template to the Automatic Certificate Request Settings Group Policy setting. The GPO with the Automatic Certificate Request Settings defined must be linked to the OU where the computer account exists.

If you are deploying to Windows XP or later computers, you can deploy the Workstation Authentication version 2 certificate template by using Autoenrollment Settings. As with the RADIUS certificate template, the computer account must belong to a group assigned Read, Enroll, and Autoenroll permissions; the Workstation Authentication certificate template must allow autoenrollment without user input; and the GPO enabling Autoenrollment Settings for computers must be linked to the OU where the computer account exists.

## Users

To connect to a wireless network, a user must acquire a certificate based on the custom version 2 certificate template discussed earlier in this chapter. To minimize the risks involved with deploying certificates, it is recommended to use autoenrollment for Windows XP computers and scripted enrollment for Windows 2000 computers.

To enable certificate autoenrollment for the user certificate template for Windows XP and Windows Server 2003 computers, you must do the following:

1. Modify the permissions of the custom certificate template to assign Read, Enroll, and Autoenroll permissions to a global or universal group containing all wireless users.
2. Modify the custom certificate template to not require user input during the enrollment process. By not requiring user input, certificates are issued to the user invisibly.
3. Ensure that the custom version 2 certificate template is available at one or more enterprise CAs for enrollment.
4. Enable the Autoenrollment Settings Group Policy setting at the OU or domain containing all wireless user accounts.



To enable scripted enrollment, you can use the `enroll.vbs` script discussed in Chapter 12. The `enroll.vbs` script can be used in a logon script to allow automated certificate enrollment for users with Windows 2000 computers.

Assuming that you have implemented an *Organization* wireless User application policy OID in the Wireless User certificate template, and that the OID assigned is 1.3.6.1.4.1.311.509.4.2.1, you can use the following code in your logon script to enroll the Wireless User certificate:

```
cscript enroll.vbs /certtype wirelessuser /keyl 1024 /csp enhanced /
app_policy 1.3.6.1.5.5.7.3.2 /app_policy 1.3.6.1.4.1.311.509.4.2.1 /fn
"Wireless User"
```

This command enrolls the certificate template named `wirelessuser` with a key length of 1,024 bits using the Microsoft Enhanced Cryptographic Service Provider v1.0. In addition, the certificate is only requested if the user does not have an existing certificate with the Client Authentication (1.3.6.1.5.5.7.3.2) and *Organization* Wireless User (1.3.6.1.4.1.311.509.4.2.1) application policy OIDs. Finally, the certificate is assigned the friendly name of Wireless User when placed in the user's certificate store.



**Note** Alternatively, you can use manual enrollment for the Wireless User certificate template. A user with a Windows XP or Windows Server 2003 computer can use the Certificates MMC console or the Certificate Services Web Enrollment pages. A user with a Windows 2000 computer can only use the Certificate Services Web Enrollment pages.

## Implementing 802.1x Authentication

To implement 802.1x authentication, you must configure the RADIUS server and the WAP to implement RADIUS.

### Configuring the RADIUS Server

In a Microsoft network, IAS provides RADIUS capabilities on the network. To deploy IAS for wireless networking, you must do the following:

- Install IAS.
- Add the IAS server to the RAS and IAS Servers (global) group.
- Define the RADIUS clients.
- Create a Wireless Computer remote access policy.
- Create a Wireless User remote access policy.

## Install IAS

IAS is Microsoft's implementation of a RADIUS server. To install IAS on the Windows Server 2003 server, use the following procedure:

1. Log on as a member of the local Administrators group.
2. From the Start menu, point to Control Panel and click Add or Remove Programs.
3. In the Add or Remove Programs dialog box, click Add/Remove Windows Components.
4. On the Windows Components page, select the words Networking Services and click Details.
5. In the Networking Services dialog box, enable Internet Authentication Services and click OK.
6. On the Windows Components page, click Next.
7. If prompted, insert the Windows Server 2003, Standard Edition or Enterprise Edition, compact disc in the CD-ROM drive and choose the i386 folder.
8. On the Completing the Windows Components Wizard page, click Finish.
9. Close the Add or Remove Programs dialog box.

## Add the IAS Server to the RAS and IAS Servers Group

Once you have installed IAS, you must add the IAS server's computer account to the RAS and IAS Servers group in the computer account's domain.

1. Ensure you are logged on as a member of the Domain Admins group.
2. From Administrative Tools, open Active Directory Users and Computers.
3. Ensure that you are connected to the domain where the IAS server's computer account exists.
4. In the console tree, expand the domain, and click Users.
5. In the details pane, double-click the RAS and IAS Servers group.
6. In the RAS and IAS Servers Properties dialog box, on the Members tab, click Add.
7. In the Select Users, Contacts, Computers, or Groups dialog box, click Object Types.
8. In the Object Types dialog box, ensure that the Computers check box is Enabled and click OK.
9. In the Select Users, Contacts, Computers, or Groups dialog box, in the Enter the Object Names to Select box, type ***ComputerName*** (where *ComputerName* is the NetBIOS name of the computer hosting IAS), and then click Check Names.

10. Ensure that the correct computer name appears and click OK.
11. In the RAS and IAS Servers Properties dialog box, click OK.
12. Close Active Directory Users and Computers.
13. Reboot the computer hosting the IAS service to use the new group membership.

## Define RADIUS Clients

Each WAP that forwards authentication requests to the RADIUS server must be added as the WAP's known clients list. The WAP's IP address, as well as a RADIUS secret or password, must be defined.

The following procedure defines a RADIUS client at the IAS server:

1. From Administrative Tools, open Internet Authentication Service.
2. In the console tree, right-click RADIUS Clients and click New RADIUS Client.
3. On the Name and Address page, in the Friendly Name box, type a descriptor for the WAP. In the Client Address box, type the IP address of the WAP and click Next.
4. On the Additional Information page, enter the following information:
  - Client-Vendor drop-down list: Select the *vendor of the WAP*.



**Tip** If the hardware vendor is not available in the listing, choose the standard RADIUS option.

- Shared Secret: A password that identifies the valid WAP.
- Confirm shared secret: Retype the password for verification.



**Warning** Do *not* enable the Request Must Contain the Message Authenticator attribute.

5. Click Finish.
6. Repeat this process for every WAP that uses the IAS server for 802.1x authentication.



**Note** Microsoft's IAS server does not support use of the "Any" designation. Each WAP must be manually defined as a RADIUS client at the IAS server.

## Define a Wireless Computer Remote Access Policy

Once you designate all RADIUS clients, you must define a remote access policy for computer accounts. This remote access policy allows wireless computers to connect initially for log on and GPO download.

Use the following process to create and configure a remote access policy for computer authentication:

1. From Administrative Tools, open Internet Authentication Service.
2. In the console tree, select Remote Access Policies.
3. In the details pane, delete any default remote access policies.



**Warning** If the IAS server is used for VPN authentication or other applications that support RADIUS authentication, do not delete any default remote access policies.

4. In the console tree, select Remote Access Policies and click New Remote Access Policy.
5. In the New Remote Access Policy Wizard, click Next.
6. On the Policy Configuration Method page, click Use the Wizard to Set Up a Typical Policy for a Common Scenario, name the policy Wireless Computers, and click Next.
7. On the Access Method page, click Wireless and click Next.
8. On the User or Group Access page, click Group and click Add.
9. In the Select Groups dialog box, type **Domain\Domain Computers** and click OK.
10. Repeat steps 8 and 9 for each domain in your forest allowed to connect to the wireless network.
11. On the User or Group Access page, click Next.
12. On the Authentication Methods page, select Smart Card or Other Certificate and click Configure.

13. In the Smart Card or Other Certificate Properties dialog box, select the Certificate Issued to *DNSName* (where *DNSName* is the Domain Name System [DNS] name of the IAS server) and click OK.
14. On the Authentication Methods page, click Next.
15. On the Completing the New Remote Access Policy Wizard page, click Finish.
16. In the details pane, double-click Wireless Computers.
17. On the Settings tab, select the NAS-Port-Type policy condition and click Edit.
18. In the NAS-Port-Type dialog box, in the Selected Types list, select Wireless – Other, click Remove, and click OK.
19. On the Settings tab, click Edit Profile.
20. In the Edit Dial-in Profile dialog box, on the Encryption tab, clear all encryption types except Strongest Encryption (MPPE 128 Bit).
21. In the Edit Dial-in Profile dialog box, click OK.
22. In the Wireless Computers Properties dialog box, click OK.
23. Close the Internet Authentication Service dialog box.

### Define the Wireless User Remote Access Policy

When enabling 802.1x authentication, you must configure a separate WAP for wireless users. Although similar, the main difference in the two policies is that the user remote access policy requires the custom *Organization* Wireless User OID in the user's certificate.

The following process creates and configures the user remote access policy:

1. From Administrative Tools, open Internet Authentication Service.
2. In the console tree, select Remote Access Policies.
3. In the console tree, right-click Remote Access Policies and click New Remote Access Policy.
4. In the New Remote Access Policy Wizard, click Next.
5. On the Policy Configuration Method page, click Use the Wizard to Set Up a Typical Policy for a Common Scenario, name the policy Wireless Users, and click Next.
6. On the Access Method page, click Wireless and click Next.
7. On the User or Group Access page, click Group and click Add.
8. In the Select Groups dialog box, type **Domain\Domain Users** and click OK.



**Note** Alternatively, you can create a custom group and only allow wireless access to members of the custom group.

9. On the User or Group Access page, click Next.
10. On the Authentication Methods page, select Smart Card or Other Certificate and click Configure.
11. In the Smart Card or Other Certificate Properties dialog box, select the Certificate Issued to *DNSName* (where *DNSName* is the DNS name of the IAS server), and click OK.
12. On the Authentication Methods page, click Next.
13. On the Completing the New Remote Access Policy Wizard page, click Finish.
14. In the details pane, double-click Wireless Users.
15. On the Settings tab, select the NAS-Port-Type policy condition and click Edit.
16. In the NAS-Port-Type dialog box, in the Selected Types list, select Wireless – Other, click Remove, and click OK.
17. On the Settings tab, click Edit Profile.
18. In the Edit Dial-in Profile dialog box, on the Encryption tab, clear *all* encryption types except Strongest Encryption (MPPE 128 Bit).
19. In the Edit Dial-in Profile dialog box, on the Advanced tab, click Add.
20. In the Add Attribute dialog box, in the Attribute list, select Allowed-Certificate–OID and click Add
21. In the Multivalued Attribute Information dialog box, click Add.
22. In the Attribute Information dialog box, in the Attribute value box, type **OID** (where *OID* is the OID assigned to the *Organization* Wireless User application policy), and click OK.



**Tip** You can also copy this OID by viewing the OIDs in the Certificate Templates console (certtmpl.msc).

23. In the Multivalued Attribute Information dialog box, click OK.
24. In the Add Attribute dialog box, click Close.
25. In the Edit Dial-in Profile dialog box, click OK.
26. In the Wireless Users Properties dialog box, click OK.

## Configuring the Wireless Access Point

WAP configuration is dependent on the installed Internetwork Operating System (IOS). Rather than provide the details for a single vendor, ensure that you define the following settings at your WAP:

1. Configure the WAP to implement RADIUS authentication.
  - Add the IP address of the IAS server for RADIUS authentication.
  - Input the RADIUS secret for the IAS server.
  - Define the RADIUS listening port used by the IAS server (UDP port 1812).
2. Configure the WAP to implement RADIUS accounting.
  - Add the IP address of the IAS server for RADIUS accounting.
  - Input the RADIUS secret for the IAS server.
  - Define the RADIUS listening port used by the IAS server (UDP port 1813).



**Important** The WAP must support RADIUS authentication. If the WAP does not support RADIUS authentication, you cannot implement 802.1x authentication for your network when using that WAP.

## Connecting to the Wireless Network

Once the infrastructure installation is complete, the wireless clients can connect to the wireless network using 802.1x authentication. The following procedure is required to connect:

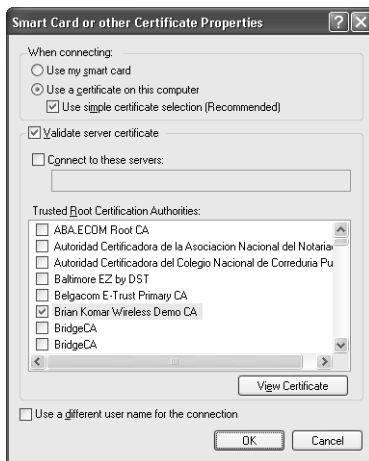
1. Open the Network Connections window.
2. Right-click your wireless adapter and click Properties.
3. In the Properties of the wireless adapter dialog box, on the Wireless Networks tab, in the Preferred Networks section, choose the Service Set Identifier (SSID) of the wireless network, and click Properties.
4. In the *SSID* Properties dialog box, on the Association tab, define the following settings.

Option	WEP	WPA
Network Authentication	Open	WPA or WPA-PSK
Data Encryption	WEP	TKIP or AES
The Key Is Provided for Me Automatically	Enabled	Enabled

- In the *SSID* Properties dialog box, on the Authentication tab, define the following settings.

Option	WEP	WPA
Enable 802.1x authentication for the network	Enabled	Enabled
EAP type	Smart Card or other Certificate	Smart Card or other Certificate
Authenticate as computer when computer information is available	Enabled if computer is a member of the forest	Enabled if computer is a member of the forest

- In the *SSID* Properties dialog box, on the Authentication tab, click Properties.
- In the Smart Card or other Certificate Properties dialog box (shown in Figure 20-2), enable the following options:



**Figure 20-2** Defining certificate settings for EAP/TLS authentication

- **Use my smart card.** Enable if using a smart card certificate.
- **Use a certificate on this computer.** Enable if using a certificate stored in the user's certificate store.



