IBM Client Security Solutions

Client Security Version 5.3 Benutzerhandbuch

IBM Client Security Solutions

Client Security Version 5.3 Benutzerhandbuch

Anmerkung

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten Sie die Informationen in Anhang B, „Bemerkungen und Marken", auf Seite 61 lesen.

- Die IBM Homepage finden Sie im Internet unter: **ibm.com**
- IBM und das IBM Logo sind eingetragene Marken der International Business Machines Corporation.
- Das e-business-Symbol ist eine Marke der International Business Machines Corporation.
- Infoprint ist eine eingetragene Marke der IBM.
- ActionMedia, LANDesk, MMX, Pentium und ProShare sind Marken der Intel Corporation in den USA und/oder anderen Ländern.
- C-bus ist eine Marke der Corollary, Inc. in den USA und/oder anderen Ländern.
- Java und alle auf Java basierenden Marken und Logos sind Marken der Sun Microsystems, Inc. in den USA und/oder anderen Ländern.
- Microsoft Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.
- PC Direct ist eine Marke der Ziff Communications Company in den USA und/oder anderen Ländern.
- SET und das SET-Logo sind Marken der SET Secure Electronic Transaction LLC.
- UNIX ist eine eingetragene Marke der Open Group in den USA und/oder anderen Ländern.
- Marken anderer Unternehmen/Hersteller werden anerkannt.

Erste Ausgabe (Mai 2004)

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Client Security Solutions Client Security Version 5.3 User's Guide,
herausgegeben von International Business Machines Corporation, USA

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
SW TSC Germany
Kst. 2877
Mai 2004

Inhaltsverzeichnis

Vorwort

Das vorliegende Handbuch enthält Informationen zum Einsatz von Client Security auf IBM Netzwerkcomputern bzw. IBM Clients, auf denen der integrierte IBM Security Chip installiert ist.

Das Handbuch enthält folgende Abschnitte:

Kapitel 1, „Einführung", enthält einen kurzen Überblick über die grundlegenden Sicherheitskonzepte, eine Übersicht über die in der Software enthaltenen Anwendungen und Komponenten sowie eine Beschreibung der PKI-Funktionen (Public Key Infrastructure).

Kapitel 3, „Standortunabhängiger Zugriff mit Berechtigungsnachweis in CSS", enthält Informationen zum Einsatz von IBM Client Security für den Schutz wichtiger Dateien und Ordner.

Kapitel 4, „Anweisungen für den Clientbenutzer", enthält Anweisungen zu unterschiedlichen Tasks, die der Clientbenutzer mit Client Security ausführen kann. Dazu gehören Anweisungen zur Verwendung der gesicherten UVM-Anmeldung, des Client Security-Bildschirmschoners, der sicheren E-Mail-Übertragung und des Benutzerkonfigurationsprogramms.

Kapitel 5, „Fehlerbehebung", enthält nützliche Informationen zum Beheben von Fehlern, die beim Umsetzen der in diesem Handbuch enthaltenen Anweisungen auftreten können.

Anhang A, „Informationen zu Kennwörtern und Verschlüsselungstexten", enthält Kriterien für Verschlüsselungstexte, die auf einen UVM-Verschlüsselungstext angewendet werden können, und Regeln für Administratorkennwörter.

Anhang B, „Bemerkungen und Marken", enthält Informationen zu rechtlichen Hinweisen und Marken.

Zielgruppe

Das vorliegende Handbuch richtet sich an die Benutzer von Clients, auf denen Client Security installiert ist. Bei den in diesem Handbuch enthaltenen Anweisungen wird davon ausgegangen, dass Installation und Konfiguration von Client Security auf Ihrem Computer abgeschlossen sind. Des Weiteren setzt das Handbuch gewisse Kenntnisse in Bezug auf digitale Zertifikate und die Verwendung von Anmeldeschnittstellen und Bildschirmschonern voraus.

Benutzung des Handbuchs

Nutzen Sie die in diesem Handbuch enthaltenen Informationen zum Einrichten des Bildschirmschoners von Client Security, zum Ändern von UVM-Verschlüsselungstexten und Windows-Kennwörtern sowie zum Einsatz der Verschlüsselungsmöglichkeiten von Client Security für Microsoft- bzw. Netscape-Anwendungen. Dieses Handbuch ist als Ergänzung der Handbücher *Client Security Installationshandbuch*, *Client Security mit Tivoli Access Manager verwenden* und *Client Security Administratorhandbuch* gedacht.

Einige der in diesem Handbuch enthaltenen Informationen finden Sie auch im *Administratorhandbuch für Client Security*. Das *Administratorhandbuch* richtet sich an Sicherheitsadministratoren, die Client Security auf IBM Clients installieren und konfigurieren.

Dieses Handbuch sowie die übrige Dokumentation zu Client Security können von der IBM Website unter folgender Adresse heruntergeladen werden: http:////www.pc.ibm.com/us/security/index.html.

Zusätzliche Informationen

Zusätzliche Informationen sowie Aktualisierungen für Sicherheitsprodukte können, wenn erhältlich, von der IBM Website unter http://www.pc.ibm.com/us/security/index.html heruntergeladen werden.

Kapitel 1. Einführung

Select ThinkPad™- und ThinkCentre™-Computer sind mit integrierter Verschlüsselungshardware ausgestattet, die gemeinsam mit einer speziellen, für den Download verfügbaren Softwaretechnologie verwendet werden kann, um auf Client-PC-Plattformen erweiterte Sicherheitsfunktionen zu aktivieren. Diese Hardware-/Softwarekombination wird allgemein als integriertes IBM Sicherheits-Subsystem (IBM Embedded Security Subsystem, ESS) bezeichnet. Dabei besteht die Hardwarekomponente aus dem integrierten IBM Security Chip und die Softwarekomponente aus IBM Client Security (CSS).

IBM Client Security ist für IBM Computer konzipiert, die den integrierten IBM Security Chip zum Verschlüsseln von Dateien und Speichern von Chiffrierschlüsseln verwenden. Client Security besteht aus Anwendungen und Komponenten, mit denen IBM Clientsysteme die entsprechenden Sicherheitsfunktionen im lokalen Netzwerk, im Unternehmen oder im Internet gewährleisten können.

Integriertes IBM Sicherheits-Subsystem (ESS)

IBM ESS unterstützt Schlüsselverwaltungsfunktionen, wie z. B. eine PKI (Public Key Infrastructure). Es besteht aus folgenden lokalen Anwendungen:

- Verschlüsselung von Dateien und Ordnern (File and Folder Encryption, FFE)
- Password Manager
- Gesicherte Windows-Anmeldung
- Mehrere konfigurierbare Authentifizierungsmethoden, einschließlich:
  - Verschlüsselungstext
  - Registrierung über Fingerabdruck
  - Smartcard
  - Proximity Badge (berührungsloser Ausweis)

Damit die Funktionen von IBM ESS effektiv genutzt werden können, muss ein zuständiger Sicherheitsadministrator mit einigen grundlegenden Konzepten vertraut sein. In den folgenden Abschnitten werden diese grundlegenden Sicherheitskonzepte beschrieben.

Integrierter IBM Security Chip

Das integrierte IBM Sicherheits-Subsystem (IBM Embedded Security Subsystem) ist eine integrierte Verschlüsselungshardwarekomponente, die besondere Sicherheitsfunktionen für ausgewählte IBM PC-Plattformen bietet. Mit Hilfe dieses Sicherheits-Subsystems werden Verschlüsselungs- und Authentifizierungsprozesse von reinen Softwarelösungen, die relativ anfällig für Angriffe sind, in die gesicherte Umgebung einer speziellen Hardwarekomponente übertragen. Dieser Ansatz bietet eine bedeutend höhere Sicherheit.

Das integrierte IBM Sicherheits-Subsystem unterstützt Folgendes:

- RSA3-PKI-Operationen, wie z. B. Verschlüsselungen aus Datenschutzgründen und digitale Unterschriften zur Authentifizierung
- RSA-Schlüsselerstellung
- Generierung von Zufallszahlen

- RSA-Funktionsverarbeitung in 200 Millisekunden
- EEPROM-Speicher für die Speicherung von RSA-Schlüsselpaaren
- Alle in Spezifikation Version 1.1 definierten TCPA-Funktionen
- Kommunikation mit dem Hauptprozessor über LPC-Bus (Low Pin Count)

IBM Client Security

IBM Client Security setzt sich aus folgenden Softwareanwendungen und -komponenten zusammen:

- **Administratordienstprogramm:** Das Administratordienstprogramm ist die Schnittstelle, die ein Administrator zum Aktivieren oder Inaktivieren des integrierten Sicherheits-Subsystems und zum Erstellen, Archivieren und erneuten Generieren von Chiffrierschlüsseln und Verschlüsselungstexten verwendet. Darüber hinaus kann ein Administrator mit diesem Dienstprogramm der Sicherheitspolicy, die von Client Security bereitgestellt wird, Benutzer hinzufügen.
- **Administratorkonsole:** Die Administratorkonsole von Client Security ermöglicht Administratoren das Konfigurieren eines Netzwerks mit standortunabhängigem Zugriff mit Berechtigungsnachweis, zum Erstellen und Konfigurieren von Dateien für die Implementierung und zum Erstellen eines administratorunabhängigen Konfigurations- und Wiederherstellungsprofils.
- **Benutzerkonfigurationsprogramm:** Das Benutzerkonfigurationsprogramm ermöglicht Clientbenutzern das Ändern des UVM-Verschlüsselungstextes, das Aktivieren von Windows-Anmeldekennwörtern, so dass sie von UVM erkannt werden, das Aktualisieren von Schlüsselarchiven und das Registrieren von Fingerabdrücken. Außerdem kann ein Benutzer Sicherungskopien der digitalen Zertifikate erstellen, die vom integrierten IBM Sicherheits-Subsystem erzeugt wurden.
- **User Verification Manager (UVM):** In Client Security werden mit UVM Verschlüsselungstexte und andere Elemente verwaltet, mit denen Systembenutzer authentifiziert werden. Mit einem Lesegerät für Fingerabdrücke kann UVM z. B. bei der Anmeldung Benutzer authentifizieren. Client Security unterstützt folgende Funktionen:
  - **UVM-Client-Policy-Schutz:** Client Security ermöglicht es Sicherheitsadministratoren, die Client-Sicherheitspolicy, die festlegt, wie ein Clientbenutzer auf dem System authentifiziert wird, einzurichten.

    Wenn die Policy festlegt, dass Fingerabdrücke für die Anmeldung erforderlich sind, und der Benutzer keine Fingerabdrücke registriert hat, hat er die Möglichkeit, Fingerabdrücke bei der Anmeldung zu registrieren. Wenn die Überprüfung von Fingerabdrücken erforderlich ist und kein Scanner angeschlossen ist, meldet UVM einen Fehler. Wenn das Windows-Kennwort nicht oder nicht richtig in UVM registriert ist, hat der Benutzer die Möglichkeit, das richtige Windows-Kennwort als Teil der Anmeldung anzugeben.
  - **UVM-Schutz bei der Anmeldung am System:** Client Security ermöglicht es Administratoren, den Zugriff auf Computer über eine Anmeldeschnittstelle zu steuern. Der UVM-Schutz stellt sicher, dass nur Benutzer, die von der Sicherheitspolicy erkannt werden, auf das Betriebssystem zugreifen können.

Beziehung zwischen Kennwörtern und Schlüsseln

Kennwörter und Schlüssel werden gemeinsam zum Überprüfen der Identität von Systembenutzern verwendet, zusammen mit anderen optionalen Authentifizierungsgeräten. Das Verständnis der Beziehung zwischen Kennwörtern und Schlüsseln ist wichtig, um die Funktionsweise von IBM Client Security zu verstehen.

Administratorkennwort

Das Administratorkennwort wird zur Authentifizierung des Administrators beim integrierten IBM Sicherheits-Subsystem verwendet. Dieses Kennwort, das acht Zeichen lang sein muss, wird innerhalb der sicheren Hardware des integrierten Sicherheits-Subsystems verwaltet und authentifiziert. Nach erfolgreicher Authentifizierung kann der Administrator folgende Aktionen ausführen:

- Benutzer registrieren
- Policy-Schnittstelle starten
- Administratorkennwort ändern

Das Administratorkennwort kann auf folgende Weise festgelegt werden:

- Über den Konfigurationsassistenten von IBM Client Security
- Über das Administratordienstprogramm
- Mit Hilfe von Scripts
- Über die BIOS-Schnittstelle (nur bei ThinkCentre-Computern)

Sie sollten eine Strategie für das Erstellen und Verwalten des Administratorkennworts festlegen. Das Administratorkennwort kann geändert werden, wenn es ausspioniert oder vergessen wurde.

Wenn Sie mit den Konzepten und der Terminologie der Trusted Computing Group (TCG) vertraut sind, ist Ihnen möglicherweise bekannt, dass das Administratorkennwort auch als "Eignerberechtigungswert" (Owner Authorization Value) bezeichnet wird. Da das Administratorkennwort mit dem integrierten IBM Sicherheits-Subsystem verknüpft ist, wird es manchmal auch als das *Hardwarekennwort* bezeichnet.

Öffentliche und private Hardwareschlüssel

Grundsätzlich kann zum integrierten IBM Sicherheits-Subsystem gesagt werden, dass er als *Root of Trust* auf einem Clientsystem fungiert. Diese Basis wird zur Sicherung der anderen Anwendungen und Funktionen verwendet. Dazu gehört auch das Erstellen eines öffentlichen und eines privaten Hardwareschlüssels. Öffentliche und private Schlüssel, auch als *Schlüsselpaare bezeichnet*, sind mathematisch in der Weise verknüpft:

- Daten, die mit dem öffentlichen Schlüssel verschlüsselt wurden, können nur mit dem zugehörigen privaten Schlüssel entschlüsselt werden.
- Daten, die mit dem privaten Schlüssel verschlüsselt wurden, können nur mit dem zugehörigen öffentlichen Schlüssel entschlüsselt werden.

Der private Hardwareschlüssel wird innerhalb der sicheren Hardwaregrenzen des Sicherheits-Subsystems erstellt, gespeichert und verwendet. Der öffentliche Hardwareschlüssel wird für verschiedene Zwecke öffentlich verfügbar gemacht (daher die Bezeichnung "öffentlicher Schlüssel"), wird aber niemals außerhalb der sicheren Hardwaregrenzen des Sicherheits-Subsystems exponiert. Die öffentlichen und privaten Schlüssel sind ein wichtiges Element in der IBM Schlüsselauslagerungshierarchie. Diese Hierarchie wird in einem der folgenden Abschnitte beschrieben.

Öffentliche und private Hardwareschlüssel können auf eine der folgenden Arten erstellt werden:

- Über den Konfigurationsassistenten von IBM Client Security
- Über das Administratordienstprogramm
- Mit Hilfe von Scripts

Wenn Sie mit den Konzepten und der Terminologie der Trusted Computing Group (TCG) vertraut sind, ist Ihnen möglicherweise bekannt, dass die öffentlichen und privaten Hardwareschlüssel auch als *SRK (Speicherbasisschlüssel, Storage Root Key)* bezeichnet werden.

Öffentliche und private Administratorschlüssel

Der öffentliche und der private Administratorschlüssel sind integraler Bestandteil der IBM Schlüsselauslagerungshierarchie. Sie ermöglichen außerdem das Sichern und Wiederherstellen von benutzerspezifischen Daten im Fall eines Systemplatinen- oder Festplattenfehlers.

Ein öffentlicher und ein privater Administratorschlüssel kann entweder für die einzelnen Systeme eindeutig sein oder für alle Systeme oder Systemgruppen gelten. Es ist wichtig zu beachten, dass diese Administratorschlüssel verwaltet werden müssen und dass das Vorhandensein einer Strategie der Verwendung eindeutiger bzw. bekannter Schlüssel entscheidend ist.

Öffentliche und private Administratorschlüssel können auf eine der folgenden Arten erstellt werden:

- Über den Konfigurationsassistenten von IBM Client Security
- Über das Administratordienstprogramm
- Mit Hilfe von Scripts

ESS-Archiv

Mit Hilfe der öffentlichen und privaten Administratorschlüssel können benutzerspezifische Daten gesichert und im Falle eines Systemplatinen- oder Festplattenfehlers wiederhergestellt werden.

Öffentliche und private Benutzerschlüssel

Das integrierte IBM Sicherheits-Subsystem erstellt öffentliche und private Benutzerschlüssel zum Schutz von benutzerspezifischen Daten. Diese Schlüsselpaare werden erstellt, wenn ein Benutzer bei IBM Client Security registriert wird. Diese Schlüssel werden transparent von der UVM-Komponente (User Verification Manager) von IBM Client Security erstellt und verwaltet. Die Verwaltung der Schlüssel erfolgt anhand der Anmeldung der einzelnen Windows-Benutzer am Betriebssystem.

IBM Schlüsselauslagerungshierarchie

Ein wesentlicher Bestandteil der Architektur des integrierten IBM Sicherheits-Subsystems ist die Schlüsselauslagerungshierarchie. Die Basis (oder ″Root″) der IBM Schlüsselauslagerungshierarchie sind der öffentliche und der private Hardwareschlüssel. Der öffentliche und der private Hardwareschlüssel, als *Hardwareschlüsselpaar* bezeichnet, werden von IBM Client Security erstellt und sind auf jedem Client statistisch eindeutig.