**Warning** Do not enable simple certificate selection if the computer is from a different forest or workgroup. By not enabling simple certificate selection, the user can choose the certificate for manual authentication.



- **Use simple certificate selection (recommended).** Enable if the certificate's subject is the same as the user's logon name.
- **Validate server certificate.** Enable this option to require mutual authentication. The client validates the RADIUS server's certificate and ensures that it chains to the root CA certificate designated in the Trusted Root Certification Authorities store in the local client machines.
- **Use a different user name for the connection.** Enable this option only if the computer is not a member of the forest. This allows the user to choose a certificate that does not contain his or her current user name.

## Using Group Policy to Enforce Client Configuration

Group Policy can be used to ensure that wireless networking settings are configured correctly for EAP/TLS authentication (for 802.1x authentication).

The GPO is applied to computer accounts and should be linked to either the domain or the OU where wireless computer accounts are located. A wireless network policy allows an organization to do the following:

- Enforce 802.1x authentication.
- Restrict wireless connectivity to WAPs, not allowing ad hoc connections.

**Note** An *ad hoc wireless network* is configured directly between two wireless clients, rather than clients connecting to a WAP connected to the corporate network.

- Enable Windows to configure wireless network settings automatically.
- Provide preferred network SSIDs and prevent connections to non-preferred networks.
- Enforce the use of WEP or WPA encryption.
- Define what form of EAP authentication is required: PEAP or EAP/TLS.
- Define whether computer authentication, user authentication, or a combination of both is required for connectivity to the wireless network.
- Enforce mutual authentication by validating the RADIUS server's certificate.

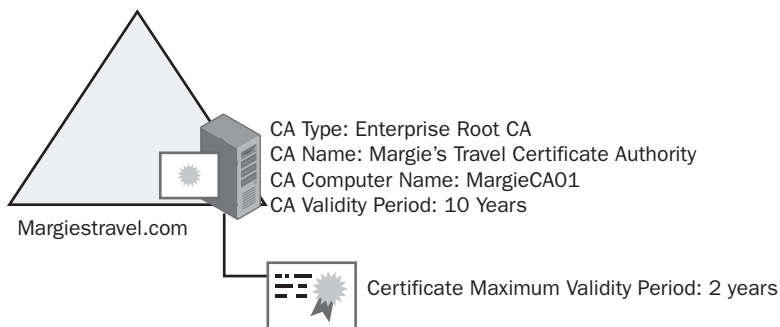


## Best Practices

- **Implement the strongest form of wireless encryption available on your WAPs.** Any form of encryption is better than no encryption. If your WAP does not support WPA, it is still better to enable WEP than to have no encryption at all, even though WEP has known weaknesses. If you do implement WEP, ensure that you regularly modify the WEP key to protect against attacks.
- **Only implement WAPs that support 802.1x authentication.** 802.1x authentication decreases some of the weaknesses associated with WEP encryption. 802.1x ensures that only authenticated clients (computers and users) can connect to the wireless network and provides automated distribution of the encryption keys.
- **Implement PEAP or EAP/TLS for authenticating all wireless clients.** Both authentication methods provide strong protection of the user's credentials. In addition, EAP/TLS and PEAP ensure that the computer or a user performs mutual authentication with a RADIUS server when connecting to the wireless network.
- **Deploy certificates using autoenrollment or scripted enrollment for domain members.** Automating the deployment of certificates ensures that all users and computers obtain the necessary certificates for wireless networking. Automated deployment reduces the chance of user error during the enrollment process.
- **Use Group Policy to define Wireless Networking settings.** Group policy can ensure that Windows XP computers are correctly configured when connecting to a wireless network. Group Policy eliminates user error when configuring the wireless networking connection.

## Case Study: Margie's Travel

You manage the network for Margie's Travel, a travel agency in Seattle. The network implements a single enterprise root CA for its PKI, as shown in Figure 20-3.

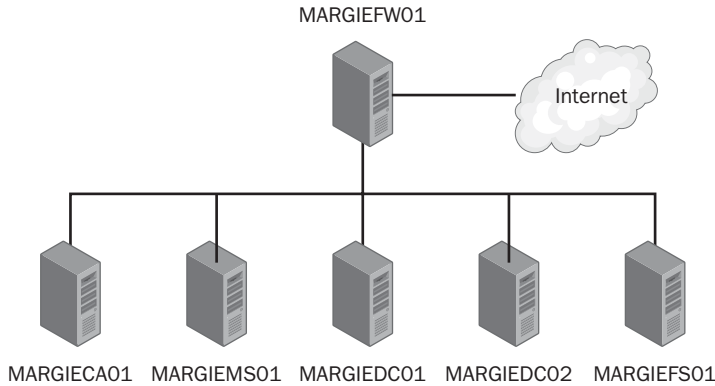


**Figure 20-3** The Margie's Travel CA hierarchy

## Scenario

Margie's Travel has changed locations each year as the business has expanded. Due to the high costs involved in rewiring the new office each time Margie's Travel changes locations, you are considering implementing wireless networking to reduce the costs associated with pulling twisted-pair cables to each desk in the office.

The servers shown in Figure 20-4 are currently deployed on the network.



**Figure 20-4** Server deployment for Margie's Travel

You have gathered the following requirements for implementing wireless networking:

- Six servers provide the network infrastructure for the Margie's Travel network. All servers are members of the margiestravel.com domain. The six servers are:
  - **MARGIEW01.** The Microsoft Internet Security and Acceleration (ISA) Server providing firewall and proxy services.
  - **MARGIEMS01.** The Microsoft Exchange 2000 server for the network providing e-mail services for the network.
  - **MARGIECA01.** The enterprise root CA for the network providing certificates to all users and computers on the network.
  - **MARGIEDC01.** The first domain controller for the margiestravel.com domain. This domain controller also provides DNS and Dynamic Host Configuration Protocol (DHCP) services for the network.
  - **MARGIEDC02.** The second domain controller for the margiestravel.com domain. This domain controller provides DNS services for the network.
  - **MARGIEFS01.** The file server for the network. All customer records and accounting information is stored on this server. In addition, Internet Information Services (IIS) is installed on the server and hosts the corporate intranet Web site.

- The file server on the network contains confidential client information, such as credit card numbers and passport numbers. Unauthorized access to the networks must be prevented to protect access to this confidential information. Only company-owned computers must be allowed to connect to the network.
- Several of the travel agents have laptop computers, but other agents work only at the office and use desktop computers to connect to the network.
- All client computers and notebooks run Windows XP with the latest service packs. All computers and notebooks are members of the margiestravel.com domain.
- All desktops and computers have wireless cards that support 802.11g. The latest updates are installed for all wireless cards.
- All servers are stored in a server room at the back of the office. The servers have 100 megabits per second (Mbps) Ethernet cards.
- The size of the current location requires at least three wireless access points to provide sufficient coverage for all areas of the office.

## Case Study Questions

1. What network infrastructure service required for wireless network is missing from the Margie's Travel network? On which server(s) would you install the missing service?
2. When you purchase the wireless access points for the networks, what features are required to meet the design requirements?
3. What certificate(s) are required on the wireless access points?
4. What certificate(s) are required at each desktop or notebook computer?
5. What certificate(s) are required for each user of the network?
6. What other certificate(s) are required for the wireless network deployment?
7. How many remote access policies are required for the wireless deployment?
8. What additional measures can be taken to ensure that only Margie's Travel users can connect to the wireless network?
9. How can you ensure that the each desktop and notebook computer is correctly configured for connectivity to the wireless network?

## Additional Information

- “Deploying Secure 802.11 Wireless Networks with Microsoft Windows” ([www.microsoft.com/mspress/books/6749.asp](http://www.microsoft.com/mspress/books/6749.asp))
- “802.11 WEP: Concepts and Vulnerability” ([www.wi-fiplanet.com/tutorials/article.php/1368661](http://www.wi-fiplanet.com/tutorials/article.php/1368661))
- “Configuring Wireless Settings Using Windows Server 2003 Group Policy” ([www.microsoft.com/technet/community/columns/cableguy/cg0703.mspix](http://www.microsoft.com/technet/community/columns/cableguy/cg0703.mspix))
- “Designing and Deploying Wireless LAN Connectivity for the Microsoft Corporate Network” ([www.microsoft.com/technet/prodtechnol/winxppro/depoy/wlandply.mspix](http://www.microsoft.com/technet/prodtechnol/winxppro/depoy/wlandply.mspix))
- “Enterprise Deployment of Secure 802.11 Networks Using Microsoft Windows” ([www.microsoft.com/technet/prodtechnol/winxppro/depoy/ed80211.mspix](http://www.microsoft.com/technet/prodtechnol/winxppro/depoy/ed80211.mspix))
- “Enterprise Deployment of Secure Wired Networks Using Microsoft Windows” ([www.microsoft.com/downloads/details.aspx?FamilyID=05951071-6b20-4cef-9939-47c397ffd3dd&displaylang=en](http://www.microsoft.com/downloads/details.aspx?FamilyID=05951071-6b20-4cef-9939-47c397ffd3dd&displaylang=en))
- “Enterprise Solutions for Wireless LAN Security” ([www.wi-fi.org/OpenSection/pdf/Whitepaper\\_Wi-Fi\\_Enterprise2-6-03.pdf](http://www.wi-fi.org/OpenSection/pdf/Whitepaper_Wi-Fi_Enterprise2-6-03.pdf))
- “Microsoft 802.1x Authentication Client for Windows 2000” ([www.microsoft.com/windows2000/server/evaluation/news/bulletins/8021xclient.asp](http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/8021xclient.asp))
- “Securing Wireless LANs—A Windows Server 2003 Certificate Services Solution” ([www.microsoft.com/technet/security/prodtech/win2003/pkiwire/swlan.mspix](http://www.microsoft.com/technet/security/prodtech/win2003/pkiwire/swlan.mspix))
- “Obtaining and Installing a VeriSign WLAN Server Certificate for PEAP-MS-CHAP v2 Wireless Authentication” (<http://download.microsoft.com/download/9/f/d/9fd73f17-2fdf-4409-b2d2-31437c7f29f3/WLANCertEnroll.doc>)
- “Security of the WEP Algorithm” ([www.isaac.cs.berkeley.edu/isaac/wep-faq.html](http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html))
- “Step-by-Step Guide for Setting Up Secure Wireless Access in a Test Lab” ([www.microsoft.com/downloads/details.aspx?FamilyID=0f7fa9a2-e113-415b-b2a9-b6a3d64c48f5&DisplayLang=en](http://www.microsoft.com/downloads/details.aspx?FamilyID=0f7fa9a2-e113-415b-b2a9-b6a3d64c48f5&DisplayLang=en))
- “Troubleshooting Windows XP IEEE 802.11 Wireless Access” ([www.microsoft.com/technet/prodtechnol/winxppro/maintain/wifitrbl.mspix](http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wifitrbl.mspix))
- “Wi-Fi Alliance” ([www.weca.net/OpenSection/index.asp](http://www.weca.net/OpenSection/index.asp))

- “Wi-Fi Protected Access” ([www.weca.net/OpenSection/protected\\_access.asp](http://www.weca.net/OpenSection/protected_access.asp))
- “Wi-Fi Protected Access (WPA) Overview” ([www.microsoft.com/technet/community/columns/cableguy/cg0303.msp](http://www.microsoft.com/technet/community/columns/cableguy/cg0303.msp))
- “Windows Server 2003 Deployment Kit: Deploying a Wireless LAN” ([www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/deployguide/dnsbm\\_wir\\_overview.asp?frame=true](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/deployguide/dnsbm_wir_overview.asp?frame=true))
- “Windows XP Wireless Deployment Technology and Component Overview” ([www.microsoft.com/technet/prodtechnol/winxp/pro/maintain/wificomp.msp](http://www.microsoft.com/technet/prodtechnol/winxp/pro/maintain/wificomp.msp))
- “Windows XP Support Patch for Wi-Fi Protected Access” (<http://microsoft.com/downloads/details.aspx?FamilyId=009D8425-CE2B-47A4-ABEC-274845DC9E91&displaylang=en>)
- “SMAC Tool” ([www.klcconsulting.net/smac/default.htm?v=readme11](http://www.klcconsulting.net/smac/default.htm?v=readme11))
- Knowledge Base Article 313664: “Using 802.1x Authentication on Computers Running Windows 2000”
- Knowledge Base Article 318710: “HOW TO: Support Wireless Connections in Windows 2000”
- Knowledge Base Article 815485: “Overview of the WPA Wireless Security Update in Windows XP”
- Knowledge Base Article 816589: “HOW TO: Support Wireless Connections That Use EAP-TLS Authentication in Windows Server 2003”
- Knowledge Base Article 837911: “Windows for Wireless and Wired Networks”



**Note** Microsoft Knowledge Base articles can be found at <http://support.microsoft.com>. Enter the article number in the Search the Knowledge Base text box.

# Chapter 21

## Code Signing

Code signing allows users and computers to trust software published on a public network, such as the Internet. When you connect to the Internet, you can download device drivers for your computer's operating system, ActiveX controls, or Java applets for advanced Web content. The question remains: How do you know the link provides you with the content it suggests and is not a virus or an attack against your computer?

As long as you trust the certificate used to sign the software—including all certificate trust validation described in Chapter 9, "Certificate Validation"—you should feel comfortable installing the software.



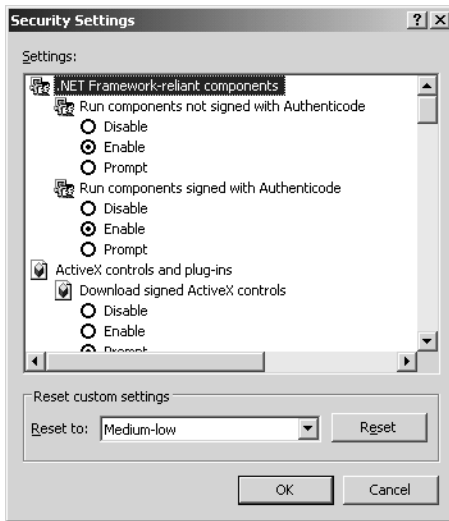
**Note** Microsoft's solution for code signing is known as Authenticode, which applies an industry-standard signature to code developed with Microsoft tools.

### How Code Signing Works

Code signing adds a digital signature to an executable file (.exe), a dynamic link library file (.dll), an Active X control, a cabinet file (.cab), a java archive file (.jar), a Java applet, or a script. The digital signature protects a user who accesses the software in the following two ways:

- The digital signature identifies the publisher of the software, allowing you to make an informed choice whether to allow or prevent software installation.
- The digital signature allows you to determine whether the software has been modified between the time the code was signed and the time you decide to install the software.

Applications that are aware of code signing can be configured to choose how to interact with software that is signed or not signed. For example, in Microsoft Internet Explorer settings, you can define how to interact with ActiveX controls for each security zone. (See Figure 21-1.)



**Figure 21-1** Defining ActiveX and Authenticode settings for an Internet Explorer security zone

You can define how Internet Explorer interacts with potentially dangerous Internet content for each security zone. For each setting, you can choose to enable the content, disable the content, or prompt each time the user interacts with the defined type of content.

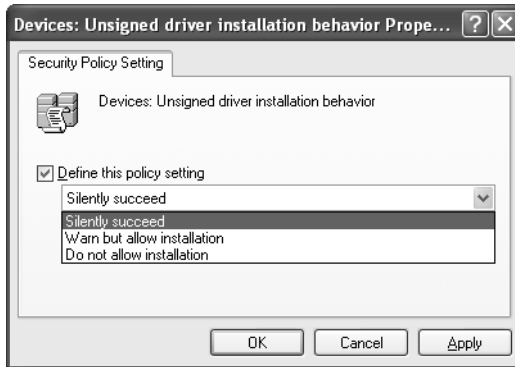


**Warning** Although code signing itself cannot guarantee that signed code is safe to run, it is a mechanism to inform users of who the software publisher is and allow the user to choose to trust (or not trust) the publisher.

In addition to applications, the Microsoft Windows operating system can use code signing to validate device drivers. You can define the following Group Policy setting to set how device driver installation proceeds if a device driver is not signed: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Unsigned driver installation behavior.

This Group Policy setting allows you to define how Windows interacts with an unsigned device driver when attempting to install a device driver. (See Figure 21-2.)





**Figure 21-2** Defining how the operating system interacts with unsigned device drivers

The following options are available in this Group Policy setting:

- **Silently succeed.** Although not recommended, some organizations choose to treat signed and unsigned device drivers equally, allowing automatic installation without user warning.
- **Warn but allow installation.** This option warns users that they are attempting to install an unsigned device driver, but it allows the installation to proceed if they so choose.
- **Do not allow installation.** This option blocks the installation of all unsigned device drivers.

It is recommended to not allow installation unless the device driver is signed. Most reputable hardware vendors provide signed device drivers, allowing you to enforce device driver signing.



**Note** Remember that only local Administrators of a Windows 2000, Windows XP, or Windows Server 2003 computer are allowed to install or update device drivers.

## Certification of Code Signing Certificates

The effectiveness of code signing is only as good as the trust of the certificate used to sign the application. The process used to certify the Code Signing certificate application varies depending on whether the certificate is obtained from a commercial or an internal source.



**Note** Because the Code Signing certificate is so important, you should provide stronger protection of the key by storing the Code Signing certificate and private key on a two-factor device, such as a smart card.

## Commercial Certification

When a Code Signing certificate is obtained from a commercial entity, the type of certificate is referred to as a Software Publishing Certificate (SPC). To enroll this form of certificate, the requestor must meet the following criteria defined by the commercial certificate provider:

- **Identification.** Requestors must submit their names, addresses, and other information that proves their identities to the commercial provider. The identification process can also require a face-to-face interview.
- **The Pledge.** Requestors must assure that they will not distribute software that they know, or should have known, contains viruses or would otherwise harm a user's computer or code. The assurance can be provided in writing or by agreeing to a statement posted on the commercial provider's enrollment Web site.



**Note** Code signing does not ensure that the code won't introduce security risks to an organization. For information and recommendations for writing secure applications, see *Writing Secure Code*, Second Edition (Microsoft Press, 2002), by Michael Howard and David LeBlanc.

- **Dun & Bradstreet Rating.** A requestor's organization must have financial standing in the business community. Typically, this is indicated by a Dun & Bradstreet rating. If an organization does not have a Dun & Bradstreet rating, it must apply for a rating before a Code Signing certificate is issued by the commercial organization.

The different strategies for acquiring a Code Signing certificate are:

- **Acquire a single certificate for the entire organization.** This method ensures that all code signing passes through a central approval mechanism. Some organizations actually test the application in a certification forest before it is signed to ensure that the application causes no damage.

- **Acquire certificate on a divisional basis.** In decentralized organizations, different divisions or departments might have the responsibility of signing the applications that they develop. In this case, the certificate's subject might also include departmental information.
- **Acquire certificates on an individual basis.** In some organizations, every developer is responsible for the code that they develop. By implementing Code Signing certificates for each developer, an organization can determine who created or modified a piece of code and whether the code was changed after the developer signed the code.

In most cases, the certificate's subject is typically the name of the software publisher's organization rather than the individual who requests the certificate. Using the organization name in the subject of the certificate is recommended because the person is signing the application on behalf of the company.



**Note** An only exception occurs when certificates are issued to each individual developer. If each developer has a personal Code Signing certificate, the Subject or Subject Alternative Name should indicate the developer's identity.

## Corporate Certification

If an application is used only within an organization, the organization can choose to issue its own Code Signing certificates. In this case, similar measures should be taken to validate the certificate requestor's identity.

It is recommended to pend the certificate request until a certificate manager validates the requestor's identity. In addition, permissions on the Code Signing certificate template can be restricted to limit which groups are assigned Read and Enroll permissions for the certificate template.

When a Code Signing certificate issued by the corporate CA hierarchy is used, the signature is recognized only by client computers that trust the CA hierarchy's root CA. Typically, this includes only computers that are members of the local forest.



**Note** It is possible to trust the Code Signing certificate of another organization. Possible methods include implementing a common root CA or by using qualified subordination to trust only Code Signing certificates issued by a partner's CA hierarchy.

## Planning Deployment of Code Signing Certificates

The deployment of a Code Signing certificate within an organization involves designing the Code Signing certificate template and planning how to deploy the certificates to the developers who perform the code signing operations.



**Important** If you are signing applications or code that will be used by people outside of your organization, it is recommended that you obtain the Code Signing certificate from a commercial vendor, such as VeriSign. This increases the amount of confidence in your organization, resulting in a larger number of organizations trusting your Code Signing certificate.

### Certificate Template Design

When deploying a Code Signing certificate, you can use the default Code Signing certificate template or develop a custom certificate template, depending on the following considerations:

- Choose the default Code Signing certificate template if your organization allows the Code Signing certificate to exist on the hard disk of the code signer's computer. The default certificate template uses the Microsoft Enhanced Cryptographic Provider v1.0.
- Create a custom version 2 certificate template if you want to deploy the Code Signing certificate on a two-factor device, such as a smart card.
- Create a custom version 2 certificate template if you want to pend Code Signing certificate to validate the requestor's identity before issuance.



**Tip** Consider creating a custom user account in Active Directory that requests the Code Signing certificate. Ensure that the user account's Common Name is the organization's name, rather than the user's. This ensures that the certificate's subject is the name of the organization, which, again, increases trust in the signed application. Alternatively, you can implement a custom certificate template that allows the certificate requestor to provide the subject information, rather than gathering it from Active Directory.

- Create a custom version 2 certificate template if you want to add an entry to the Certificate Policies extension indicating what measures were taken to validate the certificate's subject at certificate enrollment.

- Ensure that the permissions of the certificate template are modified so that only the required users have Read and Enroll permissions for the Code Signing certificate template.

## Planning Enrollment Methods

The enrollment method you choose depends on whether your organization requires CA certificate manager approval for issuance.

- If the Code Signing certificate is protected by a smart card cryptographic service provider (CSP), ensure that the person who obtains the Code Signing certificate is issued a smart card and a smart card reader before the enrollment process commences.
- If the Code Signing certificate can be acquired without certificate manager approval, the certificate can be enrolled using any enrollment method. This includes the Certificate Enrollment Wizard or the Certificate Services Web Enrollment pages.
- If the Code Signing certificate requires certificate manager approval, it is recommended to use the Certificate Services Web Enrollment pages to allow the requestor to view the status of the pending certificate request and complete the enrollment when the certificate is issued by the certificate manager.
- It is not recommended to implement autoenrollment for a Code Signing certificate. Due to the trust put in a code signing signature, the process should be initiated by the requestor.

## Performing Code Signing

The process of performing the code signing can begin once the Code Signing certificate is issued to the requestor.

## Gathering the Required Tools

The Authenticode for Internet Explorer 5.0 kit includes a code signing tool (Signcode.exe) that enables code signing of any application and the following files:

- **Makecert.exe.** Creates a self-signed X.509 certificate for testing purposes only. It is recommended that you issue the Code Signing certificate from an enterprise CA by creating a version 2 certificate template based on the Code Signing certificate template.
- **Cert2spc.exe.** Creates an SPC for testing purposes only. Again, it is recommended to issue the SPC certificate from the internal CA hierarchy, rather than generate a self-signed certificate.

- **SignCode.exe.** Signs and time stamps a file. This is the primary application used when digitally signing application files.
- **ChkTrust.exe.** Checks the validity of the file by authenticating the signature on the file, as well as determining whether the certificate used to sign the application chains to a trusted root CA.
- **MakeCTL.exe.** Creates a certificate trust list (CTL) to allow trust of certificate issued by foreign CA hierarchies.
- **CertMgr.exe.** Manages certificates, CTLs, and certificate revocation lists (CRLs) on the local computer.
- **SetReg.exe.** Sets registry keys controlling certificate verification.
- **Signer.dll.** The helper dynamic link library (DLL) that performs application signing.

The person tasked with code signing for your organization should download the Authenticode for Internet Explorer 5.0 kit ([www.microsoft.com/downloads/details.aspx?FamilyID=2B742795-D0F0-4A66-B27F-22A95FCD3425](http://www.microsoft.com/downloads/details.aspx?FamilyID=2B742795-D0F0-4A66-B27F-22A95FCD3425)) and extract these tools to a folder on the computer where code signing is performed.

## Using Signcode.exe

The following process allows you to sign an application with the Signcode.exe utility:

1. Log on to a computer with the account issued the Code Signing certificate.



**Note** This example assumes that the Code Signing certificate and the associated private key are stored on a Schlumberger smart card. If the Code Signing certificate is stored in the local profile, you must perform the code signing procedure at the same computer where you requested the Code Signing certificate or where you imported the Code Signing certificate and private key.

2. Ensure that you have a copy of the Code Signing certificate on either a USB storage device or on an available network location.
3. Copy the Signcode.exe executable and the application file to sign into a folder on the current workstation.
4. Run Signcode.exe.
5. On the Welcome to the Digital Signature Wizard page, click Next.

6. On the File Selection page, in the File Name box, type the full path to the file that you want to sign and click Next.



**Note** The location of the file does not matter during the signing process. The file can be copied to any location for the code signing process.

7. On the Signing Options page, click Custom and click Next.
8. On the Signature Certificate page, click Select from File.
9. In the Open dialog box, in the Files of Type drop-down list, select X.509 Certificate. In the File Name box, type the location to the Codesign.crt file on the USB storage device or network share and click Open.



**Note** If the certificate is stored in the user's current store, you can use the Select from Store button. This displays the Select Certificate dialog box, only showing a selection of certificates with the Code Signing object identifier (OID) from the user's current store.

10. On the Signature Certificate page, verify the certificate content information to ensure that it is the correct Code Signing certificate and that the intended purpose is Code Signing. Click Next.
11. If the Code Signing certificate is on a smart card or other two-factor device, insert the smart card containing the Code Signing certificate in the smart card reader.
12. On the Private Key page, click Private Key in a CSP, set the CSP drop-down list to Schlumberger Cryptographic Service Provider, and click Next.



**Note** You must choose the same CSP as that used during the enrollment of the Code Signing certificate. For example, if you stored the certificate in the user's profile, you would use the Microsoft Enhanced Cryptographic Provider v1.0.

13. On the Hash Algorithm page, click SHA1 and click Next.



**Note** SHA1 provides a 160-bit hash, which is longer than the 128-bit hash created by the Message Digest 5 (MD5) hash algorithm. SHA1 is preferred over MD5 because its hash algorithm is considered stronger.