Die nächste “Ebene” der Hierarchie (über der Basis- oder Rootebene) ist das Schlüsselpaar des öffentlichen und des privaten Administratorschlüssels, auch als *Administratorschlüsselpaar* bezeichnet. Das Administratorschlüsselpaar kann auf jeder Maschine eindeutig sein, oder es kann für alle Clients oder für eine Untergruppe von Clients dasselbe sein. Wie dieses Schlüsselpaar verwaltet wird, hängt davon ab, wie Sie das Netzwerk verwalten möchten. Der private Administratorschlüssel ist insofern eindeutig, als er sich auf dem Clientsystem (geschützt durch den öffentlichen Hardwareschlüssel) an einer vom Administrator festgelegten Position befindet.

IBM Client Security registriert die Windows-Benutzer in der Umgebung des integrierten IBM Sicherheits-Subsystems. Wenn ein Benutzer registriert ist, werden ein öffentlicher und ein privater Schlüssel erstellt (das *Benutzerschlüsselpaar*), und eine neue ″Schlüsselebene″ wird erstellt. Der private Benutzerschlüssel ist mit dem öffentlichen Administratorschlüssel verschlüsselt. Der private Administratorschlüssel wird durch den öffentlichen Hardwareschlüssel verschlüsselt. Daher muss zur Verwendung des privaten Benutzerschlüssels der private Administratorschlüssel (der wiederum mit dem öffentlichen Hardwareschlüssel verschlüsselt ist) in das Sicherheits-Subsystem geladen werden. Nachdem der private Administratorschlüssel in den Chip geladen wurde, wird er durch den privaten Hardwareschlüssel entschlüsselt. Der private Administratorschlüssel ist nun für die Verwendung im Sicherheits-Subsystem bereit, so dass Daten, die mit dem entsprechenden öffentlichen Administatorschlüssel verschlüsselt wurden, in das Sicherheits-Subsystem ausgelagert, entschlüsselt und verwendet werden können. Der private (mit dem öffentlichen Administratorschlüssel verschlüsselte) Schlüssel des aktuellen Windows-Benutzers wird an das Sicherheits-Subsystem weitergeleitet. Alle von einer Anwendung benötigten Daten, die das integrierte Sicherheits-Subsystem einsetzt, werden ebenso an den Chip weitergeleitet, entschlüsselt und innerhalb der sicheren Umgebung des Sicherheits-Subsystems genutzt. Ein Beispiel für diesen Prozess ist ein privater Schlüssel, der für die Authentifizierung in einem festnetzunabhängigen Netz verwendet wird.

Wenn ein Schlüssel erforderlich ist, wird er in das Sicherheits-Subsystem geladen. Die verschlüsselten privaten Schlüssel werden in das Sicherheit-Subsystem geladen und können in der gesicherten Umgebung des Chips verwendet werden. Die privaten Schlüssel sind niemals ungeschützt; sie werden niemals außerhalb dieser Hardwareumgebung verwendet. Dadurch kann eine nahezu unbegrenzte Datenmenge mit Hilfe des integrierten IBM Security Chips geschützt werden.

Die privaten Schlüssel werden verschlüsselt, da für sie die höchste Sicherheitsstufe gilt und da im integrierten IBM Sicherheits-Subsystem nur eine begrenzte Speicherkapazität zur Verfügung steht. Es können immer nur einige Schlüssel zur gleichen Zeit im Sicherheits-Subsystem gespeichert werden. Die öffentlichen und privaten Hardwareschlüssel sind die einzigen Schlüssel, die auch zwischen den einzelnen Bootvorgängen im Sicherheits-Subsystem gespeichert bleiben. Damit mehrere Schlüssel und mehrere Benutzer zugelassen werden können, verwendet CSS die IBM Schlüsselauslagerungshierarchie. Wenn ein Schlüssel erforderlich ist, wird er

in das integrierte IBM Sicherheits-Subsystem geladen. Die zugehörigen, verschlüsselten privaten Schlüssel werden in das Sicherheits-Subsystem geladen und können in der gesicherten Umgebung des Chips verwendet werden. Die privaten Schlüssel sind niemals ungeschützt; sie werden niemals außerhalb dieser Hardwareumgebung verwendet.

Der private Administratorschlüssel wird durch den öffentlichen Hardwareschlüssel verschlüsselt. Der private Hardwareschlüssel, der nur im Sicherheits-Subsystem verfügbar ist, wird zum Entschlüsseln des privaten Administratorschlüssels verwendet. Nach dem Entschlüsseln des privaten Administratorschlüssels im Sicherheits-Subsystem kann ein privater Benutzerschlüssel (der mit dem öffentlichen Administratorschlüssel verschlüsselt wurde), in das Sicherheits-Subsystem geladen und mit dem privaten Administratorschlüssel entschlüsselt werden. Mit dem öffentlichen Administratorschlüssel können verschiedene private Benutzerschlüssel verschlüsselt werden. So kann virtuell eine unbegrenzte Benutzeranzahl auf einem System mit IBM ESS zugelassen werden; die Erfahrung hat jedoch gezeigt, das eine auf 25 Benutzer pro Computer beschränkte Registrierung optimale Leistung gewährleistet.

IBM ESS verwendet eine Schlüsselauslagerungshierarchie, bei der der öffentliche und der private Hardwareschlüssel im Sicherheits-Subsystem zum Sichern weiterer Daten, die außerhalb des Sicherheits-Subsystems gespeichert sind, verwendet werden können. Der private Hardwareschlüssel wird im Sicherheits-Subsystem generiert und verlässt nie diese sichere Umgebung. Der öffentliche Hardwareschlüssel ist außerhalb des Sicherheits-Subsystems verfügbar und wird zum Verschlüsseln oder Sichern von anderen Daten, wie z. B. der privaten Schlüssel, verwendet. Wenn diese Daten mit dem öffentlichen Hardwareschlüssel verschlüsselt werden, können sie nur mit dem privaten Hardwareschlüssel entschlüsselt werden. Da der private Hardwareschlüssel nur in der gesicherten Umgebung des Sicherheits-Subsystems verfügbar ist, können die verschlüsselten Daten nur in derselben gesicherten Umgebung entschlüsselt und verwendet werden. Beachten Sie, dass die einzelnen Computer jeweils über einen eindeutigen öffentlichen und privaten Schlüssel verfügen. Die Zufallszahlfunktion des integrierten IBM Sicherheits-Subsystems stellt sicher, dass jedes Hardwareschlüsselpaar statistisch eindeutig ist.

CSS PKI-Funktionen

Client Security bietet alle erforderlichen Komponenten, um in Ihrem Unternehmen eine PKI (Public Key Infrastructure) aufzubauen, z. B.:

- **Steuerung der Client-Sicherheitspolicy durch Administratoren:** Die Authentifizierung von Endbenutzern auf Clientebene ist ein wichtiger Aspekt für Sicherheitspolicies. Client Security bietet die erforderliche Schnittstelle zur Verwaltung der Sicherheitspolicy eines IBM Clients. Diese Schnittstelle ist Teil der Authentifizierungssoftware UVM (User Verification Manager), der Hauptkomponente von Client Security.
- **Chiffrierschlüsselverwaltung für öffentliche Schlüssel:** Administratoren können mit Client Security Chiffrierschlüssel für die Computerhardware und für die Clientbenutzer erstellen. Bei der Erstellung von Chiffrierschlüsseln sind diese über eine Schlüsselhierarchie an den integrierten IBM Security Chip gebunden. In der Hierarchie wird ein Hardwareschlüssel der Basisebene verwendet, um die übergeordneten Schlüssel sowie die den einzelnen Clientbenutzern zugeordneten Benutzerschlüssel zu verschlüsseln. Die Verschlüsselung und Speicherung von Schlüsseln auf dem integrierten IBM Security Chip erweitert die Clientsicherheit um eine wesentliche zusätzliche Ebene, da die Schlüssel sicher an die Computerhardware gebunden sind.

- **Erstellung und Speicherung digitaler Signaturen, die durch den integrierten IBM Security Chip geschützt sind:** Wenn Sie ein digitales Zertifikat anfordern, das für die digitale Unterschrift oder Verschlüsselung einer E-Mail verwendet werden kann, können Sie mit Hilfe von Client Security das integrierte IBM Sicherheits-Subsystem als CSP für Anwendungen auswählen, die Microsoft CryptoAPI verwenden. Zu diesen Anwendungen gehören Internet Explorer und Microsoft Outlook Express. Dadurch wird gewährleistet, dass der private Schlüssel des digitalen Zertifikats mit dem öffentlichen Benutzerschlüssel auf dem integrierten IBM Sicherheits-Subsystem verschlüsselt wird. Benutzer von Netscape können das integrierte IBM Sicherheits-Subsystem auch für das Generieren privater Schlüssel für digitale Zertifikate verwenden, die zur Erhöhung der Sicherheit verwendet werden. Anwendungen, die das PKCS#11-Modul (Public-Key Cryptography Standard) verwenden, wie z. B. Netscape Messenger, können den Schutz nutzen, den das integrierte IBM Sicherheits-Subsystem bietet.
- **Digitale Zertifikate auf das integrierte IBM Sicherheits-Subsystem übertragen:** Das Übertragungstool für Zertifikate von IBM Client Security ermöglicht Ihnen die Übertragung von Zertifikaten, die mit Hilfe des Standard-CSP-Moduls von Microsoft erstellt wurden, auf das CSP-Modul des integrierten IBM Sicherheits-Subsystems. Dadurch wird der Schutz für die den Zertifikaten zugeordneten privaten Schlüssel erheblich gesteigert, da diese nun sicher auf dem integrierten IBM Sicherheits-Subsystem gespeichert werden, und nicht mehr in der leicht zugänglichen Software.

  Anmerkung: Digitale Zertifikate, die durch das CSP-Modul des integrierten IBM Sicherheits-Subsystems geschützt werden, können nicht zu einem anderen CSP-Modul exportiert werden.
- **Funktion zur Schlüsselarchivierung und -wiederherstellung:** Eine wichtige PKI-Funktion ist das Erstellen eines Schlüsselarchivs, aus dem Schlüssel bei Verlust oder Beschädigung der Originalschlüssel wiederhergestellt werden können. IBM Client Security bietet eine Schnittstelle, über die Sie ein Archiv für Schlüssel und digitale Zertifikate erstellen können, die mit dem integrierten IBM Sicherheits-Subsystem erstellt wurden und über die Sie diese Schlüssel und Zertifikate nötigenfalls wiederherstellen können.
- **Verschlüsselung von Dateien und Ordnern:** Die Verschlüsselung von Dateien und Ordnern ermöglicht dem Benutzer das Ver- und Entschlüsseln von Dateien und Ordnern. So wird über die Sicherheitsmaßnahmen des CSS-Systems hinaus bereits eine höhere Stufe von Datensicherheit gewährleistet.
- **Authentifizierung über Fingerabdrücke:** IBM Client Security unterstützt das Lesegerät für Fingerabdrücke von Targus als PC-Karte oder über USB für die Authentifizierung. Client Security muss installiert sein, bevor die Einheitentreiber für das Targus-Lesegerät für Fingerabdrücke installiert werden, damit ein ordnungsgemäßer Betrieb gewährleistet ist.
- **Smartcard-Authentifizierung:** IBM Client Security unterstützt bestimmte Smartcards als Authentifizierungseinheiten. Client Security ermöglicht die Verwendung von Smartcards zur Authentifizierung als Token, d. h., es kann sich jeweils nur ein Benutzer authentifizieren. Jede Smartcard ist systemgebunden, wenn nicht der standortunabhängige Zugriff (Roaming) mit Berechtigungsnachweis verwendet wird. Wenn eine Smartcard erforderlich ist, erhöht dies die Systemsicherheit, da neben einem Kennwort, das möglicherweise ausspioniert werden kann, auch die Smartcard geliefert werden muss.

- **Standortunabhängiger Zugriff mit Berechtigungsnachweis:** Der standortunabhängige Zugriff mit Berechtigungsnachweis ermöglicht es einem autorisierten Benutzer, jedes System im Netzwerk genau wie die eigene Workstation zu verwenden. Wenn ein Benutzer berechtigt ist, UVM auf irgendeinem bei CSS registrierten Client zu verwenden, kann er seine persönlichen Daten in alle anderen registrierten Clients im Netzwerk mit standortunabhängigem Zugriff importieren. Die persönlichen Daten werden im CSS-Archiv und auf jedem Computer, in den sie importiert wurden, automatisch aktualisiert und verwaltet. Aktualisierungen dieser persönlichen Daten, wie z. B. neue Zertifikate oder Änderungen des Verschlüsselungstexts, werden sofort auf allen anderen Computer verfügbar, die über eine standortunabhängige Verbindung zum Netzwerk verfügen.
- **FIPS 140-1-Zertifizierung:** Client Security unterstützt FIPS 140-1-zertifizierte, verschlüsselte Bibliotheken. FIPS-zertifizierte RSA-BSAFE-Bibliotheken werden auf TCPA-Systemen verwendet.
- **Ablauf des Verschlüsselungstexts:** Client Security legt jeweils beim Hinzufügen eines Benutzers zu UVM einen benutzerspezifischen Verschlüsselungstext und eine Policy für das Ablaufen des Verschlüsselungstexts fest.

Kapitel 2. Dateien und Ordner verschlüsseln und entschlüsseln

Die Verschlüsselungstechnologie ermöglicht es Benutzern, schutzwürdige Daten auf dem Computer zu schützen. Durch das Verschlüsseln einer Datei wird sichergestellt, dass niemand auf die Informationen in der verschlüsselten Datei zugreifen kann, ohne die vorgegebenen Sicherheitsbestimmungen zu erfüllen. Durch das Verschlüsseln von Dateien können auch schutzwürdige Daten in Dateien, die über das Internet oder ein Netzwerk versendet werden, geschützt werden.

Mit IBM Client Security können Benutzer schutzwürdige Dateien und Ordner wie folgt verschlüsseln und entschlüsseln:

- **Verschlüsselung einzelner Dateien über die rechte Maustaste mit Hilfe von Client Security**

  Diese Funktion gehört zum Basisdownload von IBM Client Security.
- **Transparente Verschlüsselung von Dateien und Ordnern während des Betriebs mit Hilfe von IBM FFE (File and Folder Encryption, Verschlüsselung von Dateien und Ordnern)**

  Anmerkung: Damit diese Funktion aktiviert werden kann, muss das Dienstprogramm "IBM FFE" (IBM File and Folder Encryption) heruntergeladen werden. IBM Client Security muss *vor* der Installation des Dienstprogramms zur Verschlüsselung von Dateien und Ordnern installiert werden.

Verschlüsselung über die rechte Maustaste

Mit Hilfe der Basisfunktion für die Verschlüsselung über die rechte Maustaste können Benutzer mit Hilfe von Client Security mit der rechten Maustaste sensible Dateien schützen. Zum Verwenden dieser Funktion muss keine zusätzliche Software heruntergeladen werden. Mit dieser Funktion verschlüsselte Dateien weisen die folgenden Merkmale auf:

- Eine verschlüsselte Datei muss manuell vor jeder Verwendung entschlüsselt werden und nach Verwendung wieder manuell verschlüsselt werden, damit sie wieder geschützt ist. Die UVM-Policy muss bei jedem Ver- und Entschlüsseln der Datei aufgerufen werden. Durch diese Bestimmungen ist eine leistungsfähige, manuelle Steuerung der Ver- und Entschlüsselung der ausgewählten Dateien gegeben, doch ist dieser stringente Schutz weniger benutzerfreundlich, da Benutzer möglicherweise nicht jedes Mal zum Verwenden einer verschlüsselten Datei ein Kennwort, einen Fingerabdruck oder eine Smartcard liefern möchten.
- Die Dateien können im verschlüsselten Zustand an einen fernen Standort gesendet werden; sie können jedoch nur auf dem Computer entschlüsselt werden, der zum Verschlüsseln verwendet wurde, da die zum Verschlüsseln der Dateien verwendeten Schlüssel im integrierten IBM Sicherheits-Subsystem (IBM Embedded Security Subsystem) auf diesem Computer eindeutig sind.

Sie können Dateien im Kontextmenü mit der rechten Maustaste manuell ver- und entschlüsseln. Wenn Sie Dateien auf diese Weise verschlüsseln, wird an den Dateinamen die Erweiterung `.$enc$` angehängt.

Diese verschlüsselten Dateien können Sie anschließend auf fernen Servern sicher speichern. Sie bleiben so lange verschlüsselt und für Anwendungen nicht verfügbar, bis Sie sie mit der rechten Maustaste wieder entschlüsseln.