14. On the Additional Certificates page, click All Certificates in the Certification Path, Including the Root Certificate, click No Additional Certificates, and click Next.
15. On the Data Description page, in the Description box, provide a text description of the signed file and click Next.
16. On the Time Stamping page, do not enable any options, and then click Next.



**Note** If you have a Time Stamping Server on the network, it is recommended that you apply a time stamp to the signature so the time that the digital signature was applied is known. If the certificate is later revoked, this allows the validator to determine whether the certificate used to sign the application was valid at the time of signing.

17. On the Completing the Digital Signature Wizard page, click Finish.
18. If you are using a smart card CSP, such as the Schlumberger Cryptographic Service Provider, in the Confirm Smart Card PIN dialog box, in the PIN box, type the PIN for the smart card, and click OK.
19. In the Digital Signature Wizard message box, click OK.

This process results in the addition of a digital signature to the application file. The application file can now be verified as a signed file by other applications.

## Visual Basic for Applications Projects

Within a Microsoft Office application, your organization might have created Microsoft Visual Basic for Applications (VBA) projects. By applying a digital signature to these VBA projects, your organization can increase the macro security level to high. (See Figure 21-3.) By adding a digital signature, you can prevent the execution of any nonsigned macros through Group Policy, providing better protection to your Office users.





**Figure 21-3** Enabling high macro security in an Office application



**Note** Office 2003 provides an additional option, Very High, which allows only macros installed in trusted locations to run. Even if a macro is signed, execution is blocked if it is not installed to a trusted location.

Follow these steps to code sign your VBA macro project:

1. Open the Office document containing the macro project you want to sign.



**Note** The same series of steps works for any Microsoft application that implements the Visual Basic Editor.

2. On the Tools menu, point to Macro and click Visual Basic Editor.
3. In the Project Explorer, select the project you want to sign.
4. On the Tools menu, click Digital Signature.
5. In the Digital Signature dialog box, click Choose to select your Code Signing certificate.
6. In the Select Certificate dialog box, select the Code Signing certificate you want to use and click OK.



**Note** You might have to view the certificate to choose the certificate with the code signing (1.3.6.1.5.5.7.3.3) OID in the Enhanced Key Usage extension.

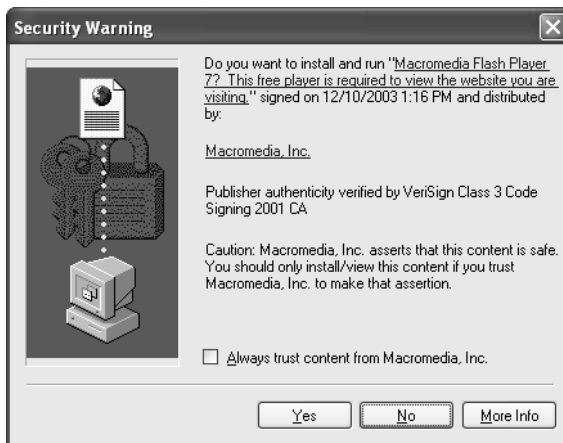
7. In the Digital Signature dialog box, verify that the selected Code Signing certificate is recognized and click OK.
8. Close the Microsoft Visual Basic window.

## Verifying the Signature

Once a digital signature is applied to an application, a user who loads the application will want to validate the application's signature.

### Internet Explorer

In Internet Explorer, when you select to install an application, a Security Warning dialog box appears indicating that the installation control is digitally signed. (See Figure 21-4.)



**Figure 21-4** Verifying the signature on an application in Internet Explorer

In this case, the Macromedia Flash Player 7 is signed by Macromedia, Inc. The dialog box also indicates that the certificate used to sign the Macromedia Flash Player 7 installation file was issued by VeriSign. To view the actual Code Signing certificate, you can click the Macromedia, Inc., link in the Security Warning dialog box.



**Note** In the Security Warning dialog box, it is stated that Macromedia, Inc., asserts that the content is safe, but it is up to the users to determine whether they trust Macromedia's assertion. As with purchasing a product at the store, it is still a case of buyer beware.

If you choose to trust the application, you can click the Yes button to proceed with the installation. Likewise, if you do not trust the entity that signed the application, you can click No to prevent installation.

## The Check Trust Program (Chktrust.exe)

If an application is not used in a Web environment, you can still validate the code signing signature applied to the application file by using the Chktrust.exe program included in the Authenticode for Internet Explorer 5.0 kit.

The Chktrust.exe program verifies the signature and signing certificate used to sign the application. Use the following process to verify the signature:

1. Copy the Chktrust.exe file from the Authenticode for Internet Explorer 5.0 kit and the digitally signed application file to a folder on the local computer.
2. Open a command prompt.
3. At the command prompt, type `chktrust filename` (where *filename* is the name of the signed application file).
4. In the Security Warning dialog box, you will see output similar to that shown in Figure 21-4. This dialog box indicates the description of the application, the subject of the certificate used to sign the application, and the organization that issued the certificate. This combination of information allows you to validate the signing certificate.



**Note** You can also view the signing certificate by clicking the More Info button in the dialog box.

5. If you trust the signature, you can click Yes.
6. The output in the command prompt will show that the validation succeeded.



**Note** Alternatively, you can run `chktrust -v -q filename`, which provides verbose output but blocks execution of the graphical interface. The output simply states whether the validation of the code signing signature has succeeded or failed.

## Best Practices

- **Enable the Unsigned driver installation Group Policy setting to either warn or prevent installation of unsigned device drivers.** This setting ensures that the local Administrator is aware that an unsigned driver is implemented, or it prevents the installation of unsigned drivers in the local operating system.
- **Use a commercially issued Code Signing certificate for publicly distributed applications.** If the application you sign is intended for public use, acquire the Code Signing certificate from a commercial CA, such as VeriSign. This certificate increases the assurance in the signed application because the signing certificate chains to a root CA trusted by most organizations.
- **Use a corporate-issued Code Signing certificate for internal applications.** There is no need to acquire a Code Signing certificate from a commercial organization for internal applications. All computers within the organization trust the local CA hierarchy's root CA.
- **Increase the protection of the Code Signing certificate's private key by using a smart card CSP.** A smart card CSP provides higher protection of the Code Signing certificate's private key by storing it on a two-factor hardware device.
- **Create a custom version 2 certificate template based on the Code Signing certificate that requires certificate manager approval.** This certificate increases the assurance of the Code Signing certificate and allows stronger identity validation of the Code Signing certificate requestor.
- **Implement code signing for all macros implemented in Office applications.** This practice allows an organization to increase the macro security level to high, preventing the execution of nonsigned macros and therefore protecting an organization from attacks based on Visual Basic macros.
- **Implement code signing for all ActiveX controls developed by your organization.** This practice allows you to increase the ActiveX security settings within Internet Explorer, blocking the execution of unsigned ActiveX controls.

- **Outsource a Timestamping Service.** The outsourcer provides a date-and-time stamp for the code signing process, which allows signature-event recognition if the signing certificate is later revoked. As long as the time stamp is a date or time *before* the revocation date, the signature is still considered valid.
- **Use the organization name as the subject of the Code Signing certificate.** This associates the Code Signing certificate with the organization rather than an individual. You can accomplish this by creating a custom user in Active Directory or by allowing the subject to be manually input by the certificate requestor.

## Case Study: Lucerne Publishing

Lucerne Publishing is a global publishing company with a two-tier CA hierarchy. Mike Danseglio manages the development team at Lucerne Publishing.

### Scenario

Over the past year, Lucerne Publishing has been hit by several macro viruses. The primary cause of the virus outbreaks is users opening unauthorized macros in Microsoft Office documents. To restrict the macros that can be executed, you decide to start digitally signing all VBA projects created by your development team.

In addition, Internet Explorer settings must be locked down to prevent the downloading and installation of unsigned ActiveX controls at organization computers. Several financial applications within Lucerne Publishing are Web-based and use ActiveX controls to increase the Web page functionality. By digitally signing these ActiveX controls, Lucerne Publishing can restrict interaction with unsigned ActiveX controls in the default security settings for Internet Explorer.

During the information-gathering stage, you identify the following requirements for the Code Signing certificate:

- The subject of the certificate must contain the company name, not the name of the programmer who signs the certificate.
- The Code Signing certificate must be stored on a GemPlus 8 KB smart card.
- All code signing must be performed by the Mike Danseglio, manager of the Application Development department.
- All Code Signing certificate requests and renewals must be approved by a certificate manager designated by Lucerne Publishing.
- The Code Signing certificate must be valid for three years.
- The Code Signing certificate must have a minimum key length of 1024 bits.

## Case Study Questions

1. Does the Code Signing certificate template meet the design requirements? What must you do to meet the design requirements?
2. In the following table, define the settings on the General tab to meet the design requirements for your custom Code Signing certificate template.

Attribute	Your Recommended Design
Template display name	
Template name	
Validity period	
Publish certificate in Active Directory	
Do not automatically re-enroll if a duplicate certificate exists in Active Directory	

3. What CSP must be enabled on the Request Handling tab to meet the design requirements for the custom Code Signing certificate template?
4. How must you configure the settings on the Subject Name tab to meet the design requirements?
5. In the following table, define the settings on the Issuance Requirements tab to meet the design requirements for the custom Code Signing certificate template.

Attribute	Your Recommended Design
CA certificate manager approval	
This number of authorized signatures	
Require the following for reenrollment	

## Additional Information

- Microsoft Official Curriculum, Course 2821: “Designing and Managing a Windows Public Key Infrastructure” ([www.microsoft.com/traincert/syllabi/2821afinal.asp](http://www.microsoft.com/traincert/syllabi/2821afinal.asp))
- “Authenticode for Internet Explorer 5.0 and Authenticode for DEC Alpha—Internet Explorer 5.0” ([www.microsoft.com/downloads/details.aspx?FamilyID=2B742795-D0F0-4A66-B27F-22A95FCD3425](http://www.microsoft.com/downloads/details.aspx?FamilyID=2B742795-D0F0-4A66-B27F-22A95FCD3425))
- “Introduction to Code Signing” ([http://msdn.microsoft.com/workshop/security/authcode/intro\\_authenticode.asp](http://msdn.microsoft.com/workshop/security/authcode/intro_authenticode.asp))

- “Frequently Asked Questions About Authenticode” (<http://msdn.microsoft.com/library/en-us/dnauth/html/signfaq.asp>)
- “Microsoft Technet: 5-Minute Security Advisor—Signing Office Objects” ([www.microsoft.com/technet/community/columns/5min/5min-402.mspx](http://www.microsoft.com/technet/community/columns/5min/5min-402.mspx))
- “ActiveX Controls and Office Security” ([www.microsoft.com/office/ork/2003/seven/ch23/SecA05.htm](http://www.microsoft.com/office/ork/2003/seven/ch23/SecA05.htm))
- Knowledge Base Article 820738: “About Digital Signatures and Code Signing in Workbooks in Excel 2003”
- Knowledge Base Article 269395: “Code Signing with IEAK 5 and Later”



**Note** Microsoft Knowledge Base articles can be found at <http://support.microsoft.com>. Enter the article number in the Search the Knowledge Base text box.





# Appendix

## Case Study Answers

### Chapter 1: Basics of Cryptography

- 1. Based on the encryption algorithms discussed in the “Default Encryption Algorithms” section of the white paper, does EFS use symmetric or asymmetric encryption?**

EFS uses symmetric encryption for actual data encryption. The File Encryption Key (FEK) can use DESX, 3DES, or AES encryption algorithms. In addition, the RSA asymmetric algorithm is used to encrypt the FEK for retrieval.

- 2. What encryption algorithm is used to encrypt EFS data on a Windows 2000 workstation?**

Windows 2000 uses the DESX algorithm to encrypt EFS data.

- 3. What encryption algorithms can be used to encrypt EFS data on Windows XP?**

Windows XP SP1 supports the DESX, 3DES, and AES-256 encryption algorithms.

- 4. How does the application of Windows XP, Service Pack 1, affect EFS encryption?**

The application of Windows XP, Service Pack 1, replaces the use of DESX for EFS encryption to AES with a 256-bit key.

- 5. What Group Policy setting enables the use of 3DES and AES encryption algorithms?**

You must enable the “System cryptography: Use FIPS-compliant algorithms for encryption” Group Policy setting in Computer configuration\Windows settings\Security settings\Local Policies\Security Options.

- 6. What asymmetric encryption algorithm is used to protect the FEK in EFS?**

EFS uses the RSA asymmetric algorithm to protect the File Encryption Key (FEK) in EFS.

- 7. A developer in your organization has a laptop that dual boots between Windows 2000, Professional, and Windows XP, Professional. Both operating systems have the latest service packs and security updates. The user's Outlook data file is encrypted, and the same EFS key pair is used in both operating systems to provide access to the Outlook data file.**

This morning, your developer was unable to access the Outlook data file when working in Windows 2000, but you are still able to create new encrypted files. Fearing that the Outlook data file was corrupt, he booted into Windows XP and was able to access the data file. What is the probable cause of this problem?

Group Policy is enabling System cryptography. Use FIPS-compliant algorithms for encryption of the Group Policy setting for the Windows XP computer account. The Outlook data file is being encrypted with 256-bit AES encryption, which cannot be encrypted by Windows 2000, Professional, as Windows 2000 only supports DESX encryption.

## Chapter 2: Primer to PKI

- 1. What version is the certificate?**

The certificate is an X.509 version 3 certificate. You can verify this by viewing the Version field on the Details tab.

- 2. What is the name of the issuing CA?**

The name of the issuing CA is CN=adatumCA,DC=adatum,DC=msft. You can verify this by viewing the Issuer field on the Details tab.

- 3. What is the subject name of the certificate?**

The subject name of the certificate is CN = SCUser1, OU = Module09, OU = Labs, DC = adatum, DC = msft. You can verify this by viewing the Subject field on the Details tab.

- 4. Are any other names included in the certificate for the subject?**

The Subject Alternative Name extension contains an additional name for the subject. The name is a user principal name, SCUser1@ADATUM.msft.

- 5. What is the length of the public key associated with the certificate?**

The public key length is 1024 bits. You can verify this by viewing the Public Key field on the Details tab.

- 6. What other X.509 extensions are included in the sample certificate?**

On the Details tab, the following X.509 version 3 extensions are included: Key Usage, Application Policies, Certificate Policies, Enhanced Key Usage, Subject Key Identifier, Authority Key Identifier, CRL Distribution Points, Authority Information Access, and Subject Alternative Name.

**7. Where is the CRL published when revocation checking is performed against the certificate?**

On the Details tab, two URLs are included in the CRL Distribution Points extension indicating where the CRL is published: *ldap://CN=adatumCA,CN=VANCOUVER,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=adatum,DC=msft?certificateRevocationList?base?objectClass=cRLDistributionPoint* and *http://vancouver.adatum.msft/CertEnroll/adatumCA.crl*.

## Chapter 3: Policies and PKI

**1. What is the relationship between a CPS, certificate policy, and security policy?**

A security policy defines an organization's security standards. The contents of an organization's security policy provides the input to the definition of a certificate policy. The certificate policy defines how a PKI will enforce the organization's security policies. Finally, the certificate practice statement defines the operating rules for the PKI in the enforcement of any defined certificate policies.

**2. In what document would you define the methods used to identify the new hires when they start with Fabrikam?**

The methods of identifying the subject of a certificate are defined in a certificate policy. The certificate policy will define the exact measures, such as different types of ID, required to validate the subject's identity before issuing a certificate.

**3. Will the identification validation requirements for existing employees differ from those implemented for new employees of Fabrikam?**

Not necessarily. The answer depends on what measures are taken by the organization to identify employees when they are originally hired by the company. For example, if similar measures were taken before providing employees with photo ID cards, the employees could just show their existing employee card as an equivalent form of identification, rather than show all the identification required for new employees.

**4. The high turnover of employees must be addressed in the CPS. Specifically, what sections must be updated to define the measures taken when an employee is terminated or resigns from Fabrikam?**

The sections of the CPS that define the revocation policies of the organization are "Identification and Authentication," which is where you define how requests for revocation are submitted to a revocation authority, and "Operational Requirements," which is where you define the circumstances under which a certificate is revoked (such as termination or resignation). Although

tempting, the “Certificate and CRL Profiles” section is related to the management of CRLs, not the actual revocation of certificates.

- 5. You are considering modeling your certificate policies after the United States Department of Defense certificate policies. What certificate class would best match your deployment of smart cards?**

The US DOD Class 4 certificate. The DOD Class 4 certificate describes certificates stored on two-factor authentication devices, such as smart cards.

## Chapter 4: Preparing an Active Directory Environment

- 1. Based on the current applications and configuration of the tailspintoys.msft forest, is there any possibility of attribute mangling when the Windows Server 2003 schema modifications are applied? Why or why not?**

Yes, there is a possibility of mangling. The Windows 2000 domain has the Exchange 2000 schema modifications, which include the non-RFC-compliant definitions for *Secretary*, *labeledURI*, and *houseIdentifier*.

- 2. Assuming you use the Exchangemod.ldf script provided on the accompanying CD-ROM to apply the necessary schema modifications, what command line will you use to implement the scripted modifications?**

`ldifde -I -f ExchangeMod.ldf -c DC=X DC=tailspintoys,DC=msft.` The command line must reference the forest root domain, which is tailspintoys.msft in this example.

- 3. What service pack level is required at each domain controller before applying the Windows Server 2003 schema modifications?**

Each domain controller in the forest must be running at least Service Pack 3 to allow an upgrade to the Windows Server 2003 schema.

- 4. What computer will you use to run adprep /forestprep? What group membership(s) is/are required?**

`adprep /forestprep` must be run at the schema operation master by a member of both the Schema Admins and Enterprise Admins groups.

- 5. What computer(s) will you use to run adprep /domainprep? What group membership(s) is/are required?**

`adprep /domainprep` must be run at the infrastructure master at each domain in the forest. In this example, the command must be run at TailspinToys\NADC01 by a member of TailspinToys\Domain Admins group and at WingtipToys\EUDC03 by a member of the WingtipToys\Domain Admins group.

6. **After installing the issuing CAs, the following error appears intermittently in the application log:**

**Event ID: 11**

**Source: Cert Server Enterprise Policy**

**Application: Warning CA was unable to publish the certificate for the Domain\server. Server is not part of the Cert Publishers group. Privilege violation.**

**What configuration change is required to resolve this error?**

The Cert Publishers group in each domain must be assigned read and write permissions for the *userCertificate* attribute in both the domain and AdminSD-Holder container in both TailspinToys and WingtipToys.

7. **How would the solution differ if the network implemented Windows Server 2003 Active Directory rather than Windows 2000 Active Directory?**

In Windows Server 2003 Active Directory, the Cert Publishers group is a domain local group, rather than a global group. This allows you to add a computer account for each issuing CA to the TailspinToys\Cert Publishers group and to the WingtipToys\Cert Publishers group.

## Chapter 5: Designing a Certification Authority Hierarchy

1. **How many tiers are required in the Fabrikam CA hierarchy?**

At least two tiers are required. The best answer is three tiers, as there is a need for multiple policy CAs in the CA hierarchy.

2. **What additional security measures are required for all CAs?**

All CAs must implement HSMs to protect each CA's key pair from theft and tampering.

3. **Are there any external requirements for the CA hierarchy?**

Yes. The corporate Web site must use a certificate that is trusted by all customers. In addition, Europe and Asia have privacy laws that require the implementation of a separate policy CA in those regions.

4. **Is role separation required in your CA hierarchy design? If so, how do you implement it?**

Yes, role separation is required to manage the CAs. A local administration team in each regional office will manage the CAs.

5. **How many policy CAs are required for the CA hierarchy?**

Two: a policy CA for the Americas and another policy CA for Europe and Asia.

**6. What CA hierarchy design best fits the organization's requirements?**

- a. A design based on certificate use.
- b. A design based on geography.
- c. A design based on company departments.
- d. A design based on a combination of certificate use and geography.

The answer is b. The CA hierarchy must be based on geography to allow decentralized administration and provide high availability of certificate templates to all regions.

**7. If offline CAs are implemented at the first and second levels of the CA hierarchy, where will you locate the offline CAs?**

The offline root and the offline policy CA for North America and South America should be located at the corporate office in Atlanta. No differentiation is provided between the Frankfurt and Singapore sites, so the policy CA for Europe and Asia can be placed at either site.

**8. In what domain will the root CA's computer account exist?**

None. The offline root CA must have a workgroup membership rather than a domain membership. Only members of a workgroup can be removed from the network for long periods of time.

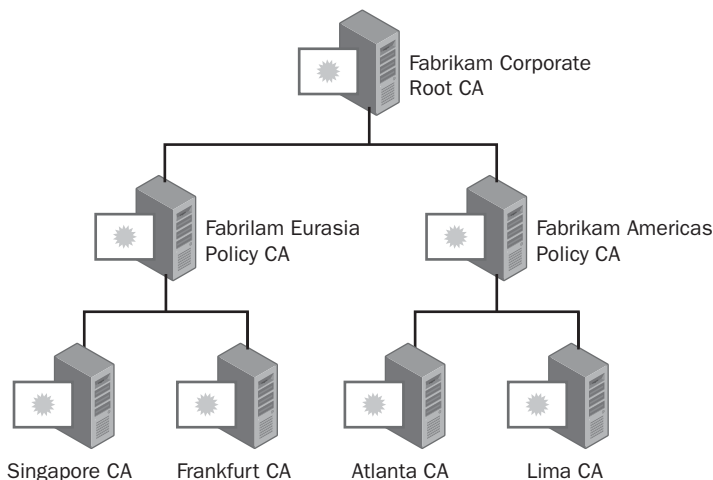
**9. In what domain will you place policy CA computer accounts?**

None. Offline policy CAs must have a workgroup membership rather than a domain membership to allow removal from the network.

**10. In what domain will you place issuing CA computer accounts?**

Place the issuing CAs in their regional domains. This allows easier delegation of administration when implementing Common Criteria role separation.

**11. Based on the requirements presented in this case study, draw your proposed CA hierarchy for Fabrikam Industries.**



- 12. Assuming that your design resulted in a three-tier CA hierarchy and the maximum validity period of a certificate issued to users, computers, services, or network devices is five years, what is the validity period of the root CA certificates, the policy CA certificate(s), and the issuing CA certificates?**

If the maximum validity period for issued certificates is five years, the validity period for the issuing CAs must be double that value, or 10 years. Likewise, the policy CA validity period would be doubled to a value of 20 years, and the validity period of the root CA would be 40 years. If your company is unsure about using a CA certificate's key pair for this extended period, lesser values can be defined, as long as the CA's certificate is renewed before the validity period of the CA certificate constrains the validity period of the certificates issued by that CA.

## Chapter 6: Implementing a CA Hierarchy

### Fabrikam Corporate Root CA

- 1. How do you define the key length of 2,048 bits for the root CA during installation of the root CA?**

The key length must be entered in the Certificate Services Installation Wizard.

- 2. How do you ensure that the key length will remain 2,048 bits when the root CA's certificate is renewed?**

In the CAPolicy.inf file, in the [certsrv\_server] section, you must add the entry `renewalkeylength=2048`.

- 3. What entries are required in the CAPolicy.inf file to define the required base CRL and delta CRL publication intervals?**

```
[certsrv_server]
CRLPeriod=months
CRLPeriodUnits = 6
CRLDeltaPeriod = days
CRLDeltaPeriodUnits = 0
```

Alternatively, you could define the CRLPeriod value as weeks and the CRLPeriodUnits as 26, as long as the overall period is equivalent to six months.

- 4. How would you suppress the inclusion of an AIA and CDP extension in the root CA certificate?**

In the CAPolicy.inf file, add the following information:

```
[AuthorityInformationAccess]

Empty = true
[CRLDistributionPoint]

Empty = true
```

Alternatively, you can just add the [AuthorityInformationAccess] and [CRLDistributionPoint] sections with no entries in the sections.

- 5. After configuring the CAPolicy.inf file, you note that none of the settings are applied to the root CA when you install Certificate Services. You check and find that the file is located in the C:\temp folder. Why did the installation not apply the settings in the CAPolicy.inf file?**

The CAPolicy.inf file must exist in the %windir% folder. If the file is not in the %windir% folder, the settings are not applied.

- 6. How do you configure the root CA to issue subordinate CA certificates with a lifetime of 10 years?**

You must run a post-installation batch file that contains the lines:

```
certutil -setreg CA\ValidityPeriodUnits 10
certutil -setreg CA\ValidityPeriod "Years"
```

- 7. How do you define the location in configuration naming context for publishing the root CA certificate and CRL to Active Directory? (Assume that the forest root domain is the same as shown in Figure 6-1.)**

```
certutil -setreg CA\DSConfigDN CN=Configuration,DC=Fabrikam,DC=com
```

- 8. What command is required to define the AIA publication URLs for the certificates issued by the root CA?**

```
certutil -setreg CA\CertPublicationURLs "1:%windir%\system32\CertSrv\CertEnroll\%1_%3%4.crt\n2:ldap:///CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11\n2:http://www.fabrikam.com/CertData/%1_%3%4.crt"
```

- 9. What command is required to define the CDP publication URLs for the certificates issued by the root CA?**

```
certutil -setreg CA\CRLPublicationURLs "1:%windir%\system32\CertSrv\CertEnroll\%3%8%9.crl\n10:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10 n2:http://www.fabrikam.com/CertData/%3%8%9.crl"
```

## Fabrikam Corporate Policy CA

- 1. On the first attempt to install the policy CA, you receive the error that the CA is unable to determine the revocation status for the policy CA certificate. What must you do to ensure that the policy CA recognizes the root CA certificate as a trusted root certificate and can determine the revocation status for the policy CA certificate?**

You must publish the root CA certificate and CRL in the local computer store of the policy CA.