Transparente Verschlüsselung während des Betriebs (FFE-Verschlüsselung)

Die Funktion für die transparente Verschlüsselung während des Betriebs von Client Security wird durch Herunterladen des Dienstprogramms ″IBM FFE″ (File and Folder Encryption) aktiviert. Sie finden es auf der Website zu IBM Client Security. FFE bietet eine benutzerfreundlichere, transparentere Art der Verschlüsselung als die Basisverschlüsselungsfunktion von CSS über die rechte Maustaste. Die Verschlüsselung von Dateien und Ordnern über FFE kann ebenso über die rechte Maustaste aufgerufen werden. Mit FFE verschlüsselte Dateien weisen die folgenden Merkmale auf:

- Die UVM-Policy muss nur beim Start aufgerufen werden. Dies ermöglicht eine benutzerfreundlichere Art der Ver- und Entschlüsselung der ausgewählten Dateien, da es *nicht* erforderlich ist, für jede Verwendung einer verschlüsselten Datei einen Verschlüsselungstext, einen Fingerabdruck oder eine Smartcard zu liefern.
- Wenn eine Anwendung eine Datei öffnet, die über das Dienstprogramm ″FFE″ (File and Folder Encryption) verschlüsselt wurde, wird die Datei automatisch entschlüsselt. Wenn eine Datei, die mit Hilfe des Dienstprogramms ″FFE″ verschlüsselt wurde, gespeichert wird, wird sie automatisch verschlüsselt.
- Dateien, die mit dem Dienstprogramm ″FFE″ verschlüsselt wurden, können an einen fernen Standort gesendet werden. Sie werden jedoch im entschlüsselten Zustand gesendet.

Das Dienstprogramm zur Plattenüberprüfung wird möglicherweise bei einem Neustart nach dem Schützen oder nach dem Aufheben des Schutzes von Ordnern ausgeführt. Warten Sie, bis das System geprüft ist, bevor Sie den Computer verwenden.

Ein in UVM registrierter Benutzer, der das Dienstprogramm ″FFE″ heruntergeladen hat, kann einen Ordner auswählen, um den Ordner mit der rechten Maustaste zu schützen oder den Schutz aufzuheben. Dadurch kann er alle Dateien innerhalb des Ordners oder alle untergeordneten Teilordner verschlüsseln. Wenn Sie Dateien auf diese Weise schützen, wird an deren Namen keine Erweiterung angehängt. Wenn Sie mit einer Anwendung auf eine Datei im verschlüsselten Ordner zugreifen, wird diese entschlüsselt, in den Speicher geladen und erneut verschlüsselt, bevor Sie sie auf der Festplatte speichern.

Alle Windows-Operationen, die auf eine Datei in einem geschützten Ordner zuzugreifen versuchen, erhalten Zugriff auf die Daten in entschlüsselter Form. Durch diese Funktion wird die Verschlüsselung benutzerfreundlicher, da eine Datei nicht für jede Verwendung entschlüsselt oder bei jeder Beendigung eines Programms erneut verschlüsselt werden muss.

FFE-Ordnerverschlüsselungsstatus

Mit dem Dienstprogramm ″FFE″ (File and Folder Encrpytion, Verschlüsselung von Dateien und Ordnern) können Benutzer mit der rechten Maustaste sensible Dateien und Ordner schützen. Die Art des Datei- oder Ordnerschutzes hängt von der ursprünglichen Verschlüsselung der Datei bzw. des Ordners ab.

Ein Ordner kann sich in einem der folgenden Status befinden:

- **Ungeschützter Ordner**

  Weder dieser Ordner noch seine Teilordner noch einer seiner übergeordneten Ordner wurde geschützt. Der Benutzer erhält die Option, diesen Ordner zu schützen.

- **Geschützter Ordner**

  Ein geschützter Ordner kann sich in einem der folgenden drei Status befinden:

  – **Vom aktuellen Benutzer geschützt**

    Der aktuelle Benutzer schützt diesen Ordner. Alle enthaltenen Dateien werden verschlüsselt, einschließlich aller Dateien in Teilordnern. Der Benutzer erhält die Option, den Schutz dieses Ordners aufzuheben.

  – **Vom aktuellen Benutzer geschützter Teilordner eines Ordners**

    Der aktuelle Benutzer schützt einen der übergeordneten Ordner dieses Ordners. Alle Dateien werden verschlüsselt. Der aktuelle Benutzer erhält keine Optionen für die rechte Maustaste.

  – **Von einem anderen Benutzer geschützt**

    Ein anderer Benutzer schützt diesen Ordner. Alle enthaltenen Dateien werden verschlüsselt, einschließlich aller Dateien in Teilordnern, und sie sind für den aktuellen Benutzer nicht verfügbar. Der aktuelle Benutzer erhält keine Optionen für die rechte Maustaste.

- **Übergeordneter Ordner eines geschützten Ordners**

  Ein übergeordneter Ordner eines geschützten Ordners kann sich in einem der folgenden drei Status befinden:

  – **Enthält mindestens einen Teilordner, der vom aktuellen Benutzer geschützt wurde**

    Der aktuelle Benutzer schützt mindestens einen Teilordner. Alle Dateien in den verschlüsselten Teilordnern werden verschlüsselt. Der Benutzer erhält die Option, den übergeordneten Ordner zu schützen. Für alle Teilordner im übergeordneten Ordner muss der Schutz aufgehoben werden, bevor der übergeordnete Ordner geschützt werden kann.

  – **Enthält mindestens einen Teilordner, der von mindestens einem anderen Benutzer geschützt wurde**

    Mindestens ein anderer Benutzer schützt mindestens einen Teilordner. Alle Dateien in den verschlüsselten Teilordnern werden verschlüsselt und sind für den aktuellen Benutzer nicht verfügbar. Der aktuelle Benutzer erhält keine Optionen für die rechte Maustaste.

  – **Enthält Teilordner, die vom aktuellen Benutzer und von mindestens einem anderen Benutzer geschützt wurden**

    Sowohl der aktuelle Benutzer als auch mindestens ein anderer Benutzer schützen Teilordner. Der aktuelle Benutzer erhält keine Optionen für die rechte Maustaste.

- **Kritischer Ordner**

  Ein kritischer Ordner ist ein Ordner in einem kritischen Pfad und kann daher nicht geschützt werden. Es gibt die beiden folgenden kritischen Pfade: den Pfad von Windows und den Pfad von Client Security.

Jeder Status wird von der Option zum Schützen eines Ordners durch Klicken mit der rechten Maustaste unterschiedlich gehandhabt.

Hinweise zum Dienstprogramm ″FFE″ (File and Folder Encryption, Verschlüsselung von Dateien und Ordnern)

Die folgenden Informationen sind möglicherweise nützlich, wenn Sie bestimmte Funktionen des Dienstprogramms ″FFE″ durchführen.

Laufwerkbuchstabenschutz

Das IBM Dienstprogramm ″FFE″ kann ausschließlich zum Verschlüsseln von Dateien und Ordnern auf Laufwerk C verwendet werden. Dieses Dienstprogramm unterstützt keine Verschlüsselung auf anderen Festplattenpartitionen oder anderen physischen Laufwerken.

Geschützte Dateien und Ordner löschen

Damit sich keine sensiblen Dateien und Ordner ungeschützt im Papierkorb befinden, müssen Sie die Tastenkombination Umschalttaste+Entf verwenden, um geschützte Ordner und Dateien zu löschen. Durch diese Tastenkombination wird eine nicht an Bedingungen gebundene Löschoperation durchgeführt, und die gelöschten Dateien werden nicht im Papierkorb abgelegt.

Vor dem Upgrade von einer älteren Version des Dienstprogramms ″IBM FFE″

Laden Sie vor einem Upgrade von einer Version bis 2.0 des Dienstprogramms ″IBM FFE″ das ACL-Reparaturtool (ACL - Access Control List, Zugriffssteuerungsliste) von der Website ″IBM Security″ herunter, und wenden Sie es an. Dieses Reparaturdienstprogramm sollte verwendet werden, *bevor* eine FFE-Version vor 2.0 deinstalliert wird. Anderenfalls schlägt die Deinstallation möglicherweise fehl, und auf die betroffenen Dateien kann nicht zugegriffen werden.

Vor dem Deinstallieren des Dienstprogramms ″IBM FFE″

Heben Sie vor dem Deinstallieren des Dienstprogramms ″IBM FFE″ mit Hilfe dieses Dienstprogramms den Schutz für alle zuvor geschützten Dateien und Ordner auf.

Einschränkungen beim Dienstprogramm zur Verschlüsselung von Dateien und Ordnern (Dienstprogramm ″FFE″)

Das Dienstprogramm ″IBM FFE″ weist folgende Einschränkungen auf:

Einschränkungen beim Verschieben von geschützten Dateien und Ordnern

Das Dienstprogramm ″IBM FFE″ unterstützt folgende Aktionen nicht:

- Dateien und Ordner innerhalb geschützter Ordner verschieben
- Dateien oder Ordner zwischen geschützten und ungeschützten Ordnern verschieben

Wenn Sie versuchen, eine dieser nicht unterstützten Verschiebeoperationen durchzuführen, wird vom Betriebssystem eine Nachricht angezeigt, die besagt, dass der Zugriff verweigert wurde. Dies ist ein normaler Vorgang.

Die Nachricht besagt lediglich, dass diese Verschiebeoperation nicht unterstützt wird. Alternativ zur Verschiebeoperation können Sie folgende Operation ausführen:

1. Kopieren Sie die geschützten Dateien oder Ordner an die neue Position.
2. Löschen Sie die ursprünglichen Dateien oder Ordner mit Hilfe der Tastenkombination Umschalttaste+Entf.

Einschränkungen beim Ausführen von Anwendungen

Das Dienstprogramm ″IBM FFE″ unterstützt nicht das Ausführen von Anwendungen von einem geschützten Ordner aus. Die ausführbare Datei PROGRAMM.EXE kann z. B. nicht von einem geschützten Ordner aus ausgeführt werden.

Längenbeschränkungen für Pfadnamen

Wenn Sie versuchen, einen Ordner mit Hilfe des Dienstprogramms ″IBM FFE″ zu schützen oder eine Datei oder einen Ordner von einem ungeschützten Ordner in einen geschützten Ordner zu verschieben, erhalten Sie möglicherweise eine Nachricht des Betriebssystems, die besagt, dass ein oder mehrere Pfadnamen zu lang sind. Wenn Sie diese Nachricht erhalten, überschreitet der Pfadname einer/eines oder mehrerer Dateien oder Ordner die maximal zulässige Zeichenlänge. Beheben Sie den Fehler, indem Sie entweder die Ordnerstruktur neu anordnen, so dass der Pfad verkürzt wird, oder indem Sie Ordner- oder Dateinamen kürzen.

Fehler beim Schützen eines Ordners

Wenn Sie versuchen, einen Ordner zu schützen und eine Nachricht mit folgendem (oder ähnlichem) Inhalt angezeigt wird: `"Der Ordner kann nicht geschützt werden. Mindestens eine Datei ist in Gebrauch."`, überprüfen Sie Folgendes:

- Überprüfen Sie, ob eine der Dateien im Ordner derzeit verwendet wird.
- Wenn im Windows Explorer ein oder mehrere Teilordner eines Ordners, den Sie schützen möchten, angezeigt werden, stellen Sie sicher, dass der Ordner, den Sie zu schützen versuchen, hervorgehoben und aktiv ist und nicht einer der Teilordner.

Kapitel 3. Standortunabhängiger Zugriff mit Berechtigungsnachweis in CSS

Mit Hilfe des standortunabhängigen Zugriffs mit Berechtigungsnachweis von IBM Client Security können Berechtigungsnachweise von UVM-Benutzern auf allen Computern in einem Netzwerk verwendet werden, auf denen TCPA aktiviert ist. Dieses Netzwerk mit standortunabhängigem Zugriff ermöglicht Benutzern eine größere Flexibilität. Außerdem sind die Anwendungen für Benutzer in diesem Netzwerk auf allen Computern gleichermaßen verfügbar.

Voraussetzungen für den Netzbetrieb bei einem standortunabhängigen Zugriff mit Berechtigungsnachweis in CSS

Ein CSS-Netzwerk mit standortunabhängigem Zugriff mit Berechtigungsnachweis besteht aus folgenden erforderlichen Komponenten:

- Roaming-Server
- Roaming-Clients
- Gemeinsam genutztes, zugeordnetes Netzlaufwerk zum Speichern der UVM-Benutzerarchive

Anmerkung: Bei dem Roaming-Server und den Roaming-Clients handelt es sich einfach um Computer, für die TCPA aktiviert wurde, die über Administratorkennwörter verfügen und auf denen IBM Client Security ab Version 5.1 installiert ist.

Roaming-Server einrichten

Um ein CSS-Netzwerk mit standortunabhängigem Zugriff mit Berechtigungsnachweis zu konfigurieren, müssen Sie einen TCPA-Computer als Roaming-*Server* definieren (dieser wird als ″System A″ bezeichnet). Wenn die übrigen Computer beim Server mit standortunabhängigem Zugriff registriert sind, sind sie berechtigte bei CSS registrierte *Clients*. (Der erste registrierte Client wird als ″System B″ bezeichnet.)

Der Computer, den Sie als Roaming-Server definieren, kann ein ganz normaler Computer sein. Sie können für diese Funktion jeden beliebigen Computer verwenden, der Teil des Netzwerks mit standortunabhängigem Zugriff ist. Über den Roaming-Server wird nur bestimmt, welche Computer für den Zugriff auf das Netzwerk berechtigt sind. Nachdem ein Computer beim Roaming-Server registriert worden ist, ist er für Verbindungen zu allen Computern in diesem Netzwerk berechtigt.

Die Konfiguration eines Roaming-Netzwerks wird in zwei Schritten ausgeführt:

1. Konfigurieren Sie System A (Server), indem Sie Schlüssel, Archiv und Benutzer mit standortunabhängigem Zugriff erstellen.
2. Registrieren Sie System B und alle weiteren Computer als Roaming-Clients im CSS-Netzwerk mit standortunabhängigem Zugriff mit Berechtigungsnachweis.

Der Roaming-Server definiert das CSS-Netzwerk mit standortunabhängigem Zugriff mit Berechtigungsnachweis und leitet die Registrierung der Roaming-Clients ein; der wichtigste Bereich in einem CSS-Netzwerk mit standortunabhängigem

Zugriff mit Berechtigungsnachweis ist jedoch das zugeordnete Netzlaufwerk, auf dem die Benutzerarchive gespeichert werden. In diesem Archiv werden alle Aktualisierungen an den Benutzerberechtigungen gespeichert. Das Archiv sollte sich *nicht* auf dem Roaming-Server oder einem der Roaming-Clients befinden. Nach der Initialisierung der CSS-Clients wird der Roaming-Server wie alle anderen für CSS registrierten Clients verwendet.

Roaming-Server konfigurieren

Gehen Sie wie folgt vor, um einen Roaming-Server zu konfigurieren:

1. Starten Sie auf dem ausgewählten Computer die Administratorkonsole, und klicken Sie auf **Standortunabhängigen Zugriff mit Berechtigungsnachweis konfigurieren**. Wenn der Computer bereits für einen standortunabhängigen Zugriff konfiguriert ist, wählen Sie die Option **Dieses System als CSS-Roaming-Server rekonfigurieren** aus, klicken Sie auf **Weiter**, und klicken Sie anschließend auf **OK**.
2. Erstellen Sie den Ordner `c:\roaming` auf dem als Roaming-Server bestimmten Computer.
3. Starten Sie die Administratorkonsole, und wählen Sie die Option **Standortunabhängigen Zugriff mit Berechtigungsnachweis konfigurieren** aus.
4. Wählen Sie die Option **Dieses System als CSS-Roaming-Server konfigurieren** aus, und klicken Sie auf **Weiter**.
5. Klicken Sie auf **Konfigurieren**.
6. Wählen Sie Option **Neue Archivschlüssel erstellen** aus, und geben Sie den neuen Ordner für Schlüssel in das Feld ″Ordner für Archivschlüssel″ ein. Der Ordner für Archivschlüssel befindet sich im Ordner `c:\roaming`.
7. Wählen Sie aus, ob Sie ein vorhandenes Schlüsselpaar verwenden oder ein neues Schlüsselpaar erstellen möchten, und klicken Sie auf **Weiter**.
8. Geben Sie den Archivordner an, und klicken Sie auf **Weiter**.

   Anmerkung: Auf den Archivordner und den Ordner für Schlüssel muss von den anderen für Roaming registrierten Computern (Roaming-Clients) aus zugegriffen werden können. Das Verzeichnis `c:\roaming` muss als Netzlaufwerk zugeordnet sein.

   Wenn das Archiv zurzeit Dateien enthält, werden Sie auf der nächsten Seite des Assistenten aufgefordert anzugeben, wie mit den Dateien verfahren werden soll.
9. Klicken Sie auf **Fertig stellen**.

Clients beim Roaming-Server registrieren

Gehen Sie wie folgt vor, um einen Roaming-Client beim Roaming-Server zu registrieren:

1. Unmittelbar nachdem die Konfiguration des Roaming-Servers abgeschlossen ist, wird die Seite zum Konfigurieren des Netzwerks mit standortunabhängigem Zugriff mit Berechtigungsnachweis angezeigt. Wählen Sie die Option **Client-Registrierung aktivieren** aus, und klicken Sie auf **Weiter**.
2. Geben Sie den Namen des Benutzers auf System B mit Administratorberechtigung an, der die Clientregistrierung abschließen wird.
3. Geben Sie ein Kennwort aus acht Zeichen für diesen Benutzer ein, und bestätigen Sie es. (Dieser Schritt bedeutet nicht, dass der Benutzer für die Verwendung von UVM berechtigt wird. Dieser Schritt wird später ausgeführt.)

4. Wenn Sie den Client mit Hilfe des Benutzerkonfigurationsprogramms registrieren möchten, müssen Sie eine Administratorkonfigurationsdatei für diesen Benutzer erstellen. Bei diesem Vorgang wird eine Datei generiert, die diesem Benutzer eindeutig zugeordnet ist. Speichern Sie diese Datei in einer Position, auf die der Benutzer und System B zugreifen können.