- 2. What command do you use to add the root CA certificate as a trusted root CA certificate on the Fabrikam Corporate Policy CA, assuming that the name of the root CA certificate is FABINCCA01\_Fabrikam Corporate Root CA.crt?**

```
certutil -addstore -f Root FABINCCA01_Fabrikam Corporate Root CA.crt
```



3. **What command do you use to allow the policy CA to access the root CA CRL, assuming that the name of the root CA certificate is Fabrikam Corporate Root CA.crl?**

```
certutil -addstore -f Root Fabrikam Corporate Root CA.crl
```

4. **How do you configure the CAPolicy.inf file on the policy CA to include the CPS and related OID?**

You add the following lines to the CAPolicy.inf file stored in the %windir% of the policy CA:

```
[PolicyStatementExtension]
```

```
Policies = FabrikamPolicy
```

```
[FabrikamPolicy]
```

```
OID = 1.3.6.1.4.1.311.509.4.1
```

```
URL = http://www.fabrikam.com/CPS/Fabrikampolicy.asp
```

### Fabrikam Corporate Issuing CA

1. **What commands do you use to ensure that the root CA and policy CA certificates are automatically added to the local machine store of all Windows 2000, Windows XP, and Windows Server 2003 domain members?**

```
certutil -dsublish -f FABINCCA01_Fabrikam Corporate Root CA.crt RootCA certutil  
-dsublish -f FABINCCA02_Fabrikam Corporate Policy CA.crt SubCA
```

2. **What commands do you use to ensure that the root CA and policy CA CRLs are automatically added to the Local Machine store of all Windows 2000, Windows XP, and Windows Server 2003 domain members?**

```
certutil -dsublish -f Fabrikam Corporate Root CA.crl
```

```
certutil -dsublish -f Fabrikam Corporate Policy CA.crl
```

3. **On the first attempt to install the issuing CA, you receive the error that the CA is unable to determine the revocation status for the policy CA certificate. Assuming that you have successfully published the root and policy CA information to Active Directory, what must you do to ensure that the issuing CA can determine the revocation status for the issuing CA certificate?**

You must ensure that the root and policy CA information is downloaded to the computer. Run `gpupdate /target:machine /force`, wait 90 minutes for automatic application of Group Policy, or reboot the computer to download the certificates and CRLs to the local computer.

4. **What are the minimum components of the World Wide Web Service required to install the Certificate Services Web Enrollment pages?**

Active Server Pages and World Wide Web Service

5. **What commands are required at the issuing CA to publish the base CRL daily and the delta CRL every eight hours?**

```
Certutil -setreg CA\CRLPeriodUnits 1
```

```
Certutil -setreg CA\CRLPeriod "Days"
```

```
Certutil -setreg CA\CRLDeltaPeriodUnits 8
```

```
Certutil -setreg CA\CRLDeltaPeriod "Hours"
```

## Chapter 7: Securing a CA Heirarchy

1. **If you were to script the configuration of auditing settings for the offline CAs, what command would you include in the script to meet the auditing requirements?**

```
certutil -setreg CA\Auditfilter 127
```

2. **What command is required to meet the audit setting requirements for the online CAs?**

```
certutil -setreg CA\Auditfilter 126
```

3. **Can you meet the security requirements for the CA hierarchy by implementing either a software-based CSP or a smart card CSP? Why or why not?**

No to both. The security policies of the organization require that all CA private key material is protected with FIPS 140-2 level 3 protection; this is only possible by implementing HSMs.

4. **Can you use dedicated HSMs at each CA in the hierarchy and meet the design requirements? What are the drawbacks to this approach if it is possible?**

Yes, you can deploy a dedicated HSM at each of the six CAs in the proposed hierarchy. The only drawback is the cost of purchasing six dedicated HSMs rather than using network-attached HSMs for the online CAs.

5. **Can you use network-attached HSMs at each CA in the CA hierarchy and meet the design requirements? What are the drawbacks to this approach if it is possible?**

No. The City Power and Light security policies do not allow any network connectivity for offline CAs, and this excludes the implementation of network-attached HSMs for the offline CAs.

6. **If you want to implement network-attached HSMs for the issuing CAs in the CA hierarchy, how many network-attached HSMs would you recommend to City Power and Light?**

Two network-attached HSMs are required to meet the design requirement to minimize configuration changes when IP addressing is changed on the network. By deploying a network-attached HSM at both the Atlanta and Anaheim locations, you can attach the HSM and the two issuing CAs at each location on a private network using addressing in a private network address range.

**7. If you were to implement Luna HSMs for the solution, how would you implement the management requirements for operations of the offline CAs?**

The five managers must be issued a green key for validation of any security officer or partition manager tasks. To ensure that the security requirements are met at all times, only one manager in the group of five should be designated as a blue or black key holder. This ensures that three distinct managers are required for any blue or black key operations.

**8. If you were to implement nCipher HSMs for the solution, how would you implement the management requirements for operations of the offline CAs?**

Each of the five managers must be issued a card from the ACS and the OCS. For any HSM management actions, three of five managers must be present to provide the PINs for their cards.

## Chapter 8: Designing Certificate Templates

**1. What MMC console do you use to perform certificate template management?**

The Certificate Templates (certtmpl.msc) console.

**2. Does the default Code Signing certificate template meet the design requirements?**

No. The Code Signing certificate template has a one-year validity period and does not implement any issuance requirements.

**3. Can you modify the default Code Signing certificate template? If not, what would you do?**

No. The Code Signing certificate template is a version 1 certificate template. You must duplicate the existing Code Signing certificate template to create a custom version 2 certificate template.

4. In the table that follows, define the settings on the General tab to meet the design requirements for your custom code signing certificate template.

Attribute	Your recommended design
Template Display Name	Any valid name
Template Name	Any valid name with no spaces
Validity Period	Four years
Publish Certificate in Active Directory	Disabled
Do Not Automatically Re-Enroll If a Duplicate Certificate Exists in Active Directory	Disabled

5. In the table that follows, define the settings on the Request Handling tab to meet the design requirements for the custom code signing certificate template.

Attribute	Your recommended design
Purpose	Signature
Allow Private Key to Be Exported	Disabled
Minimum Key Size	1,024
Do the Following When the Subject Is Enrolled and When the Private Key Associated with This Certificate Is Used	Enroll subject without requiring any user input
CSPs	Only enable the Gemplus GemSAFE Card CSP v1.0

6. In the table that follows, define the settings on the Issuance Requirements tab to meet the design requirements for the custom code signing certificate template.

Attribute	Your recommended design
CA Certificate Manager Approval	Enabled
This Number of Authorized Signatures	Disabled
Require the Following for Re-Enrollment	Valid existing certificate

7. How should you configure the settings on the Superseded Templates tab to ensure that all certificates a CA issues for code signing use the version 2 certificate template?

Add the Code Signing certificate template to the Superseded Templates tab.

**8. What permission assignment modifications are required for the custom code signing certificate?**

You must assign Read and Enroll permissions to the Code Signing group. To meet the design requirements, you also must remove the Enroll permission assignment for the Domain Admins and Enterprise Admins groups.

## **Chapter 9: Certificate Validation**

**1. What URLs do you include in the Northwind Traders root CA certificate for the AIA and CDP extensions?**

None. The best practice is to create a root CA certificate without AIA and CDP extensions so that revocation checking is not performed on root CA certificates.

**2. Are there any network design issues that prevent you from implementing an LDAP URL as the first URL in the list of available URLs for CA certificates and CRLs?**

Yes. The default format of the LDAP URL is not accessible by Windows servers that are not members of the forest. The format also is not accessible by BSD Unix servers. You would have to include the DNS name of the LDAP server in the URL for it to be accessible to nondomain members or UNIX computers.

**3. What form of URL should you implement as the first URL in CDP and AIA URL listings?**

To allow access by nondomain members, you should implement an HTTP URL as the first URL in both the AIA and CDP URL listings.

**4. What protocol by default provides redundancy and high availability in an Active Directory environment?**

LDAP URLs reference the Configuration naming context. The Configuration naming context is available on every domain controller in the forest.

**5. How do you provide redundancy and high availability for HTTP URLs?**

You can publish CRLs and CA certificates to Web server clusters to provide high availability and redundancy for HTTP URLs.

## **Chapter 10: Role Separation**

- 1. The backup software implemented by Tailspin Toys uses a centralized backup services account. When reviewing the event logs, the backup operator notices that the backup fails every night on the two issuing CAs. On inspecting the event logs further, the backup software reports that the failed backup item is the System State backup. What is the likely cause of the error?**

The backup services account is assigned two or more of the Common Criteria roles. Typically, the issue is that the account is a member of the local Administrators group. This group is assigned both the backup privilege and the auditing privilege.

- 2. When inspecting the security permission assignments at the Tailspin Toys Infrastructure CA, you accidentally assign the CA Administrator group the Issue and Manage Certificates permission. When you try and fix the permissions assignment error, you find that access is denied. What must be done to fix the issue?**

A local administrator must first disable the CA\EnableRoleSeparation registry entry. Once role separation is disabled, the local administrator can fix the permissions assignment. Once the assignment is fixed, the local administrator should re-enable the CA\EnableRoleSeparation registry entry.

- 3. The certificate for the Tailspin Toys Employee CA is reaching the halfway point of its validity period and must be renewed. You are logged on to the CA as a CA Administrator but all attempts to renew the CA certificate fail. Who must perform the renewal of the CA certificate?**

A local administrator must perform the CA certificate renewal. Only a local administrator has the necessary access to the Local Machine store to generate or access the CA key pair and generate the certificate request. If role separation is enabled, it must be disabled for the renewal process.

- 4. The Tailspin Toys Employee CA implements key archival for both EFS certificates and e-mail encryption certificates. The security policy of your organization requires that all key recovery operations be performed by at least two employees. If you are assigned the key recovery agent role, what Common Criteria role can you not hold, as this would break the security policy for key recovery?**

You cannot hold the Certificate Manager role. In the key recovery process, a Certificate Manager extracts the encrypted private key from the CA database and then the Key Recovery Agent decrypts the encrypted private key.

- 5. Tailspin Toys implements several version 1 certificate templates at the Tailspin Toys Infrastructure CA. You have delegated the task of managing Certificate Templates to Andy, a member of the IT security team. Andy is able to create new version 2 certificates but is unable to modify the permissions for any of the version 1 certificate templates deployed at the Tailspin Toys Infrastructure CA. Why is Andy unable to modify the version 1 certificate templates?**

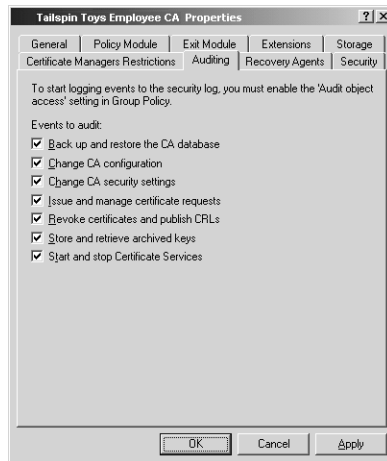
Andy, or a group in which Andy has membership, was delegated permission at both the Certificate Templates and the OID container. Andy (or a group in

which Andy has membership) was not assigned permissions on the existing certificate templates. This prevents him from modifying the permissions on the version 1 certificate templates.

6. **Tailspin Toys wishes to deploy a new enterprise subordinate CA named Tailspin Toys Contractor CA to issue certificates to contractors and vendors working on-site. When you attempt to install the enterprise CA, the options for both enterprise root CA and enterprise subordinate CA are unavailable. What group memberships are required to install an enterprise CA?**

You must be a member of the Enterprise Admins group to install an enterprise CA. Only Enterprise Admins have the necessary permissions to create objects in the Configuration naming context when a new enterprise CA is installed.

7. **You have enabled auditing at all issuing CAs in the CA hierarchy. Today, you received a call from the audit department indicating that no events related to Certificate Services exist in the Windows Security log. You view the properties of each CA and find that the auditing is configured at each CA, as shown in Figure 10-2.**



**Figure 2-1** Auditing settings defined at the Tailspin Toys Employee CA

### **Why are there no audit entries related to Certificate Services?**

The CA does not have success and failure auditing enabled for Object Access. The auditing must be enabled either in the local security policy or in a Group Policy object linked to the organizational unit where the CA's computer account exists in Active Directory.

## Chapter 11: Planning and Implementing Disaster Recovery

- 1. When you perform the installation of the replacement root CA computer, can you use the default installation folder for Windows Server 2003?**

No. The original CA was installed in the folder C:\winnt. The replacement computer must use the same folder for installation.

- 2. Can you assign the replacement CA computer the NetBIOS name FABINCCA01A to designate that this is the second instance of the root CA computer? Why or why not?**

No. You cannot change the name of the computer when you replace the CA computer hardware. The CRL distribution point (CDP) in Active Directory includes the CA computer name in the publication path.

- 3. Which registry key should you back up on the original CA computer to reduce the replacement CA computer configuration?**

HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\CAName, where *CAName* is the logical name of the CA.

- 4. What type of backup should you perform on the original root CA computer before you start the installation of the replacement CA computer—a System State backup or a manual backup?**

Assuming that the replacement hardware has advanced greatly in the last five years, it's most likely you would perform a manual backup of the CA database and log files. Due to hardware differences, a System State backup can result in the failure of the replacement computer.

- 5. What software must be installed on the replacement CA computer before you start the installation of Certificate Services? Why?**

The HSM support software must be installed on the replacement CA computer to allow the replacement computer to communicate with the HSM and access the certificate and key material on the HSM.

- 6. How does the installation of Certificate Services differ from the original installation of Certificate Services?**

You must choose to use an existing certificate by choosing the HSM's CSP and the certificate with the original name of the CA computer.

- 7. Once the installation of Certificate Services is complete, what must be done to allow the CA to recognize the certificates issued by the CA on the previous computer?**

Assuming you performed a manual backup before replacing the hardware, you must restore the CA database and log files to the original locations using the Certificate Services Restore Wizard.



**8. What should be done to the original hardware before it is returned to the leasing company?**

The hard drives from the original hardware should be erased and degaussed to ensure that no data can be accessed from the original hardware. The use of the HSM reduces the risks, as the private key material never existed on the hard drive—only on the HSM.

**9. Do you have to republish the root CA certificate in Active Directory once the hardware replacement is complete?**

No. The replacement CA is still using the same certificate and private key. There is no need to republish the same certificate.