   Anmerkung: Diese Datei muss nicht generiert werden, wenn Sie einen Client mit Hilfe des Administratordienstprogramms registrieren.
5. Geben Sie das Administratorkennwort für System B ein, und klicken Sie auf **Weiter**.
6. Wenn Sie eine Administratorkonfigurationsdatei erstellt haben, speichern Sie die Datei in einer Position, auf die der Benutzer und System B zugreifen können.

Nachdem Sie diese Vorgänge abgeschlossen haben, ist der Roaming-Server konfiguriert. Die Registrierung muss auf jedem Roaming-Client durchgeführt werden, bevor das Netzwerk mit standortunabhängigem Zugriff betriebsbereit ist.

Registrierungsprozess für Roaming-Clients durchführen

Nachdem die gesicherten Systeme in der Liste beim Roaming-Server registriert wurden, müssen Sie eine der folgenden Prozeduren auf den Client-Systemen durchführen. Der Roaming-Server muss aktiv und mit dem Archiv verbunden sein, damit Sie den Registrierungsprozess für die Roaming-Clients durchführen können.

Roaming-Clients mit Hilfe des Administratordienstprogramms registrieren

Gehen Sie wie folgt vor, um einen Roaming-Client mit Hilfe des Administratordienstprogramms zu registrieren:

1. Klicken Sie auf **Schlüsselkonfiguration**.
2. Klicken Sie auf **Nein** auf die Frage, ob Sie Schlüssel aus dem Archiv wiederherstellen möchten.
3. Wählen Sie die Option "System beim CSS-Roaming-Server registrieren" aus, und klicken Sie auf **Weiter**.
4. Geben Sie die von System A erstellte Archivposition ein, geben Sie das Systemregistrierungskennwort ein, das für diesen Benutzer auf System A definiert wurde, und klicken Sie auf **Weiter**.

   Der Registrierungsprozess nimmt ungefähr eine Minute in Anspruch.

Roaming-Clients mit Hilfe des Benutzerkonfigurationsprogramms registrieren

Gehen Sie wie folgt vor, um einen Roaming-Client mit Hilfe des Benutzerkonfigurationsprogramms zu registrieren:

1. Klicken Sie auf der Registerkarte "Benutzerkonfiguration" auf **Beim CSS-Roaming-Server registrieren**.
2. Wählen Sie die Administratorkonfigurationsdatei aus, die Sie auf System A erstellt haben, geben Sie das Systemregistrierungskennwort für diesen Benutzer auf System A ein, und klicken Sie dann auf **Weiter**.
3. Geben Sie die von System A erstellte Archivposition an, und klicken Sie auf **Weiter**.

   Der Registrierungsprozess nimmt ungefähr eine Minute in Anspruch.

Roaming-Clients mit Hilfe von Massenimplementierung (im Hintergrund) registrieren

Um einen Roaming-Client automatisch über Massenimplementierung zu registrieren, führen Sie die folgenden Schritte aus:

1. Erstellen Sie die Datei `csec.ini`. Weitere Informationen zum Erstellen einer .ini-Datei in CSS finden Sie im Installationshandbuch zu Client Security.
2. Fügen Sie im Abschnitt `csssetup` der Datei den Eintrag `"enableroaming=1"` hinzu. Dies bedeutet, dass der Computer als Roaming-Client registriert werden soll.
3. Fügen Sie im selben Abschnitt den Eintrag `"username=OPTION"` hinzu. Für diesen Wert gibt es drei Optionen:
   - **Option 1: Die Zeichenfolge `"[promptcurrent]"` - einschließlich der eckigen Klammern.** Diese Bezeichnung sollte verwendet werden, wenn eine .dat-Datei für den derzeit angemeldeten Benutzer auf dem Roaming-Server generiert wurde und der derzeitige Benutzer das Systemregistrierungskennwort kennt. Es wird ein Dialogfenster geöffnet, und der Benutzer wird aufgefordert, vor der Implementierung das Systemregistrierungskennwort (`sysregpwd`) einzugeben.
   - **Option 2: Die Zeichenfolge `"[current]"` - einschließlich der eckigen Klammern.** Diese Bezeichnung sollte verwendet werden, wenn für den derzeit angemeldeten Benutzer auf dem Server eine .dat-Datei generiert wurde. `sysregpwd` wird wie im nächsten Schritt beschrieben behandelt.
   - **Option 3: Ein tatsächlicher Benutzername, wie z. B. `"joseph"` .** Wenn ein solcher designierter Benutzername verwendet wird, muss die Datei `"joseph.dat"` zuvor durch den Roaming-Server generiert worden sein. Das Systemregistrierungskennwort (`sysregpwd`) wird in diesem Fall wie unter dem nächsten Punkt beschrieben behandelt.
4. Wenn die zuvor beschriebene Option 2 oder 3 verwendet wird, muss als weiterer Eintrag `"sysregpwd=SYSREGPW"` hinzugefügt werden. Hierbei handelt es sich um das achtstellige Systemregistrierungskennwort, das entweder dem aktuellen Benutzer (bei Implementierung der zweiten Option) oder dem designierten Benutzer (bei Implementierung der dritten Option) zugeordnet ist.
5. Um die Clientregistrierung abzuschließen, verbinden Sie den Computer über den Roaming-Server mit der Archivkonfiguration. Dieses Archiv wird in der Datei `csec.ini` benannt. Der Ordner für Schlüssel, der auf dem CSS-Roaming-Server mit Berechtigungsnachweis erstellt wurde, wird auch als Datei `csec.ini` bezeichnet.
6. Verschlüsseln Sie die Datei `csec.ini` über die Adminsitratorkonsole.

Beispiele für die Datei "csec.ini"

In den folgenden Beispielen werden eine `csec.ini-Datei` und deren Veränderung, je nachdem, welche Option für standortunabhängigen Berechtigungsnachweis ausgewählt wird, gezeigt. Es gibt folgende Optionen:

- **Keine Werte für standortunabhängigen Zugriff.** Diese Basisdatei ist nicht für standortunabhängigen Zugriff mit Berechtigungsnachweis aktiviert.
- **Option 1 für standortunabhängigen Zugriff.** Diese Datei ist für standortunabhängigen Zugriff unter Verwendung der Option 1 für die Clientregistrierung aktiviert. Der derzeitige Benutzer muss das Systemregistrierungskennwort vor der Implementierung angeben.
- **Option 2 für standortunabhängigen Zugriff.** Diese Datei ist für standortunabhängigen Zugriff unter Verwendung der Option 2 für die Clientregistrie-

rung aktiviert. Der derzeitige Benutzer muss die Benutzer-ID und das Systemregistrierungskennwort angeben, das in der .ini-Datei festgelegt ist.

- **Option 3 für standortunabhängigen Zugriff.** Diese Datei ist für standortunabhängigen Zugriff unter Verwendung der Option 3 für die Clientregistrierung aktiviert. Der Benutzer ist in der .ini-Datei festgelegt. Das Systemregistrierungskennwort für den festgelegten Benutzer muss in der .ini-Datei vorhanden sein.

Im Folgenden finden Sie Beispiele für vier verschiedene CSEC.INI-Dateien:

[CSSSetup]	**Option 1** [CSSSetup]	**Option 2** [CSSSetup]	Option 3 [CSSSetup]
suppw=bootup	suppw=bootup	suppw=bootup	suppw=bootup
hwpw=11111111	hwpw=11111111	hwpw=11111111	hwpw=11111111
newkp=1	newkp=1	newkp=1	newkp=1
keysplit=1	keysplit=1	keysplit=1	keysplit=1
kpl=c:\jgk	kpl=c:\\computer name\jgk, wo der Computer das Schlüsselpaar auf dem Roaming-Server gespeichert hat	kpl=c:\\computer name\jgk, wo der Computer das Schlüsselpaar auf dem Roaming-Server gespeichert hat	kpl=c:\\computer name\jgk, wo der Computer das Schlüsselpaar auf dem Roaming-Server gespeichert hat
kal=c:\jgk\archive	kal=c:\\computer name\archive, wo der Computer das Archiv auf dem Roaming-Server gespeichert hat	kal=c:\\computer name\archive, wo der Computer das Archiv auf dem Roaming-Server gespeichert hat	kal=c:\\computer name\archive, wo der Computer das Archiv auf dem Roaming-Server gespeichert hat
pub= c:\jk\admin.key	pub= c:\jk\admin.key	pub= c:\jk\admin.key	pub= c:\jk\admin.key
pri= c:\jk\private1.key	pri= c:\jk\private1.key	pri= c:\jk\private1.key	pri= c:\jk\private1.key
wiz=0	wiz=0	wiz=0	wiz=0
clean=0	**enableroaming=1** **username=** **[promptcurrent]** clean=0	**enableroaming=1** **username=** **[current]** **sysregpwd=12345678** clean=0	**enableroaming=1** **username=** **joseph** **sysregpwd=12345678** clean=0
[UVMEnrollment]	[UVMEnrollment]	[UVMEnrollment]	[UVMEnrollment]
enrollall=0	enrollall=0	enrollall=0	enrollall=0
enrollusers=1	enrollusers=1	enrollusers=1	enrollusers=1
user1=joseph	user1=joseph	user1=joseph	user1=joseph
user1uvmpw= q1234r	user1uvmpw=q1234r	user1uvmpw=q1234r	user1uvmpw=q1234r
user1winpw=	user1winpw=	user1winpw=	user1winpw=
user1domain=0	user1domain=0	user1domain=0	user1domain=0
user1ppchange=0	user1ppchange=0	user1ppchange=0	user1ppchange=0
user1ppexppolicy=0	user1ppexppolicy=0	user1ppexppolicy=0	user1ppexppolicy=0
user1ppexpdays= 184	user1ppexpdays=184	user1ppexpdays=184	user1ppexpdays=184
[UVMAppConfig]	[UVMAppConfig]	[UVMAppConfig]	[UVMAppConfig]
uvmlogon=0	uvmlogon=0	uvmlogon=0	uvmlogon=0
entrust=0	entrust=0	entrust=0	entrust=0
notes=0	notes=0	notes=0	notes=0
netscape=0	netscape=0	netscape=0	netscape=0

passman=0	passman=0	passman=0	passman=0
folderprotect=0	folderprotect=0	folderprotect=0	folderprotect=0
autoprotect=0	autoprotect=0	autoprotect=0	autoprotect=0

Netzwerk mit standortunabhängigem Zugriff verwalten

Der Netzadministrator eines Netzwerks mit standortunabhängigem Zugriff muss die Benutzer autorisieren und den Benutzer- und den Client-Zugriff auf das Netz verwalten. Dazu gehört z. B. das Importieren eines Benutzerprofils, das Synchronisieren von Benutzerdaten oder das Hinzufügen und Entfernen von Benutzern und Clients. Diese Vorgänge können im CSS-Netzwerk mit standortunabhängigem Zugriff auf einfache Weise ausgeführt werden. Auch Aufgaben wie das Wiederherstellen des Netzwerks mit standortunabhängigem Zugriff, das Ändern des Administratorschlüsselpaars oder das Ändern der Archivposition können anfallen.

Benutzer autorisieren

Nachdem Sie diese Schritte abgeschlossen haben, ist das CSS-Netzwerk mit standortunabhängigem Zugriff mit Berechtigungsnachweis konfiguriert und die Roaming-Clients sind für den standortunabhängigen Zugriff registriert. Nun können Benutzer mit Hilfe des Administratordienstprogramms autorisiert werden.

Benutzerdaten synchronisieren

Die Daten der einzelnen Benutzer werden in der Archivposition gespeichert. Eine Kopie dieser Daten wird außerdem lokal auf allen Computern gespeichert, die der Benutzer für einen standortunabhängigen Zugriff verwendet hat. Wenn Änderungen vorgenommen werden, wie z. B. das Abrufen eines Zertifikats oder das Ändern eines Verschlüsselungstextes, werden die lokalen Daten aktualisiert. Wenn der Computer über eine Verbindung zum Archiv verfügt, werden die Benutzerdaten ebenfalls aktualisiert. Wenn sich der Benutzer auf einem anderen Computer anmeldet, werden die Aktualisierungen automatisch auf diesen Computer heruntergeladen, vorausgesetzt, der Computer verfügt ebenfalls über eine Verbindung zum Archiv.

Eine Verbindung zum Archiv kann jedoch nicht immer gewährleistet werden, d. h., dass die Benutzerdaten auf den Computern und im Archiv möglicherweise nicht konsistent sind. Wenn die Benutzerdaten auf einem Computer geändert werden, der nicht mit dem Archiv verbunden ist, werden diese Änderungen im Archiv und demzufolge auch auf den anderen Computern nicht übernommen. Wenn der Computer eine Verbindung zum Archiv herstellt, werden die Änderungen im Archiv aktualisiert, und die Dateninkonsistenzen auf allen anderen Computern, zu denen eine Verbindung besteht, werden behoben. Wenn jedoch Änderungen auf einem anderen Computer mit einer Verbindung zum Archiv vorgenommen werden, bevor der erste Computer, auf dem Änderungen vorgenommen wurden, eine Verbindung zum Archiv herstellen kann, entsteht eine nicht behebbare Dateninkonsistenz. Die Daten im Archiv enthalten Änderungen, die auf dem ersten Computer nicht vorhanden sind, während dieser Computer Änderungen enthält, die nicht im Archiv gespeichert wurden. Wenn dieser Fall eintritt, wird der Benutzer benachrichtigt, dass zwei unterschiedliche Konfigurationen vorhanden sind. Er wird aufgefordert, die Konfiguration auszuwählen, die er übernehmen möchte, die lokale oder die archivierte Konfiguration. Die Änderungen in der Konfiguration, die nicht ausgewählt wird, gehen verloren. Aus diesem Grund ist es wichtig, sicherzustellen, dass alle Änderungen in einer Benutzerkonfiguration im Archiv ebenfalls aktualisiert werden, bevor Änderungen auf einem anderen Computer vorgenommen werden.

Verloren gegangenen Verschlüsselungstext in einer Umgebung mit standortunabhängigem Zugriff wiederherstellen

Wenn ein Verschlüsselungstext verloren geht oder vergessen wird, kann der Administrator den Verschlüsselungstext des Benutzers auf dem Roaming-Server oder auf einem registrierten Client zurücksetzen. Diese Änderung wird auf allen Systemen im Netzwerk aktualisiert, *außer* auf den Systemen, die der Benutzer importiert hat, um den sicheren UVM-Anmeldeschutz zu aktivieren. In diesen Fällen wird die Aktualisierung des Verschlüsselungstextes *nicht* auf dem Computer dargestellt. Damit der Benutzer auf den Computer zugreifen kann, braucht er eine Datei zum Überschreiben des Verschlüsselungstextes und muss einen Prozess zum Überschreiben des Verschlüsselungstextes durchführen.

Benutzerprofil importieren

Sie können ein Benutzerprofil auf einen neuen Computer im Netzwerk mit standortunabhängigem Zugriff mit Hilfe des Administratordienstprogramms, des Benutzerkonfigurationsprogramms oder mit UVM GINA importieren. Wenn Sie einen Benutzer importieren möchten, der auf dem neuen Computer über keinen Benutzeraccount verfügt, müssen Sie über die Windows-Systemsteuerung einen Windows-Benutzeraccount erstellen.

Anmerkung: Damit ein Benutzer in ein Netzwerk mit standortunabhängigem Zugriff importiert werden kann, muss dieser Benutzer auf einem anderen Computer in diesem Netzwerk autorisiert sein.

Benutzerprofil mit Hilfe des Benutzerkonfigurationsprogramms importieren

Um ein Benutzerprofil mit Hilfe des Benutzerkonfigurationsprogramms auf einen neuen Computer im Netzwerk mit standortunabhängigem Zugriff zu importieren, melden Sie sich als der Benutzer, der importiert werden soll, an, klicken Sie auf **Start > Programme > Access IBM > IBM Client Security > Sicherheitseinstellungen ändern**, und klicken Sie dann auf der Registerkarte "Benutzerkonfiguration" auf **Vorhandene Konfiguration aus Archiv importieren**.

Benutzerprofil mit Hilfe des Administratordienstprogramms importieren

Um ein Benutzerprofil mit Hilfe des Administratordienstprogramms auf einen neuen Computer im Netzwerk mit standortunabhängigem Zugriff zu importieren, wählen Sie den Benutzer aus, und klicken Sie auf **Berechtigen**. Klicken Sie auf **Ja** auf die Frage, ob Sie den Benutzer aus dem Archiv importieren möchten.

Benutzerprofil mit Hilfe von UVM GINA importieren

Sie können ein Benutzerprofil auf einen neuen Computer in einem Netzwerk mit standortunabhängigem Zugriff mit Hilfe von UVM GINA importieren. Dieser Prozess wird von der UVM-Anmeldeanzeige aus gestartet. Wenn ein Benutzer noch nicht für die Verwendung von UVM auf einem System in dem Netzwerk autorisiert ist, wird eine entsprechende Nachricht mit der Frage angezeigt, ob der Benutzer aus dem Archiv importiert werden soll.

Anmerkungen:

1. Wenn Sie einen Benutzer importieren möchten, der auf dem neuen Computer über keinen Benutzeraccount verfügt, müssen Sie über die Windows-Systemsteuerung einen Windows-Benutzeraccount erstellen, bevor Sie fortfahren können.
2. Damit Sie auf das Archiv auf dem Roaming-Server zugreifen können, muss es sich bei dem Verzeichnis um ein zugeordnetes Netzlaufwerk handeln.

Gehen Sie wie folgt vor, um auf einem Computer mit Windows 2000 ein Benutzerprofil mit UVM-GINA aus dem Archiv auf einen neuen Computer im Netzwerk mit standortunabhängigem Zugriff zu importieren:

1. Geben Sie bei der Anmeldung den Benutzernamen und den UVM-Verschlüsselungstext des Benutzers ein, der importiert werden soll. Eine Nachricht mit der Frage, ob Sie das Benutzerprofil aus dem Archiv importieren möchten, wird angezeigt.
2. Klicken Sie an der Eingabeaufforderung auf **Ja**, um den Benutzer zu importieren, und klicken Sie dann auf **OK**.
3. Wenn sich die Archivposition auf einem Netzlaufwerk befindet, klicken Sie bei der Eingabeaufforderung, die besagt, das ein gemeinsam benutztes Netzwerk angegeben werden muss, auf **Ja**.
4. Geben Sie in der Standard-Anmeldeanzeige von Windows das Windows-Kennwort ein. Daraufhin wird eine Eingabeaufforderung für den Archivpfad angezeigt.
5. Geben Sie den Archivnetzpfad ein.
6. Geben Sie den Benutzernamen und das Kennwort für den Netzpfad ein.
7. Klicken Sie auf **OK**. Wenn die Operation ordnungsgemäß durchgeführt wurde, wird eine Nachricht angezeigt, die besagt, dass das Profil erfolgreich importiert wurde.

Gehen Sie wie folgt vor, um auf einem Computer mit Windows XP ein Benutzerprofil mit UVM-GINA aus dem Archiv auf einen neuen Computer im Netzwerk mit standortunabhängigem Zugriff zu importieren:

1. Geben Sie bei der Anmeldung den Benutzernamen und den UVM-Verschlüsselungstext des Benutzers ein, der importiert werden soll. Eine Nachricht mit der Frage, ob Sie das Benutzerprofil aus dem Archiv importieren möchten, wird angezeigt.
2. Klicken Sie an der Eingabeaufforderung auf **Ja**, um den Benutzer zu importieren, und klicken Sie dann auf **OK**.
3. Wenn sich die Archivposition auf einem Netzlaufwerk befindet, klicken Sie bei der Eingabeaufforderung, die besagt, das ein gemeinsam benutztes Netzwerk angegeben werden muss, auf **Ja**.
4. Geben Sie an der Standard-Eingabeaufforderung von Windows zum Zuordnen eines Netzlaufwerks den Archivnetzpfad ein.
5. Klicken Sie auf **Fertig stellen**.
6. Geben Sie den Benutzernamen und das Kennwort für den Netzpfad ein, und klicken Sie auf **OK**. Wenn die Operation ordnungsgemäß durchgeführt wurde, wird eine Nachricht angezeigt, die besagt, dass das Profil erfolgreich importiert wurde.

Anmerkung: Damit ein Benutzer in ein Netzwerk mit standortunabhängigem Zugriff importiert werden kann, muss dieser Benutzer auf einem anderen Computer in diesem Netzwerk autorisiert sein.

Nach dem Importieren des Benutzerprofils wird die Authentifizierung mit UVM entsprechend der auf diesem Computer definierten Sicherheitspolicy durchgeführt. Der Benutzer muss über die Sicherheitsbestimmungen für diesen Computer informiert werden, bevor er sich anmelden kann.

Benutzer aus einem Netzwerk mit standortunabhängigem Zugriff entfernen und wiederherstellen

Zum Entfernen eines Benutzers aus einem Netzwerk mit standortunabhängigem Zugriff muss der Netzadministrator die folgende Prozedur in der Administratorkonsole durchführen:

1. Starten Sie die Administratorkonsole, und geben Sie das Administratorkennwort ein.
2. Klicken Sie auf die Option **Standortunabhängigen Zugriff mit Berechtigungsnachweis konfigurieren**.
3. Wählen Sie die Option **Benutzer von UVM und dem Netzwerk mit standortunabhängigem Zugriff mit Berechtigungsnachweis entfernen** aus, und klicken Sie auf **Weiter**. Wiederholen Sie, je nach Bedarf, die Prozedur.
4. Wählen Sie den zu entfernenden Benutzer aus, und klicken Sie auf **Entfernen**.

   Anmerkung: Wenn ein Benutzer aus dem Netz entfernt wurde, gehen alle Berechtigungsnachweise dieses Benutzers dauerhaft verloren.

Entfernte Benutzer können erst wieder zur Verwendung von UVM und des Netzwerks mit standortunabhängigem Zugriff autorisiert werden, wenn Sie vom Netzadministrator wiederhergestellt werden.

Zum Wiederherstellen eines Benutzers in einem Netzwerk mit standortunabhängigem Zugriff muss der Netzadministrator die folgende Prozedur in der Administratorkonsole durchführen:

1. Starten Sie die Administratorkonsole, und geben Sie das Administratorkennwort ein.
2. Klicken Sie auf die Option **Standortunabhängigen Zugriff mit Berechtigungsnachweis konfigurieren**.
3. Wählen Sie die Option **Entfernte Benutzer wiederherstellen** aus, und klicken Sie auf **Weiter**.
4. Wählen Sie den Benutzer aus, der wiederhergestellt werden soll, und klicken Sie auf **Wiederherstellen**. Wiederholen Sie, je nach Bedarf, die Prozedur.

   Wenn der Benutzer wiederhergestellt ist, kann er erneut für UVM autorisiert werden. Durch das Wiederherstellen eines Benutzers allein ist der Benutzer jedoch nicht automatisch für die Verwendung von UVM autorisiert.

Registrierte Clients aus einem Netzwerk mit standortunabhängigem Zugriff entfernen und wiederherstellen

Zum Entfernen eines registrierten Clients aus einem Netzwerk mit standortunabhängigem Zugriff muss der Netzadministrator die folgende Prozedur in der Administratorkonsole durchführen:

1. Starten Sie die Administratorkonsole, und geben Sie das Administratorkennwort ein.
2. Klicken Sie auf die Option **Standortunabhängigen Zugriff mit Berechtigungsnachweis konfigurieren**.
3. Wählen Sie die Option **Registrierte Clients aus dem Netzwerk mit standortunabhängigem Zugriff mit Berechtigungsnachweis entfernen** aus, und klicken Sie auf **Weiter**.
4. Wählen Sie das zu entfernende System aus, und klicken Sie auf **Entfernen**. Wiederholen Sie, je nach Bedarf, die Prozedur.

Anmerkung: Wenn ein Client aus dem Netz entfernt wurde, gehen alle systembasierten Berechtigungsnachweise dieses Systems dauerhaft verloren.

Entfernte Clients können erst beim Roaming-Server des Servers registriert werden, wenn Sie vom Netzadministrator wiederhergestellt wurden.

Zum Wiederherstellen eines registrierten Clients in einem Netzwerk mit standortunabhängigem Zugriff muss der Netzadministrator die folgende Prozedur in der Administratorkonsole durchführen:

1. Starten Sie die Administratorkonsole, und geben Sie das Administratorkennwort ein.
2. Klicken Sie auf die Option **Standortunabhängigen Zugriff mit Berechtigungsnachweis konfigurieren**.
3. Wählen Sie die Option **Entfernte Clients wiederherstellen** aus, und klicken Sie auf **Weiter**.
4. Wählen Sie den Client aus, der wiederhergestellt werden soll, und klicken Sie auf **Wiederherstellen**. Wiederholen Sie, je nach Bedarf, die Prozedur.

   Wenn der Client wiederhergestellt wurde, kann er erneut beim Roaming-Server registriert werden. Durch das Wiederherstellen eines Clients ist dieser noch nicht automatisch erneut registriert.

Anmerkung: Alle Benutzer, deren Berechtigungsnachweise auf dem System gespeichert waren, als der Client entfernt wurde, müssen ihre Berechtigungsnachweise möglicherweise erneut importieren.

Zugriffsberechtigung für registrierte Clients in einem Netzwerk mit standortunabhängigen Zugriff entziehen

Manchmal möchte ein Netzadministrator möglicherweise für manche Benutzer den Zugriff auf einen bestimmten registrierten Client zulassen, während er anderen Benutzern den Zugriff entziehen möchte.

Zum Verwalten der Zugriffsberechtigungen von Benutzern muss der Netzadministrator die folgende Prozedur in der Administratorkonsole durchführen:

1. Starten Sie die Administratorkonsole, und geben Sie das Administratorkennwort ein.
2. Klicken Sie auf die Option **Standortunabhängigen Zugriff mit Berechtigungsnachweis konfigurieren**.
3. Wählen Sie die Option **Benutzerzugriff auf registrierte Clients verwalten** aus, und klicken Sie auf **Weiter**.
4. Wählen Sie den registrierten Client, der verwaltet werden soll, im Feld **Wählen Sie ein System im CSS-Netzwerk mit standortunabhängigem Zugriff mit Berechtigungsnachweis aus** aus. Benutzer mit und ohne Zugriffsberechtigung sind in den beiden Listenfenstern aufgeführt.
5. Führen Sie einen der folgenden Schritte aus:
   - Um einem Benutzer den Zugriff zu entziehen, wählen Sie den Benutzer aus der Liste **Benutzer mit Zugriff** aus, und klicken Sie auf **Entziehen**. Wiederholen Sie, je nach Bedarf, die Prozedur.
   - Um den Zugriff für einen Benutzer ohne Zugriffsberechtigung zuzulassen, wählen Sie den Benutzer aus der Liste **Benutzer ohne Zugriff** aus, und klicken Sie auf **Zulassen**. Wiederholen Sie, je nach Bedarf, die Prozedur.

Für die Zugriffsmanagementfunktionen des Netzwerks mit standortunabhängigem Zugriff muss im Archiv ein neuer Ordner erstellt werden. Der neue Ordner mit der Bezeichnung "Geschützt" muss Schreibzugriff für den Netzadministrator und Lesezugriff für andere Benutzer aufweisen. Wenn Benutzer über Schreibzugriff auf diesen Ordner verfügen, können sie sich selbst oder ihr System manuell wiederherstellen.

Netzwerk mit standortunabhängigem Zugriff wiederherstellen

Im Falle eines Software- oder Hardwarefehlers muss das Netzwerk mit standortunabhängigem Zugriff möglicherweise wiederhergestellt werden. Wenn ein Fehler am Roaming-Server vorliegt oder die von CSS verwendeten Daten auf einem registrierten Client beschädigt sind, stellen Sie die Daten mit Hilfe des Administratordienstprogramms auf die gleiche Weise wieder her, wie Sie es bei einer normalen Netzwerkumgebung tun würden. Wurde das integrierte IBM Sicherheits-Subsystem auf einem registrierten Client beschädigt oder gelöscht, muss der Client erneut beim Roaming-Server registriert werden. Es ist keine weitere Maßnahme erforderlich.

Administratorschlüsselpaar ändern

Es ist nicht empfehlenswert, das Administratorschlüsselpaar in einem Netzwerk mit standortunabhängigem Zugriff zu ändern.

Um ein Administratorschlüsselpaar in einem Netzwerk mit standortunabhängigem Zugriff zu ändern, müssen Sie folgende Schritte ausführen, damit die Änderung an alle Computer im Netzwerk weitergeleitet wird.

1. Ändern Sie auf dem Roaming-Server das Administratorschlüsselpaar mit Hilfe des Administratordienstprogramms.
2. Registrieren Sie alle Clients im Netzwerk erneut.
3. Speichern bzw. übernehmen Sie bei allen entsprechenden Eingabeaufforderungen die vorhandenen Dateien.

Archivordner ändern

Die Vorgehensweise zum Ändern des Archivordners in einer Umgebung mit standortunabhängigem Zugriff unterscheidet sich etwas von der in einer anderen Umgebung, da die einzelnen Computer im Netzwerk auf dieselbe Archivposition zugreifen.

Gehen Sie wie folgt vor, um den Archivordner in einem Netzwerk mit standortunabhängigem Zugriff zu ändern:

1. Kopieren Sie die Dateien aus dem alten Archivordner folgendermaßen in den neuen:
   a. Starten Sie das Administratordienstprogramm, und geben Sie das Administratorkennwort ein.
   b. Klicken Sie auf **Schlüsselkonfiguration**.
   c. Wählen Sie die Option "Archivposition ändern" aus, und klicken Sie auf **Weiter**.
   d. Geben Sie den neuen Archivordner ein, und klicken Sie dann auf **Weiter**.
   e. Klicken Sie auf **Ja**, wenn Sie aufgefordert werden, alle Dateien aus dem alten Ordner in den neuen zu kopieren.

2. Aktualisieren Sie alle übrigen Computer im Netzwerk mit dem neuen Archivordner; gehen Sie dazu wie folgt vor:
   a. Starten Sie das Administratordienstprogramm, und geben Sie das Administratorkennwort ein.
   b. Klicken Sie auf **Schlüsselkonfiguration**.
   c. Wählen Sie die Option "Archivposition ändern" aus, und klicken Sie auf **Weiter**.
   d. Geben Sie den neuen Archivordner ein, und klicken Sie dann auf **Weiter**.
   e. Klicken Sie auf **Nein** auf die Frage, ob Sie alle Dateien vom alten in den neuen Ordner kopieren möchten.

FFE (File and Folder Encryption)

Die FFE-Funktionalität (File and Folder Encryption, Verschlüsselung von Dateien und Ordnern) ist in einer Umgebung mit standortunabhängigem Zugriff nicht beeinträchtigt. Geschützte Ordner werden jedoch auf den einzelnen Computern gesondert verwaltet. Wenn z. B. ein Ordner von Benutzer A auf System A geschützt wird, ist ein Ordner mit demselben Namen auf System B - falls ein solches vorhanden ist - nicht geschützt, es sei denn, der Benutzer schützt diesen Ordner ebenfalls explizit auf System B.

IBM Password Manager

Alle mit Hilfe von IBM Password Manager geschützten Kennwörter sind auf allen Computern im Netzwerk mit standortunabhängigem Zugriff verfügbar.

Begriffe und Begriffsbestimmungen in Bezug auf standortunabhängigen Zugriff

Im Hinblick auf die Konzepte und Prozeduren in Verbindung mit der Konfiguration eines Netzwerks mit standortunabhängigem Zugriff ist es nützlich, die Definitionen der folgenden Begriffe zu kennen:

Registrierung für Roaming-Clients
Das Registrieren eines Computers auf dem Roaming-Server.

Roaming-Clients
Alle gesicherten TCPA-Computer in dem Netzwerk mit standortunabhängigem Zugriff.

Roaming-Server
Der TCPA-Computer, der für die Initialisierung des Netzwerks mit standortunabhängigem Zugriff verwendet wird.

Kennwort für Roaming-Client-Registrierung
Das Kennwort zum Registrieren des Computers auf dem Roaming-Server.

Kapitel 4. Anweisungen für den Clientbenutzer

Hier finden Sie Informationen zu den folgenden Tätigkeiten von Clientbenutzern:

- UVM-Schutz für die Anmeldung am System verwenden
- Benutzerkonfigurationsprogramm verwenden
- E-Mails sicher versenden und im World Wide Web sicher navigieren
- Einstellungen für UVM-Signaltöne konfigurieren

UVM-Schutz für die Anmeldung am System verwenden

In diesem Abschnitt finden Sie Informationen zur Verwendung der gesicherten UVM-Anmeldung für die Anmeldung am System. Bevor Sie den UVM-Schutz verwenden können, muss dieser für den Computer aktiviert sein.

Mit dem UVM-Schutz können Sie den Zugriff auf das Betriebssystem über eine Anmeldeschnittstelle steuern. Die gesicherte UVM-Anmeldung ersetzt die Anmeldeanwendung von Windows, so dass sich beim Entsperren des Computers durch einen Benutzer statt des Windows-Anmeldefensters das UVM-Anmeldefenster öffnet. Wenn der UVM-Schutz für den Computer aktiviert ist, wird die UVM-Anmeldeschnittstelle beim Start des Computers aufgerufen.

Während das System aktiv ist, können Sie die UVM-Anmeldeschnittstelle mit der Tastenkombination **Strg+Alt+Entf** aufrufen, um damit den Computer herunterzufahren, zu sperren, den Task-Manager zu öffnen oder den aktuellen Benutzer abzumelden.

Client entsperren

Einen Windows-Client mit aktiviertem UVM-Schutz können Sie folgendermaßen entsperren:

1. Drücken Sie die Tastenkombination **Strg+Alt+Entf**, um auf die UVM-Anmeldeschnittstelle zuzugreifen.
2. Geben Sie den Benutzernamen und die Domäne ein, an der Sie angemeldet sind, und klicken Sie anschließend auf **Entsperren**.

   Das Fenster "UVM-Verschlüsselungstext" wird geöffnet.

   Anmerkung: Obwohl UVM mehrere Domänen erkennt, muss das Benutzerkennwort für alle Domänen übereinstimmen.
3. Geben Sie den UVM-Verschlüsselungstext ein, und klicken Sie anschließend auf **OK**, um auf das Betriebssystem zuzugreifen.

Anmerkungen:

1. Wenn der UVM-Verschlüsselungstext für den eingegebenen Benutzernamen und für die eingegebene Domäne nicht der richtige ist, wird das UVM-Anmeldefenster erneut geöffnet.
2. Je nach den Authentifizierungsbestimmungen der UVM-Policy für den Client kann möglicherweise eine weiter reichende Authentifizierung erforderlich sein.