## Chapter 12: Deploying Certificates

**1. Assume that a custom version 2 certificate template is created for code signing that requires CA certificate manager approval. What enrollment method should you use for deploying the custom code signing certificates to the three members of the Quality Assurance team?**

The Certificate Services Web Enrollment site method is recommended because the Web site implements cookies to allow the user to return and complete a pending certificate request.

**2. Assume that a custom version 2 certificate template is created for EFS certificates. What options must be enabled in the certificate template to permit autoenrollment for all users in the Lucerne Publishing forest?**

The certificate template must assign all users Read, Enroll, and Autoenroll permissions.

**3. Where must you configure Group Policy to enable autoenrollment of the custom EFS certificate to all users in the LucernePublish.msft domain?**

You must configure a GPO linked to the LucernePublish.msft domain that enables all Autoenrollment Settings check boxes in User Configuration\Windows Settings\Security Settings\Public Key Policies\Autoenrollment Settings.

**4. Does autoenrollment deploy custom EFS certificates to all Windows 2000 and Windows XP laptop users? Why or why not?**

No. Autoenrollment Settings only deploy custom EFS certificates to users with Windows XP laptops.

**5. What method of enrollment allows EFS certificates to be deployed to users with Windows 2000 laptops without user intervention?**

Lucerne Publishing can develop a Microsoft Visual Basic script that utilizes the Certificate Enrollment Control to submit a request for the custom EFS certificate. To provide automation, this script can be executed at logon to automate the distribution of the custom EFS certificate.

- 6. Assume that the default EFS Recovery Agent certificate template is modified so that only the two EFS recovery agents are assigned Read and Enroll permissions for the certificate template. What enrollment method(s) can they use to acquire their EFS Recovery Agent certificates?**

The agents can use any manual enrollment method, such as the Certificates MMC console focused on the current user or the Certificate Services Web Enrollment pages, to request their EFS Recovery Agent certificates.

- 7. Assuming that the default IPsec certificate is used for the IPsec tunnel mode project, do you use ACRS or Autoenrollment Settings to automate the deployment of IPsec certificates to Windows Server 2003 computers at the corporate office?**

You must use ACRS to deploy the IPsec certificates. The IPsec certificate is a version 1 certificate that can be deployed only by using ACRS.

- 8. What must be done to the IPsec certificate template and the Automatic Certificate Request Settings Group Policy setting to enable automatic enrollment of the IPsec certificates by Windows Server 2003 computers?**

The permissions on the IPsec certificate template must enable Read and Enroll permissions for a group that contains the Windows Server 2003 computer accounts. A Group Policy that enables the Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Automatic Certificate Request Settings GPO with the IPsec certificate template must be linked to the OU containing the Windows Server 2003 computer accounts.

- 9. What must be done to the IPsec certificate template and the Autoenrollment Settings Group Policy setting to enable automatic enrollment of the IPsec certificates by Windows Server 2003 computers?**

The IPsec certificate must be duplicated to create a custom version 2 certificate template. The permissions on the custom IPsec certificate template must enable Read, Enroll, and Autoenroll permissions for a group that contains the Windows Server 2003 computer accounts. Finally, the Autoenrollment Settings Group Policy must be linked to an OU containing the computer accounts and enable all options in Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Autoenrollment Settings.

- 10. How do you deploy IPsec certificates to the third-party VPN devices at the remote offices?**

A PKCS #10 request file can be created at each third-party VPN device and submitted to an enterprise CA by using the Certificate Services Web Enrollment pages.

- 11. If the VPN devices were Cisco VPN devices, what method could you use to automate the IPsec certificate distribution? What additional configuration is required at the enterprise CA?**

Cisco VPN devices support the use of SCEP. SCEP requires that cepsetup.exe be installed at each enterprise CA.

## Chapter 13: Creating Trust Between Organizations

- 1. Which CA in the production hierarchy must be issued the Cross Certification Authority certificate to meet the design requirements?**

It must be issued to The Phone Company South CA. If you issue the Cross Certification Authority certificate to The Phone Company Policy CA, certificates could be trusted from The Phone Company Policy CA and its two subordinate CAs: The Phone Company North CA and The Phone Company South CA, subject to any defined basic constraints.

- 2. What CA must be used to issue the Cross Certification Authority certificate on the certification network to meet the design requirements?**

The Cross Certification Authority certificate can be issued by either The Phone Company Test North CA or The Phone Company Test South CA. Both CAs are enterprise CAs, and there are no restrictions on which issuing CA must be used. It is easier to work with two CAs at the same location (Barcelona), so this example uses The Phone Company Test South CA.

- 3. If the Cross Certification Authority certificate is issued to the The Phone Company Policy CA, what lines must be included in the Policy.inf file to recognize certificates issued by the The Phone Company South CA?**

```
[BasicConstraintsExtension]
PathLength = 1
```

- 4. If the Cross Certification Authority certificate is issued to the The Phone Company South CA, what lines must be included in the Policy.inf file to recognize certificates issued by the The Phone Company South CA?**

```
[BasicConstraintsExtension]
PathLength = 0
```

- 5. What name constraints are required in the Policy.inf to limit permitted certificates to the single certificate issued to the software development manager?**

```
[NameConstraintsExtension]
Include = NameConstraintsPermitted
Critical = true
```

```
[NameConstraintsPermitted]
DirectoryName = "CN=The Phone Company,OU=PKI Roles,DC=ad,DC=thephonecom-
pany,DC=msft"
```

6. **What application policy entries are required in the Policy.inf to limit the certificates to only code signing certificates?**

```
[ApplicationPolicyStatementExtension]
```

```
Policies = AppCodeSignPolicy
```

```
Critical = false
```

```
[AppCodeSignPolicy]
```

```
OID = 11.3.6.1.5.5.7.3.3 ; Code Signing
```

7. **Assuming that the Cross Certification Authority certificate is issued by The Phone Company Test South CA to The Phone Company South CA, how does the certificate chain for the manager's certificate look when viewed at a Windows XP computer in the certification forest?**

The Phone Company Test Root CA => The Phone Company Test Policy CA => The Phone Company Test South CA => The Phone Company South CA => The Phone Company

8. **Assuming that the Cross Certification Authority certificate is issued by The Phone Company Test South CA to The Phone Company South CA, how does the certificate chain for the manager's certificate look when viewed at a Windows XP computer in the production forest?**

The Phone Company Root CA => The Phone Company Policy CA => The Phone Company

## Chapter 14: Archiving Encryption Keys

1. **At what CAs in the CA hierarchy must you enable key archival? How many key recovery agents must be defined at each CA?**

Key archival must be enabled at each of the regional issuing CAs. At each regional CA, you must define two key recovery agents: one at the corporate head office in Chicago, and one at the regional office where the issuing CA is located.

2. **What operating system must be installed on the issuing CAs to allow key archival?**

The issuing CAs must be running Windows Server 2003, Enterprise Edition, or Windows Server 2003, Datacenter Edition, to enable key archival.

3. **Can you combine the key recovery agent role with the roles of CA administrator, certificate manager, auditor, or backup operator? Why or why not?**

You can combine the key recovery agent role with any of the Common Criteria roles, as the key recovery agent is not a Common Criteria role.

**4. What Common Criteria role is blocked from being a key recovery agent due to the design requirements?**

The key recovery agent cannot be assigned the certificate manager role. The design requirement specifying two individuals for all key recovery operations excludes this combination of roles.

**5. What certificate template must be available to allow secure transmission of the requestor's private key to the issuing CA?**

The CA Exchange certificate provides the encryption of the requestor's private key as it is transmitted from the requesting computer to the issuing CA.

**6. What certutil command is used by a certificate manager to extract the encrypted BLOB from the CA database?**

The certutil -getkey command allows the certificate manager to extract the encrypted BLOB from the CA database.

**7. What certutil command is used by a key recovery agent to decrypt the PKCS #12 file within the encrypted BLOB file?**

The certutil -recoverkey command allows the key recovery agent to extract the PKCS #12 file from the encrypted BLOB file.

**8. What risk is there to allowing the key recovery agent to send the PKCS #12 file and password to the user in the same e-mail message?**

If attackers gain access to the message, they have the ability to import the PKCS #12 file into their profile.

**9. What risk is there to archiving a certificate template with the purpose of Signature and Encryption?**

If a certificate has the purpose of Signature and Encryption, the certificate can be used for both digital signing and encryption. The digital signing purpose can lead to impersonation if the private key is recovered from the CA database.

## Chapter 15: Smart Card Deployment

**1. Can you use the default Enrollment Agent certificate template to meet the design requirements for City Power and Light? Why or why not?**

No, you cannot use the default certificate template because the default certificate template does not enforce CA certificate manager approval.

**2. If you create a custom certificate template for the enrollment agent, how do you enforce that only Andy receives a custom enrollment agent certificate?**

You can modify the permissions of the certificate template to assign only Andy's account Read and Enroll permissions. Also, once Andy enrolls the certificate from the City Power and Light Eastern Employee CA, you can remove the certificate template from the templates available for enrollment.

**3. How do you enforce the Atlanta certificate manager's authorization of the Enrollment Agent certificate issued to Andy?**

You must modify the custom Enrollment Agent certificate template to enable the CA certificate manager approval check box on the Issuance Requirements tab of the custom certificate template.

**4. Can you use the default Smart Card User certificate template for the administrative smart cards?**

No, the Smart Card User certificate template also allows Secure Email. The administrative cards are limited to client authentication and smart card logon purposes.

**5. Do you have to use a custom certificate template to meet the design goals of City Power and Light?**

Yes. Only a custom certificate template allows you to designate a specific CSP, such as the Schlumberger CSP. The default Smart Card User and Smart Card Logon certificate templates are version 1 certificate templates that do not allow you to designate a specific CSP.

**6. How do you limit enrollment of the smart card certificate template to Andy?**

You must assign either Andy or a custom global group with Andy as the sole member Read and Enroll permissions for the custom smart card certificate template. No other security principals can be assigned Enroll permissions for the certificate template.

**7. Assuming that the administrators can log on from both servers and desktop workstations spread among any OU in the forest, how do you enforce smart cards for interactive logon for the Administrator accounts?**

You must modify each administrator user account's properties to enable the Smart Card Is Required For Interactive Logon option. You cannot use Group Policy, as this setting enforces smart card logon for nonadministrative staff.

**8. If the administrators are to use Terminal Services to administer servers, where must you install the updated Schlumberger smart card CSP?**

The updated Schlumberger smart card CSP must be installed at both the administrator's desktop computers and at the server to which they are connecting. Both the client and the server must recognize the submitted smart card.

**9. How do you enforce smart card authentication for remote access connections by the administrative staff?**

A separate remote access policy must be created that enforces EAP/TLS authentication. In addition, the remote access policy conditions should allow application only to a custom global or universal group that contains all administrative user accounts.

## Chapter 16: Encrypting File System

- 1. Does the default EFS Recovery Agent certificate template meet the design requirements for the Lucerne Publishing EFS project?**

Yes. There are no specific design requirements for the enrollment of the EFS Recovery Agent certificate template. By assigning permissions so that only members of the Internal Audit department have Read and Enroll permissions, the enrollment is restricted to approved users.

- 2. Does the default Key Recovery Agent certificate template meet the design requirements for the Lucerne Publishing EFS project?**

Yes. There are no specific design requirements for the enrollment of the Key Recovery Agent certificate template. By default, members of the Enterprise Admins group have Read and Enroll permissions for the Key Recovery Agent certificate template.

- 3. Do the design requirements allow the EFS Recovery Agent and Key Recovery Agent certificate templates to be published only at the Lucerne Publishing Americas CA?**

Yes. It does not matter which issuing CA in the CA hierarchy publishes these certificate templates. As long as the issued certificates chain to the Lucerne Publishing Root CA certificate, they are recognized at all locations in the Lucerne Publishing network.

- 4. Does Andy's proposed solution meet the design requirements for designation of key recovery agents in the forest?**

No. The design requirements demand that key archival and recovery are only enabled at the Lucerne Publishing Americas CA. To meet the requirements, the key recovery agents from each region should be designated as key recovery agents at the Lucerne Publishing Americas CA. The proposed solution only designates a single key recovery agent at each region's CA, enabling key archival at all issuing CAs, not just the Lucerne Publishing Americas CA.

- 5. Is EFS encryption disabled for all Windows 2000 computers not in the OU named OU=Notebooks,OU=Computer Accounts,DC=lucernepublish,DC=msft?**

No. The configured GPO resorts to using the locally defined EFS recovery agent. To prevent encryption at the Windows 2000 computers, an empty Encrypting File System policy must be defined. The application of no Encrypting File System policy results in the use of the EFS encryption settings defined in the local security policy.

**6. Does Andy's proposed design disable EFS encryption for Windows XP computer accounts not in the OU named OU=Notebooks,OU=Computer Accounts,DC=lucernepublish,DC=msft?**

No. The design does not disable EFS encryption for any Windows XP computers. To disable EFS encryption for Windows XP computers, clear the Allow Users To Encrypt Files Using Encrypting File System (EFS) check box on the property sheet of the Encrypting File System Group Policy setting.

**7. Does the Lucerne Publishing EFS certificate template allow for autoenrollment by Windows XP users?**

Yes. The certificate template correctly enables Read, Enroll, and Autoenroll permissions for the Lucerne Publishing EFS certificate template.

**8. Does the proposed EFS Autoenrollment GPO enable autoenrollment of the Lucerne Publishing EFS certificate template by users with Windows XP computers?**

No. The EFS Autoenrollment GPO must be applied to the OU where the user accounts, not the computer accounts, exist. The EFS Autoenrollment GPO also must be modified to enable autoenrollment for user accounts, not computer accounts. Because no user OUs are defined, you can define the GPO at the Lucernepublish.com domain, but limit Read, Enroll, and Autoenroll permissions to members of a custom universal or global group.