Benutzerkonfigurationsprogramm

Das Benutzerkonfigurationsprogramm ermöglicht es den Clientbenutzern, verschiedene Vorgänge zum Verwalten der Systemsicherheit auszuführen, für die keine Administratorberechtigungen erforderlich sind.

Funktionen des Benutzerkonfigurationsprogramms

Das Benutzerkonfigurationsprogramm bietet Clientbenutzern folgende Möglichkeiten:

- **Kennwörter und Archiv aktualisieren.** Auf dieser Registerkarte können die folgenden Funktionen ausgeführt werden:
  - **Den UVM-Verschlüsselungstext ändern:** Zum Erhöhen der Sicherheit können Sie den UVM-Verschlüsselungstext regelmäßig ändern.
  - **Windows-Kennwort aktualisieren:** Wenn Sie das Windows-Kennwort für einen UVM-berechtigten Clientbenutzer mit dem Benutzerverwaltungsprogramm von Windows ändern, müssen Sie das betreffende Kennwort auch über das Benutzerkonfigurationsprogramm von IBM Client Security ändern. Wenn ein Administrator das Administratordienstprogramm zum Ändern des Windows-Anmeldekennworts für einen Benutzer verwendet, werden alle zuvor für diesen Benutzer erstellten Chiffrierschlüssel gelöscht, und die zugeordneten digitalen Zertifikate werden ungültig.
  - **Lotus Notes-Kennwort zurücksetzen:** Zur Erhöhung der Sicherheit können Lotus Notes-Benutzer ihr Notes-Kennwort ändern.
  - **Das Schlüsselarchiv aktualisieren:** Wenn Sie digitale Zertifikate erstellen und von den privaten Schlüsseln, die auf dem integrierten IBM Security Chip gespeichert sind, Kopien erstellen möchten, oder wenn Sie das Schlüsselarchiv an eine andere Position versetzen möchten, aktualisieren Sie das Schlüsselarchiv.
- **Einstellungen für UVM-Signaltöne konfigurieren:** Mit dem Benutzerkonfigurationsprogramm können Sie eine Audiodatei auswählen, die bei erfolgreicher oder fehlgeschlagener Authentifizierung wiedergegeben werden soll.
- **Benutzerkonfiguration.** Auf dieser Registerkarte können die folgenden Funktionen ausgeführt werden:
-
  - **Benutzer zurücksetzen.** Mit dieser Funktion können Sie Ihre Sicherheitskonfiguration wiederherstellen. Beim Zurücksetzen der Sicherheitskonfiguration werden alle Schlüssel, Zertifikate und Fingerabdrücke gelöscht.
  - **Benutzerkonfiguration über Archiv wiederherstellen:** Mit dieser Funktion können Sie Einstellungen über das Archiv wiederherstellen. Dies ist nützlich, wenn Dateien beschädigt wurden oder Sie eine vorherige Konfiguration wiederherstellen möchten.
  - **Bein einem CSS-Roaming-Server registrieren.** Mit Hilfe dieser Funktion können Sie dieses System bei einem CSS-Roaming-Server registrieren. Wenn das System registriert ist, können Sie Ihre aktuelle Konfiguration in dieses System importieren.

Einschränkungen des Benutzerkonfigurationsprogramms unter Windows XP

Unter Windows XP gibt es unter bestimmten Umständen Zugriffseinschränkungen für die für einen Clientbenutzer verfügbaren Funktionen.

Windows XP Professional

Unter Windows XP Professional können die Einschränkungen für Clientbenutzer in den folgenden Situationen auftreten:

- Client Security ist auf einer Partition installiert, die später in das NTFS-Format konvertiert wird.
- Der Windows-Ordner befindet sich auf einer Partition, die später in das NTFS-Format konvertiert wird.
- Der Archivordner befindet sich auf einer Partition, die später in das NTFS-Format konvertiert wird.

In den vorgenannten Fällen können Benutzer von Windows XP Professional mit eingeschränkter Berechtigung möglicherweise folgende Tasks im Benutzerkonfigurationsprogramm nicht ausführen:

- Den UVM-Verschlüsselungstext ändern
- Das mit UVM registrierte Windows-Kennwort aktualisieren
- Das Schlüsselarchiv aktualisieren

Diese Einschränkungen gelten nicht mehr, nachdem ein Administrator das Administratordienstprogramm gestartet und beendet hat.

Windows XP Home

Benutzer von Windows XP Home mit eingeschränkter Berechtigung können in den folgenden Fällen das Benutzerkonfigurationsprogramm nicht verwenden:

- Client Security ist auf einer Partition im NTFS-Format installiert.
- Der Windows-Ordner befindet sich auf einer Partition im NTFS-Format.
- Der Archivordner befindet sich auf einer Partition im NTFS-Format.

Benutzerkonfigurationsprogramm verwenden

Gehen Sie wie folgt vor, um das Benutzerkonfigurationsprogramm zu verwenden:

1. Klicken Sie auf **Start > Programme > Access IBM > IBM Client Security > Sicherheitseinstellungen ändern**.

   Die Hauptanzeige des Benutzerkonfigurationsprogramms von IBM Client Security wird angezeigt.
2. Wählen Sie eine der folgenden Registerkarten aus:
   - **Kennwörter und Archiv aktualisieren.** Über diese Registerkarte können Sie Ihren UVM-Verschlüsselungstext ändern, Ihr Windows-Kennwort in UVM aktualisieren, Ihr Lotus Notes-Kennwort in UVM zurücksetzen und Ihr Verschlüsselungsarchiv aktualisieren.
   - **UVM-Signaltöne konfigurieren.** Über diese Registerkarte können Sie eine Audiodatei auswählen, die bei erfolgreicher oder fehlgeschlagener Authentifizierung wiedergegeben werden soll.
   - **Benutzerkonfiguration.** Auf dieser Registerkarte kann ein Benutzer die Benutzerkonfiguration aus dem Archiv wiederherstellen, die Sicherheitskonfiguration zurücksetzen oder sich beim Roaming-Server registrieren lassen (wenn der Computer als Roaming-Client verwendet werden kann).
3. Klicken Sie auf **OK**, um die Konfiguration zu beenden.

E-Mails sicher versenden und im World Wide Web sicher navigieren

Wenn Sie über das Internet ungesicherte Transaktionen senden, können diese abgefangen und gelesen werden. Den unbefugten Zugriff auf Ihre Internet-Transaktionen können Sie verhindern, indem Sie sich ein digitales Zertifikat besorgen und damit die E-Mails signieren und verschlüsseln oder den Webbrowser sichern.

Ein digitales Zertifikat (auch digitale ID oder Sicherheitszertifikat genannt) ist ein elektronischer Berechtigungsnachweis, der von einer Zertifizierungsinstanz ausgestellt und digital signiert wird. Wenn Sie ein digitales Zertifikat erhalten, bescheinigt die Zertifizierungsinstanz dadurch Ihre Identität als Eigner des Zertifikats. Bei der Zertifizierungsinstanz handelt es sich um einen vertrauenswürdigen Anbieter von digitalen Zertifikaten, z. B. eine Firma wie VeriSign oder einen Server, der als Zertifizierungsinstanz innerhalb Ihres Unternehmens eingerichtet wird. Das digitale Zertifikat enthält Ihre Identität, d. h. Ihren Namen und Ihre E-Mail-Adresse, die Ablaufdaten des Zertifikats, eine Kopie des öffentlichen Schlüssels sowie die Identität der Zertifizierungsinstanz und deren digitale Unterschrift.

Client Security mit Microsoft-Anwendungen einsetzen

Die nachfolgenden Informationen beziehen sich auf die Verwendung von Client Security für das Anfordern und Anwenden digitaler Zertifikate im Zusammenhang mit Anwendungen, die die Schnittstelle Microsoft CryptoAPI (z. B. Outlook Express) unterstützen.

Weitere Informationen zur Erstellung der Sicherheitseinstellungen und zur Verwendung von E-Mail-Anwendungen wie Outlook Express und Outlook finden Sie in der Dokumentation, die mit diesen Anwendungen geliefert wird.

Digitales Zertifikat für Microsoft-Anwendungen beziehen

Wenn Sie über eine Zertifizierungsinstanz ein für Microsoft-Anwendungen zu verwendendes digitales Zertifikat erstellen, werden Sie aufgefordert, für das Zertifikat einen CSP (Cryptographic Service Provider) auszuwählen.

Damit Sie die Verschlüsselungsfunktionen des integrierten IBM Security Chips für Microsoft-Anwendungen nutzen können, müssen Sie bei Erhalt des digitalen Zertifikats als CSP das **CSP-Modul des integrierten IBM Sicherheits-Subsystems** auswählen. Dadurch ist sichergestellt, dass der private Schlüssel des digitalen Zertifikats auf dem IBM Security Chip gespeichert wird.

Wenn Sie die Sicherheit noch erhöhen möchten, können Sie den hohen Verschlüsselungsgrad auswählen. Da der integrierte IBM Security Chip einen Verschlüsselungsgrad von bis zu 1024 Bit für die Verschlüsselung des privaten Schlüssels des digitalen Zertifikats verarbeiten kann, sollten Sie diese Option auswählen, wenn sie von der Schnittstelle der Zertifizierungsinstanz angeboten wird; die 1024-Bit-Verschlüsselung wird hier auch als hochgradige Verschlüsselung bezeichnet.

Wenn Sie **CSP-Modul des integrierten IBM Sicherheits-Subsystems** als CSP ausgewählt haben, müssen Sie unter Umständen Ihren UVM-Verschlüsselungstext eingeben und/oder sich durch eine Sensorabtastung Ihrer Fingerabdrücke ausweisen, um die Authentifizierungsbestimmungen für das digitale Zertifikat zu erfüllen. Die Authentifizierungsbestimmungen sind in der UVM-Policy für den Computer definiert.

Zertifikate vom Microsoft-CSP übertragen

Mit Hilfe des Assistenten zur Übertragung von Zertifikaten von IBM CSS können Sie Zertifikate können Sie Zertifikate, die mit dem Standard-Microsoft-CSP erstellt wurden, an das CSP-Modul des integrierten IBM Sicherheits-Subsystems (IBM Embedded Security Subsystem) übertragen. Durch das Übertragen der Zertifikate wird der Schutz für die den Zertifikaten zugeordneten privaten Schlüssel erheblich gesteigert, da diese nun sicher auf dem integrierten IBM Sicherheits-Subsystem gespeichert werden, und nicht mehr in der leicht zugänglichen Software.

Zwei Typen von Zertifikaten können übertragen werden:

- **Benutzerzertifikate:** Der Zweck eines Benutzerzertifikats besteht in der Autorisierung eines bestimmten Benutzers. Es ist allgemein üblich, ein Benutzerzertifikat bei einer Zertifizierungsstelle, wie z. B. cssdesk, anzufordern. Eine Zertifizierungsstelle ist eine zuverlässige Instanz, die Zertifikate speichert, ausgibt und veröffentlicht. Möglicherweise benötigen Sie ein Benutzerzertifikat zum Signieren und Verschlüsseln von E-Mails oder zum Anmelden an einem bestimmten Server.
- **Zertifikate im Zertifikatsspeicher der Maschine:** Der Zweck eines Zertifikats im Zertifikatsspeicher der Maschine besteht darin, einen bestimmten Computer eindeutig zu identifizieren. Wenn ein Zertifikat im Zertifikatsspeicher der Maschine verwendet wird, basiert die Authentifizierung auf dem verwendeten Computer, nicht auf dem Benutzer.

Der Assistent zur Übertragung von Zertifikaten von CSS überträgt nur Microsoft-Zertifikate, die als exportierbar gekennzeichnet sind und deren Schlüsselgröße 1024 Bits nicht überschreitet.

Wenn ein Benutzer ein Zertifikat im Zertifikatsspeicher der Maschine übertragen muss und nicht über die Administratorberechtigung für das System verfügt, kann der Administrator ihm eine Administratorkonfigurationsdatei senden, mit deren Hilfe der Benutzer ein Zertifikat ohne Angabe des Administratorkennworts übertragen kann. Verwenden Sie das Dienstprogramm "Administratorkonsole" im Ordner `c:\\program files\ibm\security`, um eine Administratorkonfigurationsdatei zu erstellen.

Gehen Sie wie folgt vor, um den Assistenten zur Übertragung von Zertifikaten von CSS auszuführen:

1. Klicken Sie auf **Start > Access IBM > IBM Client Security > IBM Client Security - Assistent zur Übertragung von Zertifikaten**.

   Die Willkommensseite des Assistenten zur Übertragung von Zertifikaten von IBM CSS wird angezeigt.
2. Klicken Sie zum Starten auf **Weiter**.
3. Wählen Sie die Zertifikatstypen aus, die übertragen werden sollen, und klicken Sie auf **Weiter**. Der Assistent zur Übertragung von Zertifikaten von CSS kann nur Zertifikate in den Microsoft-Zertifikatsspeicher übertragen, die als exportierbar gekennzeichnet sind.
4. Wählen Sie die zu übertragenden Zertifikate durch Klicken auf den Zertifikatsnamen im Ausgabebereich der Schnittstelle aus, und klicken Sie dann auf **Weiter**. Eine Nachricht teilt mit, dass das Zertifikat erfolgreich übertragen wurde.

   Anmerkung: Für das Übertragen eines Zertifikats im Zertifikatsspeicher der Maschine ist ein Administratorkennwort oder eine Administratorkonfigurationsdatei erforderlich.

5. Klicken Sie auf **OK**, um zum Assistenten zur Übertragung von Zertifikaten von CSS zurückzukehren.

Nach dem Übertragen sind die Zertifikate dem CSP-Modul des integrierten IBM Sicherheits-Subsystems zugeordnet, und die privaten Schlüssel werden durch das integrierte IBM Sicherheits-Subsystem geschützt. Alle Operationen, bei denen diese privaten Schlüssel verwendet werden, z. B. beim Erstellen digitaler Signaturen oder beim Entschlüsseln von E-Mails, werden von der geschützten Umgebung des integrierten IBM Sicherheits-Subsystems aus ausgeführt.

Schlüsselarchiv für Microsoft-Anwendungen aktualisieren

Sichern Sie das digitale Zertifikat nach seiner Erstellung, indem Sie das Schlüsselarchiv aktualisieren. Sie können das Schlüsselarchiv mit dem Administratordienstprogramm aktualisieren.

Digitales Zertifikat für Microsoft-Anwendungen verwenden

Verwenden Sie zur Anzeige und zur Verwendung digitaler Zertifikate die Sicherheitseinstellungen in den Microsoft-Anwendungen. Weitere Informationen hierzu finden Sie in der Dokumentation von Microsoft.

Nachdem Sie das digitale Zertifikat erstellt und damit eine E-Mail signiert haben, werden Sie von UVM aufgefordert, die Authentifizierungsbestimmungen beim ersten digitalen Signieren einer E-Mail zu erfüllen. Möglicherweise müssen Sie den UVM-Verschlüsselungstext eingeben, die Fingerabdrücke scannen oder beides, damit Sie die Authentifizierungsbestimmungen zur Verwendung des digitalen Zertifikats erfüllen. Die Authentifizierungsbestimmungen sind in der UVM-Policy für den Computer definiert.

Einstellungen für UVM-Signaltöne konfigurieren

Über die Schnittstelle des Benutzerkonfigurationsprogramms können Einstellungen für Signaltöne konfiguriert werden. Gehen Sie wie folgt vor, um die Standardeinstellung für Signaltöne zu ändern:

1. Klicken Sie auf **Start > Programme > Access IBM > IBM Client Security > Sicherheitseinstellungen ändern**.

   Die Anzeige des Benutzerkonfigurationsprogramms von IBM Client Security wird angezeigt.
2. Klicken Sie auf die Registerkarte **UVM-Signaltöne konfigurieren**.
3. Geben Sie im Abschnitt "UVM-Authentifizierungstöne" in das Feld "Erfolgreiche Authentifizierung" den Dateipfad zur Audiodatei ein, die bei erfolgreicher Authentifizierung wiedergegeben werden soll, oder klicken Sie auf **Durchsuchen**, wenn Sie eine Datei auswählen wollen.
4. Geben Sie im Abschnitt "UVM-Authentifizierungstöne" in das Feld "Authentifizierungsfehler" den Dateipfad zur Audiodatei ein, die bei nicht erfolgreicher Authentifizierung wiedergegeben werden soll, oder klicken Sie auf **Durchsuchen**, wenn Sie eine Datei auswählen wollen.
5. Klicken Sie auf **OK**, um den Vorgang abzuschließen.

Kapitel 5. Fehlerbehebung

Im Folgenden finden Sie Informationen zur Vermeidung, Erkennung und Behebung von Fehlern, die bei der Verwendung von Client Security auftreten können.

Administratorfunktionen

Dieser Abschnitt enthält Informationen für Administratoren zur Konfiguration und zur Verwendung von Client Security.

IBM Client Security kann nur auf IBM Computern verwendet werden, die über das integrierte IBM Sicherheits-Subsystem (IBM Embedded Security Subsystem) verfügen. Diese Software besteht aus Anwendungen und Komponenten, mit denen IBM Clients schutzwürdige Daten über sichere Hardware anstatt durch anfälligere Software sichern können.

Benutzer autorisieren

Bevor die Clientbenutzerinformationen geschützt werden können, **muss** IBM Client Security auf dem Client installiert sein, und die Benutzer **müssen** für Nutzung der Software autorisiert sein. Ein benutzerfreundlicher Installationsassistent leitet Sie durch den gesamten Installationsprozess.

Wichtig: Mindestens ein Clientbenutzer **muss** bei der Installation für die Verwendung von UVM autorisiert werden. Wenn bei der ersten Installation von Client Security kein Benutzer zur Verwendung von UVM berechtigt wird, werden die Sicherheitseinstellungen **nicht** übernommen, und Ihre Daten werden **nicht** geschützt.

Wenn Sie den Installationsassistenten beendet haben, ohne Benutzer berechtigt zu haben, fahren Sie den Computer herunter, und starten Sie ihn erneut; führen Sie dann den Installationsassistenten von Client Security über das Windows-Startmenü aus, und autorisiseren Sie einen Windows-Benutzer für die Benutzung von UVM. Auf diese Weise wird IBM Client Security für das Übernehmen der Sicherheitseinstellungen und für den Schutz der schutzwürdigen Daten aktiviert.

Benutzer löschen

Wenn Sie einen Benutzer löschen, wird der Benutzername in der Benutzerliste des Administratordienstprogramms gelöscht.

BIOS-Administratorkennwort festlegen (ThinkCentre)

Über die Sicherheitseinstellungen im Programm "Configuration/Setup Utility" können Administratoren folgende Vorgänge durchführen:

- Das integrierte IBM Sicherheits-Subsystem aktivieren oder inaktivieren
- Den Inhalt des integrierten IBM Sicherheits-Subsystems löschen

Achtung:

- Wenn der Inhalt des integrierten IBM Sicherheits-Subsystems gelöscht wird, gehen alle in diesem Subsystem gespeicherten Chiffrierschlüssel und Zertifikate verloren.

Da auf Ihre Sicherheitseinstellungen über das Programm "Configuration/Setup Utility" des Computers zugegriffen werden kann, legen Sie ein Administratorkennwort fest, um zu verhindern, dass diese Einstellungen durch nicht autorisierte Benutzer geändert werden.

Gehen Sie wie folgt vor, um ein BIOS-Administratorkennwort festzulegen:

1. Fahren Sie das System herunter, und starten Sie es erneut.
2. Drücken Sie während der Eingabeaufforderung des Programms "Configuration/Setup Utility" die Taste **F1**.

   Das Hauptmenü des Programms "Configuration/Setup Utility" wird geöffnet.
3. Wählen Sie die Option **System Security** aus.
4. Wählen Sie die Option **Administrator Password** aus.
5. Geben Sie das Kennwort ein, und drücken Sie auf der Tastatur die Taste mit dem Abwärtspfeil.
6. Geben Sie das Kennwort erneut ein, und drücken Sie auf der Tastatur die Taste mit dem Abwärtspfeil.
7. Wählen Sie die Option **Change Administrator password** aus, und drücken Sie die Eingabetaste. Drücken Sie danach erneut die Eingabetaste.
8. Drücken Sie die Taste **Esc**, um die Einstellungen zu speichern und das Programm zu verlassen.

Nachdem Sie ein BIOS-Administratorkennwort festgelegt haben, wird jedes Mal, wenn Sie auf das Programm "Configuration/Setup Utility" zugreifen, eine Eingabeaufforderung angezeigt.

Wichtig: Notieren Sie Ihr BIOS-Administratorkennwort, und bewahren Sie es an einem sicheren Ort auf. Wenn Sie das BIOS-Administratorkennwort verlieren oder vergessen, können Sie auf das Programm "Configuration/Setup Utility" nicht mehr zugreifen und können das BIOS-Administratorkennwort nicht mehr ändern oder löschen, ohne die Computerabdeckung zu entfernen und eine Brücke auf der Systemplatine zu versetzen. Weitere Informationen hierzu finden Sie in der Hardwaredokumentation, die mit Ihrem Computer geliefert wurde.

Administratorkennwort festlegen (ThinkPad)

Mit den Sicherheitseinstellungen im Programm "IBM BIOS Setup Utility" können Administratoren folgende Vorgänge durchführen:

- Das integrierte IBM Sicherheits-Subsystem aktivieren oder inaktivieren
- Den Inhalt des integrierten IBM Sicherheits-Subsystems löschen

Achtung:

- Bei einigen ThinkPad-Modellen ist es vor der Installation oder dem Upgrade von Client Security notwendig, das Administratorkennwort vorübergehend zu inaktivieren.

Nach der Konfiguration von Client Security legen Sie ein Administratorkennwort fest, um nicht berechtigte Benutzer daran zu hindern, diese Einstellungen ändern.

Gehen Sie nach einer der beiden Prozeduren vor, um ein Systemadministrator festzulegen:

Beispiel 1

1. Fahren Sie das System herunter, und starten Sie es erneut.
2. Drücken Sie die Taste F1, wenn die Eingabeaufforderung des Programms "Setup Utility" angezeigt wird.

   Das Hauptmenü des Programms "Setup Utility" wird geöffnet.
3. Wählen Sie die Option **Password** aus.
4. Wählen Sie die Option **Supervisor Password** aus.
5. Geben Sie das Kennwort ein, und drücken Sie die Eingabetaste.
6. Geben Sie das Kennwort erneut ein, und drücken Sie die Eingabetaste.
7. Klicken Sie auf **Continue**.
8. Drücken Sie die Taste F10, um die Einstellungen zu speichern und das Programm zu beenden.

Beispiel 2

1. Fahren Sie das System herunter, und starten Sie es erneut.
2. Wenn die Nachricht "To interrupt normal startup, press the blue Access IBM button" angezeigt wird, drücken Sie die blaue Taste "Access IBM".

   Die Access IBM Predesktop Area wird geöffnet.
3. Klicken Sie doppelt auf **Konfigurationsdienstprogramm starten**.
4. Wählen Sie mit Hilfe der Navigationstasten den Menüpunkt **Security** aus.
5. Wählen Sie die Option **Password** aus.
6. Wählen Sie die Option **Supervisor Password** aus.
7. Geben Sie das Kennwort ein, und drücken Sie die Eingabetaste.
8. Geben Sie das Kennwort erneut ein, und drücken Sie die Eingabetaste.
9. Klicken Sie auf **Continue**.
10. Drücken Sie die Taste F10, um die Einstellungen zu speichern und das Programm zu beenden.

Nach dem Festlegen eines Administratorkennworts wird bei jedem Zugriff auf das Programm "BIOS Setup Utility" eine Eingabeaufforderung angezeigt.

Wichtig: Bewahren Sie Ihr Administratorkennwort an einem sicheren Ort auf. Sollten Sie das Administratorkennwort verlieren oder vergessen, können Sie nicht auf das Programm "IBM BIOS Setup Utility" zugreifen und das Kennwort nicht ändern oder löschen. Weitere Informationen hierzu finden Sie in der Hardwaredokumentation, die mit Ihrem Computer geliefert wurde.

Administratorkennwort schützen

Das Administratorkennwort dient als Schutz für den Zugriff auf das Administratordienstprogramm. Halten Sie das Administratorkennwort geheim, um zu verhindern, dass Benutzer ohne Berechtigung Einstellungen im Administratordienstprogramm ändern können.

Inhalt des integrierten IBM Sicherheits-Subsystems löschen (ThinkCentre)

Wenn Sie alle Chiffrierschlüssel für Benutzer aus dem integrierten IBM Sicherheits-Subsystem entfernen und das Administratorkennwort für das Subsystem löschen möchten, müssen Sie den Inhalt des Chips löschen. Lesen Sie die folgenden Hinweise, bevor Sie den Inhalt des integrierten IBM Sicherheits-Subsystems löschen.

Achtung:

- Wenn der Inhalt des integrierten IBM Sicherheits-Subsystems gelöscht wird, gehen alle in diesem Subsystem gespeicherten Chiffrierschlüssel und Zertifikate verloren.

Gehen Sie wie folgt vor, um den Inhalt des integrierten IBM Sicherheits-Subsystems zu löschen:

1. Fahren Sie das System herunter, und starten Sie es erneut.
2. Drücken Sie die Taste F1, wenn die Eingabeaufforderung des Programms "Setup Utility" angezeigt wird. Das Hauptmenü des Programms "Setup Utility" wird geöffnet.
3. Wählen Sie die Option **Security** aus.
4. Wählen Sie **IBM TCPA Feature Setup** aus.
5. Wählen Sie **Clear IBM TCPA Security Feature** aus, und drücken Sie die Eingabetaste.
6. Wählen Sie **Yes** aus.
7. Drücken Sie die Taste F10, und wählen Sie **Yes** aus.
8. Drücken Sie die Eingabetaste. Der Computer wird erneut gestartet.

Inhalt des integrierten IBM Sicherheits-Subsystems löschen (ThinkPad)

Wenn Sie alle Chiffrierschlüssel für Benutzer aus dem integrierten IBM Sicherheits-Subsystem entfernen und das Administratorkennwort löschen möchten, müssen Sie den Inhalt des Subsystems löschen. Lesen Sie die folgenden Hinweise, bevor Sie den Inhalt des integrierten IBM Sicherheits-Subsystems löschen.

Achtung:

- Wenn der Inhalt des integrierten IBM Sicherheits-Subsystems gelöscht wird, gehen alle in diesem Subsystem gespeicherten Chiffrierschlüssel und Zertifikate verloren.

Gehen Sie wie folgt vor, um den Inhalt des integrierten IBM Sicherheits-Subsystems zu löschen:

1. Fahren Sie den Computer herunter.
2. Halten Sie beim erneuten Starten des Computers die Taste Fn gedrückt.
3. Drücken Sie die Taste F1, wenn die Eingabeaufforderung des Programms "Setup Utility" angezeigt wird. Das Hauptmenü des Programms "Setup Utility" wird geöffnet.
4. Wählen Sie die Option **Config** aus.
5. Wählen Sie **IBM Security Chip** aus.
6. Wählen Sie **Clear IBM Security Chip** aus.
7. Wählen Sie **Yes** aus.
8. Drücken Sie die Eingabetaste, um fortzufahren.
9. Drücken Sie die Taste F10, um die Einstellungen zu speichern und das Programm zu beenden.

Bekannte Probleme oder Einschränkungen bei CSS Version 5.2

Die folgenden Informationen sind möglicherweise zur Verwendung der Funktionen von Client Security Version 5.2 nützlich.

Einschränkungen bei standortunabhängigem Zugriff

CSS-Roaming-Server verwenden

Die Aufforderung zur Eingabe des CSS-Administratorkennworts erscheint immer dann, wenn jemand versucht, sich am CSS-Roaming-Server anzumelden. Normalerweise kann der Computer aber auch ohne die Eingabe dieses Kennworts benutzt werden.

IBM Security Password Manager in einer Umgebung mit standortunabhängigem Zugriff verwenden

Kennwörter, die in einem System gespeichert wurden, das IBM Client Security Password Manager verwendet, können auch in anderen Systemen innerhalb einer Umgebung mit standortunabhängigem Zugriff verwendet werden. Neue Einträge werden automatisch vom Archiv abgerufen, wenn sich der Benutzer bei einem anderen System im Netzwerk mit standortunabhängigem Zugriff anmeldet (wenn das Archiv verfügbar ist). Aus diesem Grund muss sich der Benutzer, wenn er bereits an einem System angemeldet ist, zunächst abmelden und erneut anmelden, bevor neue Einträge im Netzwerk mit standortunabhängigem Zugriff verfügbar sind.

Verzögerungen bei der Aktualisierung des Zertifikats für den Internet Explorer und des standortunabhängigen Zugriffs

Die Zertifikate für den Internet Explorer werden alle 20 Sekunden im Archiv aktualisiert. Wurde durch einen standortunabhängigen Benutzer ein neues Zertifikat für den Internet Explorer erstellt, muss der Benutzer mindestens 20 Sekunden warten, bis er seine CSS-Konfiguration auf einem anderen System importieren, wiederherstellen oder ändern kann. Bei dem Versuch, eine dieser Aktionen vor dem Ende des Aktualisierungsintervalls von 20 Sekunden durchzuführen, geht das Zertifikat verloren. Auch wenn der Benutzer keine Verbindung zum Archiv hatte, während das Zertifikat erstellt wurde, sollte er 20 Sekunden warten, nachdem die Verbindung zum Archiv hergestellt wurde, um sicherzustellen, dass das Zertifikat im Archiv aktualisiert wurde.

Lotus Notes-Kennwort und standortunabhängiger Zugriff mit Berechtigungsnachweis

Wenn die Lotus Notes-Unterstützung aktiviert ist, wird das Lotus Notes-Kennwort des Benutzers durch UVM gespeichert. Die Benutzer brauchen ihr Notes-Kennwort künftig nicht mehr einzugeben, um sich bei Lotus Notes anzumelden. Sie werden nach ihrem UVM-Verschlüsselungstext, dem Fingerabdruck, der Smartcard usw. (je nach Einstellungen der Sicherheitspolicy) gefragt, um auf Lotus Notes zugreifen zu können.

Wenn ein Benutzer sein Notes-Kennwort von Lotus Notes aus ändert, wird die Lotus Notes-ID-Datei mit dem neuen Kennwort aktualisiert und die UVM-Kopie des neuen Notes-Kennworts wird ebenfalls aktualisiert. In einer Umgebung mit standortunabhängigem Zugriff sind die UVM-Berechtigungsnachweise des Benutzers auch in anderen Systemen des Netzwerks mit standortunabhängigem Zugriff verfügbar, auf die der Benutzer zugreifen kann. Es ist möglich, dass die Kopie des Notes-Kennworts von UVM nicht mit dem Notes-Kennwort in der ID-Datei auf anderen Systemen im Netzwerk mit standortunabhängigem Zugriff übereinstimmt,

wenn die Notes-ID-Datei mit dem aktualisierten Kennwort nicht ebenfalls auf einem anderen System verfügbar ist. Wenn dies der Fall ist, kann der Benutzer nicht auf Lotus Notes zugreifen.

Wenn die Notes-ID-Datei mit dem aktualisierten Kennwort eines Benutzers nicht auch in einem anderen System verfügbar ist, sollte die ID-Datei in die anderen Systeme innerhalb des Netzwerks mit standortunabhängigem Zugriff kopiert werden, so dass das Kennwort in der ID-Datei mit der durch UVM gespeicherten Kopie übereinstimmt. Alternativ können die Benutzer im Startmenü auch die Anwendung "Sicherheitseinstellungen ändern" ausführen und das Notes-Kennwort in den alten Wert ändern. Das Notes-Kennwort kann dann über Lotus Notes wieder aktualisiert werden.

Verfügbarkeit von Berechtigungsnachweisen in einer Umgebung mit standortunabhängigem Zugriff

Befindet sich ein Archiv in einem gemeinsam benutzten Netzwerk, wird die aktuellste Gruppe von Benutzerberechtigungen aus dem Archiv heruntergeladen, sobald der Benutzer auf das Archiv zugreifen kann. Bei der Anmeldung haben die Benutzer nicht sofort Zugriff auf das gemeinsam benutzte Netzwerk, so dass die aktuellsten Berechtigungsnachweise erst heruntergeladen werden können, nachdem die Anmeldung am System abgeschlossen ist. Wenn z. B. der UVM-Verschlüsselungstext auf einem anderen System im Netzwerk mit standortunabhängigem Zugriff geändert wurde oder wenn neue Fingerabdrücke in einem anderen System registriert wurden, sind diese Aktualisierungen erst verfügbar, wenn der Anmeldeprozess beendet ist. Sind die aktualisierten Benutzerberechtigungen nicht verfügbar, sollten die Benutzer versuchen, sich mit dem früheren Verschlüsselungstext oder mit anderen registrierten Fingerabdrücken am System anzumelden. Sobald die Anmeldung beendet ist, sind die aktualisierten Benutzerberechtigungen verfügbar, und das neue Kennwort sowie der Fingerabdruck sind bei UVM registriert.

Einschränkungen bei berührungslosem Ausweis (Proximity Badge)

Sicheren UVM-Anmeldeschutz mit berührungslosem Ausweis (Proximity Badge) von XyLoc aktivieren

Um die Unterstützung des sicheren UVM-Anmeldeschutzes für die Verwendung eines berührungslosen Ausweises (Proximity Badge) bei CSS erfolgreich zu aktivieren, müssen Sie die Komponenten in folgender Reihenfolge installieren:

1. Installieren Sie Client Security.
2. Aktivieren Sie den sicheren UVM-Anmeldeschutz mit Hilfe des CSS-Administratordienstprogramms.
3. Starten Sie den Computer erneut.
4. Installieren Sie die Software von XyLoc für die Unterstützung von berührungslosen Ausweisen (Proximity Badges).

Anmerkung: Wenn die Software von XyLoc für den berührungslosen Ausweis zuerst installiert wird, wird die Anmeldeschnittstelle für Client Security nicht angezeigt. Wenn dies eintritt, müssen Sie Client Security und die Software von wXyLoc deinstallieren und anschließend in der oben genannten Reihenfolge erneut installieren, um den sicheren UVM-Anmeldeschutz wiederherzustellen.

Unterstützung von berührungslosem Ausweis (Proximity Badge) und Cisco LEAP

Durch das Aktivieren des Zugriffsschutzes mit berührungslosem Ausweis (Proximity Badge) und die Unterstützung von Cisco LEAP können unerwartete Ergebnisse auftreten. Es wird empfohlen, diese Komponenten nicht zusammen auf demselben System zu installieren oder zu verwenden.