## Chapter 17: Implementing SSL Encryption for Web Servers

**1. Which CA should issue the Web Server certificate for the customer billing system Web site?**

The customer billing system requires a Web Server certificate from a commercial CA so that there is greater trust in the customer billing system Web site. By using a commercial CA, more customers trust the root CA certificate of the Web Server certificate's certificate chain.

**2. Which CA should issue the Web Server certificate for the employee benefits Web site?**

The Web Server certificates for the employee benefits Web site can be issued by any of the three issuing CA's in The Phone Company's CA hierarchy.

**3. Where should the Web server certificate(s) be deployed for the customer billing system Web site?**

For the customer billing system Web site, the Web Server certificate must be installed on the DALTXIIS01 computer.



**4. Where should the Web Server certificate(s) be deployed for the employee benefits Web site?**

For the employee benefits Web site, a separate Web Server certificate must be installed at each computer in the cluster: DALTXIIS02, AMSNLIIS01, and TORONIIS01.

**5. How do you implement certificate mapping for the customer billing Web site?**

Certificate mapping should be deployed by using Active Directory mapping. The same certificate mappings are required at any of the three Web servers.

**6. If you perform an implicit certificate mapping, what form of name must be included in the Subject or the Subject Alternative Name extension of the user certificate? Does the Smart Card User certificate template meet this condition?**

The Subject Alternative Name must include the user's UPN in the certificate's Subject Alternative Name extension. The Smart Card User certificate does meet this requirement, as the user's UPN is also required in the certificate to support smart card login.

**7. What subject is required for the Web Server certificate for the customer billing system Web site?**

The subject of the customer billing system Web site's certificate must be *www.thephonecompany.com*.

**8. What subjects are required for the Web Server certificate for the employee benefits Web site?**

The subject of the three employee benefits Web site's certificates must be *benefits.thephonecompany.com*. You can deploy the same Web Server certificate and private key at each Web server or deploy individual certificates and private keys at each Web server.

## Chapter 18: Secure E-Mail

**1. Based on the security policies related to e-mail usage, how many e-mail certificates must be distributed to each user?**

Each user must be issued two e-mail certificates: one for e-mail signing and one for e-mail encryption.

**2. What certificate(s) must be published to Active Directory to enable the sending of encrypted e-mail between employees of Adventure Works?**

The encryption certificate must be published into the *userCertificate* attribute of the recipient's user account in Active Directory to allow a sender to obtain the recipient's public key from the global catalog.

- 3. Will the current CA infrastructure allow the e-mail signing and e-mail encryption certificates to be recognized by the customers of Adventure Works?**

Yes, as long as the customer has not removed the VeriSign Class 3 Public Primary Certification Authority from the Trusted Root store (of client machines).

- 4. What method would you use to deploy the e-mail certificate(s) to the Adventure Works users? What certificate template settings are required to allow this method of enrollment?**

You can use autoenrollment settings to enable autoenrollment of the two certificate templates. The two certificate templates must enable the Read, Enroll, and Autoenroll permission for all users that will receive the certificates.

- 5. One of the travel agents is able to open his encrypted e-mail at only one of the available agent computers. When he attempts to open his encrypted e-mail at the other computers, the attempt fails. What can you do to ensure that the travel agent can open the encrypted e-mail at any of the travel agent computers?**

You must implement a roaming profile for each travel agent user account so that the user's certificate store is downloaded to each computer that he or she works at. The current computer must be used when the roaming profile is enabled so that the roaming profile is updated with the certificates in the Current User store.

- 6. How do you propose to enforce the security policy that two or more people must be involved in the recovery?**

The Adventure Works Issuing CA must ensure that different people hold the key recovery agent and certificate manager roles. Separating the roles ensures that two people must be involved in every key recovery operation.

- 7. How do you enforce that users must provide a password to access the private keys associated with the e-mail signing and e-mail encryption certificates?**

The certificate templates for both e-mail signing and e-mail encryption must enable the Prompt the User During Enrollment and Require User Input When The Private Key Is Used option.

- 8. What must a travel agent do to allow a customer to send an encrypted e-mail message?**

To send the travel agent an encrypted e-mail message, the customer must access the travel agent's encryption public key. This can be accomplished by the travel agent sending the customer a signed e-mail message or by creating an externally available LDAP directory for customers to retrieve the travel agent's encryption certificate.

- 9. What solution can be used to allow remote travel agents to securely access their e-mail and use S/MIME to protect the e-mail messages without enabling an additional e-mail client?**

Because Travel Works uses Exchange Server 2003 and Outlook 2003, it can implement RPC over HTTPS to enable secure client access to mail services from the Outlook client. There is no need to implement RFC-based protocols, such as POP3 or IMAP4.

- 10. One of the travel agents has forgotten the password used to protect the e-mail encryption certificate and can no longer read encrypted e-mail. What must you do to allow the travel agent to access the encrypted e-mail?**

You must delete the existing certificate and private key from the user's certificate store and recover the private key from the CA database. When you import the certificate, the user can choose a new password for the encryption certificate's private key.

- 11. When performing the proof of concept test of your e-mail solution, you are told that customers are complaining that their e-mail applications are reporting that the digital signatures are failing. You look at the certificate and find the following URLs in the CDP extension:**

- *LDAP:///CN=Adventure Works Issuing CA,CN=ADVCA01,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=travelworks,DC=com*
- *http://advca01/certenroll/Adventure%%20Works%%20%%20Issuing%%20CA.crl*

**What is causing the certificate validation to fail? What must you do to fix the problem?**

None of the CDP URLs are available from the Internet. The customer computers are unable to retrieve a valid CRL for the Adventure Works Issuing CA. You must add an Internet-accessible URL to the CDP extension, and then revoke and re-issue the e-mail encryption and signing certificates so that they include the correct URLs in the CDP extension.

## Chapter 19: Virtual Private Networking

- 1. What authentication protocol must be enforced for VPN communications to meet the initial authentication requirements?**

MS-CHAPv2 must be enforced for the initial authentication requirements. MS-CHAPv2 provides the ability to type the user name and password for authentication and enforce mutual authentication between the VPN user and the RADIUS server.

2. **What certificates are required for the initial VPN solution? Provide your answers in the following table:**

<b>Principal</b>	<b>Certificate</b>
VPN User	<b>No certificates required</b>
VPN Client Computer	<b>IPSec certificate</b>
RADIUS Server	<b>No certificate required</b>
VPN Server	<b>IPSec certificate</b>

3. **What authentication protocol must be enforced for VPN communications to meet the modified authentication requirements to enforce smart card authentication?**

EAP-TLS must be enforced for the initial authentication requirements. EAP-TLS enforces mutual authentication between the VPN user and the RADIUS server and can be configured to require smart card authentication.

4. **What certificates are required for the modified VPN solution that uses smart cards? Provide your answers in the following table:**

<b>Principal</b>	<b>Certificate</b>
VPN User	<b>Smart Card User or Smart Card Logon certificate</b>
VPN Client Computer	<b>IPSec certificate</b>
RADIUS Server	<b>RAS and IAS Server certificate</b>
VPN Server	<b>IPSec certificate</b>

5. **How can Lucerne Publishing implement the ability to immediately shut down all VPN access?**

Lucerne Publishing can implement RADIUS authentication by installing Internet Authentication Services on a computer (or on two computers to implement fault-tolerant remote access policy application).

6. **What certificate template(s) are required for the L2TP/IPSec tunnel? What CA should you publish the certificates at?**

You must publish the IPSec and IPSec (offline request) certificate templates. The certificate templates must be published at each of the three issuing CAs: Lucerne Publishing Americas CA, Lucerne Publishing EMEA CA, and Lucerne Publishing APAC CA.

**7. What method could you use to deploy the IPSec certificates to forest member computers?**

You could deploy the IPSec certificates to forest members by using Automatic Certificate Request Settings.

**8. What method could you use to deploy the IPSec certificates to nonforest member computers?**

You could have users request the IPSec (offline request) certificate template and save the issued certificate and private key to a floppy disk. The certificate could then be imported on their home computers.

**9. When Lucerne Publishing switches to using Smart Card certificates, how can the Smart Card certificate template be modified to further restrict VPN access to the network?**

A custom version 2 certificate template can be created that implements a custom application policy OID. The RADIUS server can then be configured to require the custom application policy OID in the certificate to allow access to the network.

**10. What certificate(s) would you deploy at the VPN server when using RADIUS authentication?**

You would only require the IPSec certificate template at the VPN server.

**11. What application would you use to configure the client computers to ensure that the VPN client software is correctly configured?**

You would use the CMAK to create a Connection Manager profile that defines the correct settings for connecting to the network.

**12. What additional VPN software is required for some of the home computers?**

The Microsoft L2TP/IPSec VPN Client for Windows 98, Windows Millennium Edition, and Windows NT 4.0 Workstation is required for home computers not running Windows 2000 Professional or Windows XP.

## Chapter 20: Wireless Networking

**1. What network infrastructure service required for wireless network is missing from the Margie's Travel network? On which server(s) would you install the missing service?**

There are no RADIUS servers on the network. You must install IAS on at least two computers to ensure redundancy. The most logical choice is to deploy IAS on the two domain controllers.

**2. When you purchase the wireless access points for the networks, what features are required to meet the design requirements?**

The wireless access points must support RADIUS authentication. Ideally, the wireless access points should support WPA to ensure the strongest level of encryption.

**3. What certificate(s) are required on the wireless access points?**

No certificates are required on the wireless access points. The wireless access points simply translate EAP authentication request packets to RADIUS authentication request packets and RADIUS authentication responses to EAP authentication responses.

**4. What certificate(s) are required at each desktop or notebook computer?**

Each computer or notebook must have a certificate that includes the Client Authentication application policy OID.

**5. What certificate(s) are required for each user of the network?**

Each user must have a certificate that includes the Client Authentication application policy OID.

**6. What other certificate(s) are required for the wireless network deployment?**

The two IAS servers must have certificates that include the Server Authentication application policy OID. For example, the RAS and IAS Server certificate provides this application policy OID.

**7. How many remote access policies are required for the wireless deployment?**

Two remote access policies are required: one for computer authentication and one for user authentication.

**8. What additional measures can be taken to ensure that only Margie's Travel users can connect to the wireless network?**

The user and computer certificates can include a custom application policy OID that uniquely identifies the certificates as approved wireless certificates. The remote access policies can include remote access profile settings requiring the existence of the custom application policy OID for a successful connection.

**9. How can you ensure that each desktop and notebook computer is correctly configured for connectivity to the wireless network?**

You can use Group Policy to ensure that the correct wireless security settings are applied to all domain members.

## Chapter 21: Code Signing

1. **Does the Code Signing certificate template meet the design requirements? What must you do to meet the design requirements?**

No. The Code Signing certificate template has a one-year validity period and does not implement any issuance requirements. You must create a custom version 2 certificate template based on the Code Signing certificate template.

2. **In the following table, define the settings on the General tab to meet the design requirements for your custom Code Signing certificate template.**

Attribute	Your Recommended Design
Template display name	<b>Any valid name</b>
Template name	<b>Any valid name (no spaces allowed)</b>
Validity period	<b>3 years</b>
Publish certificate in Active Directory	<b>Disabled</b>
Do not automatically re-enroll if a duplicate certificate exists in Active Directory	<b>Disabled</b>

3. **What CSP must be enabled on the Request Handling tab to meet the design requirements for the custom Code Signing certificate template?**

The Gemplus GemSAFE Card CSP v1.0 CSP must be enabled in the custom Code Signing certificate template. All other CSPs should be disabled.

4. **How must you configure the settings on the Subject Name tab to meet the design requirements?**

You must allow the requestor to supply the subject in the request. This allows Mike Danseglio to provide Lucerne Publishing as the subject of the custom Code Signing certificate.

5. **In the following table, define the settings on the Issuance Requirements tab to meet the design requirements for the custom Code Signing certificate template.**

Attribute	Your Recommended Design
CA certificate manager approval	<b>Enabled</b>
This number of authorized signatures	<b>Disabled</b>
Require the following for reenrollment	<b>Same criteria as for enrollment</b>





## About the Author

Brian Komar is the President and co-founder of IdentIT Inc., a consulting firm specializing in identity integration and network security solutions. Together with Paul Adare, Brian's business partner, IdentIT Inc. works with Microsoft Consulting Services in delivering PKI and network security consulting engagements for Microsoft's customers.

Brian has written several books related to computer security during the past few years, including the *Microsoft Windows Security Resource Kit*, *MCSE Training Kit: Designing Microsoft Windows 2000 Network Security*, and *Firewalls for Dummies*. In addition to writing books, Brian has written three white papers related to PKI for Microsoft: "Implementing and Administering Certificate Templates in Windows Server 2003," "Troubleshooting Certificate Status and Revocation," and "Planning and Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003," and he developed course 2821, *Designing and Managing a Windows Public Key Infrastructure*, the Microsoft Official Curriculum course on PKI. Brian is also a frequent speaker at IT industry conferences such as Microsoft Tech Ed, Windows & .NET Magazine Connections, and Microsoft IT Forum. Brian specializes in sessions that look under the hood at security and discuss practical implementation of security based on experiences from the field.

If you wish to contact Brian, you can reach him at [bkomar@identit.ca](mailto:bkomar@identit.ca).