Unterstützung für Ensure-Software

Bei Client Security 5.2 ist es erforderlich, dass die Benutzer eines berührungslosen Ausweises (Proximity Badge) ihre Ensure-Software auf die Ensure-Softwareversion 7.41 aufrüsten. Wenn Sie einen Upgrade von einer früheren Version von Client Security aus durchführen, müssen Sie zuerst die Ensure-Software aufrüsten, bevor Sie auf Client Security 5.2 aufrüsten können.

Wiederherstellen von Schlüsseln

Nach der Durchführung einer Wiederherstellungsoperation für die Schlüssel müssen Sie den Computer erneut starten, bevor Sie Client Security weiterhin verwenden können.

Namen des lokalen Benutzers und des Domänenbenutzers

Wenn die Namen des Domänenbenutzers und des lokalen Benutzers gleich sind, sollten Sie für beide Konten dasselbe Windows-Kennwort verwenden. IBM User Verification Manager speichert nur ein Windows-Kennwort pro ID. Die Benutzer sollten daher dasselbe Kennwort für die lokale Anmeldung und für die Domänenanmeldung verwenden. Wenn dies nicht der Fall ist, werden die Benutzer dazu aufgefordert, das IBM UVM Windows-Kennwort zu aktualisieren, wenn sie zwischen lokaler und Domänenanmeldung umschalten, wenn die Ersetzung der gesicherten IBM UVM Windows-Anmeldung aktiviert ist.

CSS ist nicht in der Lage, getrennte Domänenbenutzer und lokale Benutzer mit demselben Kontonamen zu registrieren. Wenn Sie versuchen, lokale Benutzer und Domänenbenutzer mit derselben ID zu registrieren, wird folgende Nachricht angezeigt: "Die ausgewählte Benutzer-ID wurde bereits konfiguriert". Bei CSS ist es nicht möglich, allgemeine IDs von Domänen- und von lokalen Benutzern einzeln in einem System zu registrieren, so dass mit der allgemeinen Benutzer-ID auf dieselbe Gruppe von Berechtigungsnachweisen, wie z. B. Zertifikate, gespeicherte Fingerabdrücke usw., zugegriffen werden kann.

Targus-Software zum Lesen von Fingerabdrücken erneut installieren

Wurde die Targus-Software zum Lesen von Fingerabdrücken entfernt und anschließend erneut installiert, müssen die erforderlichen Registrierungseinträge zum Aktivieren der Unterstützung für das Lesen von Fingerabdrücken bei Client Security manuell aktiviert werden. Laden Sie die Registrierungsdatei mit den erforderlichen Einträgen (atplugin.reg) herunter, und klicken Sie doppelt darauf, um die Registrierungseinträge dem Register hinzuzufügen. Klicken Sie bei entsprechender Aufforderung auf "Ja", um diese Operation zu bestätigen. Das System muss erneut gestartet werden, damit die Änderungen von Client Security erkannt werden und die Unterstützung für das Lesen von Fingerabdrücken aktiviert wird.

Anmerkung: Für das Hinzufügen dieser Registrierungseinträge ist die Administratorberechtigung auf dem System erforderlich.

Administratorverschlüsselungstext für das BIOS

IBM Client Security 5.2 und frühere Versionen unterstützen nicht die auf einigen ThinkPad-Systemen verfügbare Funktion für den Administratorverschlüsselungstext für das BIOS. Wenn Sie die Verwendung des Administratorverschlüsselungstextes für das BIOS aktivieren, muss jede Aktivierung und Inaktivierung des Sicherheits-Subsystems über das Programm "IBM BIOS Setup Utility" vorgenommen werden.

Netscape 7.x verwenden

Netscape 7.x unterscheidet sich von Netscape 4.x. Die Eingabeaufforderung für den Verschlüsselungstext erscheint nicht, sobald Netscape gestartet wurde. Stattdessen wird das PKCS#11-Modul nur bei Bedarf geladen, so dass die Eingabeaufforderung für den Verschlüsselungstext nur dann angezeigt wird, wenn eine Operation ausgeführt wird, bei der das PKCS#11-Modul erforderlich ist.

Diskette zum Archivieren verwenden

Wenn Sie bei der Konfiguration der Sicherheitssoftware eine Diskette als Archivposition angegeben haben, müssen Sie mit langen Verzögerungen rechnen, wenn die Daten während des Konfigurationsprozesses auf die Diskette geschrieben werden. Ein anderer Datenträger, wie z. B. ein gemeinsam benutztes Netzwerk oder ein USB Memory Key, eignet sich möglicherweise besser als Archivposition.

Einschränkungen bei der Verwendung von Smartcards

Smartcard-Registrierung

Smartcards müssen erst bei UVM registriert werden, bevor ein Benutzer eine Authentifizierung mit Hilfe der Karte erfolgreich durchführen kann. Wenn eine Karte mehreren Benutzern zugeordnet ist, kann nur der letzte Benutzer, der die Karte registrieren ließ, diese auch verwenden. Aus diesem Grund sollten Smartcards nur für einen Benutzeraccount registriert werden.

Smartcard-Authentifizierung

Ist für die Authentifizierung eine Smartcard erforderlich, zeigt UVM ein Dialogfeld an, in dem die Smartcard angefordert wird. Wenn die Smartcard in die Leseeinheit eingelegt wird, erscheint ein Dialogfenster, in dem die PIN-Nummer der Smartcard angefordert wird. Gibt der Benutzer eine falsche PIN-Nummer ein, fordert UVM die Smartcard noch einmal an. Die Smartcard muss entnommen und erneut eingelegt werden, bevor die PIN-Nummer erneut eingegeben werden kann. Die Benutzer müssen die Smartcard so oft entnehmen und erneut einlegen, bis die richtige PIN-Nummer für die Karte eingegeben wurde.

Pluszeichen (+) wird auf Ordnern nach der Verschlüsselung angezeigt

Nach der Verschlüsselung von Dateien oder Ordnern zeigt der Windows Explorer möglicherweise ein Pluszeichen (+) vor dem Ordnersymbol an. Dieses zusätzliche Zeichen wird nicht mehr angezeigt, wenn das Explorer-Fenster aktualisiert wird.

Einschränkungen für Benutzer mit eingeschränkter Berechtigung unter Windows XP

Benutzer mit eingeschränkter Berechtigung unter Windows XP können ihren UVM-Verschlüsselungstext, das Windows-Kennwort oder ihr Schlüsselarchiv nicht mit Hilfe des Benutzerkonfigurationsprogramms aktualisieren.

Andere Einschränkungen

Dieser Abschnitt enthält Informationen zu anderen bekannten Einschränkungen in Bezug auf Client Security.

Client Security mit Windows-Betriebssystemen einsetzen

Alle Windows-Betriebssysteme weisen die folgende bekannte Einschränkung auf: Wenn ein in UVM registrierter Clientbenutzer seinen Windows-Benutzernamen ändert, geht die gesamte Funktionalität von Client Security verloren. Der Benutzer muss den neuen Benutzernamen erneut in UVM registrieren und alle neuen Berechtigungsnachweise anfordern.

Windows XP-Betriebssysteme weisen die folgende bekannte Einschränkung auf: In UVM registrierte Benutzer, deren Windows-Benutzername zuvor geändert wurde, werden von UVM nicht erkannt. UVM verweist auf den früheren Benutzernamen, während Windows nur den neuen Benutzernamen erkennt. Diese Einschränkung gilt selbst dann, wenn der Windows-Benutzername vor der Installation von Client Security geändert wurde.

Client Security mit Netscape-Anwendungen einsetzen

Netscape wird nach einem Berechtigungsfehler geöffnet: Wenn das Fenster "UVM-Verschlüsselungstext" geöffnet wird, müssen Sie den UVM-Verschlüsselungstext eingeben und auf **OK** klicken, bevor Sie fortfahren können. Wenn Sie einen falschen UVM-Verschlüsselungstext eingeben (oder bei einer Scannerabtastung von Fingerabdrücken einen falschen Fingerabdruck liefern), wird eine Fehlernachricht angezeigt. Wenn Sie auf **OK** klicken, wird Netscape zwar geöffnet, Sie können aber das vom integrierten IBM Sicherheits-Subsystem generierte digitale Zertifikat nicht verwenden. Sie müssen Netscape verlassen, erneut aufrufen und den richtigen UVM-Verschlüsselungstext eingeben, bevor Sie das Zertifikat für das integrierten IBM Sicherheits-Subsystem verwenden können.

Algorithmen werden nicht angezeigt: Alle Hashverfahren-Algorithmen, die vom PKCS #11-Modul des integrierten IBM Sicherheits-Subsystems unterstützt werden, erscheinen bei der Anzeige des Moduls in Netscape als nicht ausgewählt. Folgende Algorithmen werden zwar vom PKCS #11-Modul des integrierten IBM Sicherheits-Subsystems unterstützt, in der Netscape-Anzeige jedoch nicht als unterstützt angegeben.

- SHA-1
- MD5

Zertifikat des integrierten IBM Sicherheits-Subsystems und Verschlüsselungsalgorithmen

Im folgenden Abschnitt erhalten Sie Informationen zu den Verschlüsselungsalgorithmen, die zusammen mit dem Zertifikat des integrierten IBM Sicherheits-Subsystems verwendet werden können. Aktuelle Informationen zu Verschlüsselungsalgorithmen für die jeweilige E-Mail-Anwendung erhalten Sie von Microsoft oder Netscape.

Beim Senden von E-Mails von einem Outlook Express-Client (128 Bit) an einen anderen Outlook Express-Client (128 Bit): Wenn Sie Outlook Express mit der 128-Bit-Version von Internet Explorer 4.0 oder 5.0 verwenden, um verschlüsselte E-Mails an andere Clients mit Outlook Express (128 Bit) zu senden, können mit dem Zertifikat des integrierten IBM Sicherheits-Subsystems verschlüsselte E-Mails nur mit dem 3DES-Algorithmus verschlüsselt werden.

Beim Senden von E-Mails zwischen einem Outlook Express-Client (128 Bit) und einem Netscape-Client: Eine Verschlüsselungsanforderung gemäß RC2(40), RC2(64) oder RC2(128) von einem Netscape-Client an einen Outlook Express-Client (128 Bit) wird an den Netscape-Client immer mit dem RC2(40)-Algorithmus zurückgesendet.

Möglicherweise stehen einige Algorithmen im Outlook Express-Client (128 Bit) nicht zur Auswahl: Je nachdem, wie die Version von Outlook Express (128 Bit) konfiguriert oder aktualisiert wurde, sind möglicherweise einige RC2-Algorithmen und andere Algorithmen für die Verwendung mit dem Zertifikat des integrierten IBM Sicherheits-Subsystems nicht verfügbar. Aktuelle Informationen zu den Verschlüsselungsalgorithmen, die mit den verschiedenen Versionen von Outlook Express verwendet werden, erhalten Sie von Microsoft.

UVM-Schutz für eine Lotus Notes-Benutzer-ID verwenden

Der UVM-Schutz funktioniert nicht, wenn Sie innerhalb einer Notes-Sitzung die Benutzer-ID wechseln: Sie können den UVM-Schutz nur für die aktuelle Benutzer-ID einer Notes-Sitzung konfigurieren. Gehen Sie wie folgt vor, um von einer Benutzer-ID, für die UVM-Schutz aktiviert wurde, zu einer anderen Benutzer-ID zu wechseln:

1. Verlassen Sie Lotus Notes.
2. Inaktivieren Sie den UVM-Schutz für die aktuelle Benutzer-ID.
3. Rufen Sie Lotus Notes auf, und wechseln Sie die Benutzer-ID. Weitere Informationen zum Wechseln von Benutzer-IDs finden Sie in der Dokumentation zu Lotus Notes.

   Wenn Sie den UVM-Schutz für die Benutzer-ID, zu der Sie gewechselt haben, konfigurieren möchten, fahren Sie mit Schritt 4 fort.
4. Rufen Sie das von Client Security bereitgestellte Tool zur Lotus Notes-Konfiguration auf, und konfigurieren Sie den UVM-Schutz.

Einschränkungen für das Benutzerkonfigurationsprogramm

Unter Windows XP gibt es für einen Clientbenutzer unter bestimmten Umständen Zugriffseinschränkungen für die verfügbaren Funktionen.

Windows XP Professional

Unter Windows XP Professional können die Einschränkungen für Clientbenutzer in den folgenden Situationen auftreten:

- Client Security ist auf einer Partition installiert, die später in das NTFS-Format konvertiert wird.
- Der Windows-Ordner befindet sich auf einer Partition, die später in das NTFS-Format konvertiert wird.
- Der Archivordner befindet sich auf einer Partition, die später in das NTFS-Format konvertiert wird.

In den vorgenannten Fällen können Benutzer von Windows XP Professional mit eingeschränkter Berechtigung möglicherweise folgende Tasks im Benutzerkonfigurationsprogramm nicht ausführen:

- Den UVM-Verschlüsselungstext ändern
- Das mit UVM registrierte Windows-Kennwort aktualisieren
- Das Schlüsselarchiv aktualisieren

Windows XP Home

Benutzer von Windows XP Home mit eingeschränkter Berechtigung können in den folgenden Fällen das Benutzerkonfigurationsprogramm nicht verwenden:

- Client Security ist auf einer Partition im NTFS-Format installiert.
- Der Windows-Ordner befindet sich auf einer Partition im NTFS-Format.
- Der Archivordner befindet sich auf einer Partition im NTFS-Format.

Einschränkungen bei Tivoli Access Manager

Das Markierungsfeld **Keinen Zugriff auf ausgewähltes Objekt zulassen** ist nicht inaktiviert, wenn die Tivoli Access Manager-Steuerung ausgewählt wurde. Wenn Sie im UVM-Policy-Editor die Option **Access Manager steuert ausgewähltes Objekt** auswählen, um ein Authentifizierungsobjekt über Tivoli Access Manager zu steuern, wird das Markierungsfeld **Keinen Zugriff auf ausgewähltes Objekt zulassen** nicht inaktiviert. Auch wenn das Markierungsfeld **Keinen Zugriff auf ausgewähltes Objekt zulassen** weiterhin aktiviert ist, kann die Tivoli Access Manager-Steuerung nicht über dieses Markierungsfeld außer Kraft gesetzt werden.

Fehlernachrichten

Fehlernachrichten für Client Security werden in das Ereignisprotokoll geschrieben: Client Security verwendet einen Einheitentreiber, der möglicherweise Fehlernachrichten in das Ereignisprotokoll schreibt. Die Fehler, auf denen diese Nachrichten basieren, wirken sich auf den normalen Betrieb des Computers nicht aus.

UVM ruft Fehlernachrichten auf, die vom zugeordneten Programm generiert werden, wenn für ein Authentifizierungsobjekt der Zugriff verweigert wird: Wenn in der UVM-Policy die Verweigerung des Zugriffs für ein Authentifizierungsobjekt, z. B. für die E-Mail-Verschlüsselung festgelegt ist, variiert die Nachricht über den verweigerten Zugriff je nach verwendeter Software. Eine Fehlernachricht von Outlook Express über die Verweigerung des Zugriffs auf ein Authentifizierungsobjekt unterscheidet sich somit von einer Netscape-Fehlernachricht über verweigerten Zugriff.

Fehlerbehebungstabellen

Im folgenden Abschnitt finden Sie Tabellen, die Ihnen bei der Behebung von Fehlern in Verbindung mit Client Security weiterhelfen können.

Fehlerbehebungsinformationen zur Installation

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Installation von Client Security weiterhelfen können.

Fehlersymptom	**Mögliche Lösung**
Während der Softwareinstallation wird eine Fehlernachricht angezeigt.	**Maßnahme**
Bei der Softwareinstallation werden Sie in einer Nachricht gefragt, ob Sie die ausgewählte Anwendung und alle zugehörigen Komponenten entfernen möchten.	Klicken Sie auf **OK**, um das Fenster zu verlassen. Beginnen Sie erneut mit dem Installationsprozess, um die neue Version von Client Security zu installieren.
Während der Installation wird eine Nachricht angezeigt, die besagt, dass Sie das Programm aufrüsten oder entfernen müssen.	Führen Sie einen der folgenden Schritte aus: • Wenn eine ältere Version als Client Security 5.0 installiert ist, wählen Sie aus, dass das Programm entfernt werden soll, und löschen Sie den Inhalt des Sicherheits-Subsystems im Programm "IBM BIOS Setup". • Wählen Sie andernfalls aus, dass das Programm aufgerüstet werden soll, und fahren Sie mit der Installation fort.
Der Installationszugriff wird verweigert, da das Administratorkennwort unbekannt ist	**Maßnahme**
Wenn Sie die Software auf einem IBM-Client mit einem aktivierten integrierten IBM Sicherheits-Subsystem installieren, ist das Administratorkennwort für das integrierte IBM Sicherheits-Subsystem unbekannt.	Löschen Sie den Inhalt des Sicherheits-Subsystems, um mit der Installation fortzufahren.

Fehlerbehebungsinformationen zum Administratordienstprogramm

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Verwendung des Administratordienstprogramms weiterhelfen können.

Fehlersymptom	Mögliche Lösung
Die Schaltfläche ″Weiter″ ist nicht verfügbar, nachdem Sie im Administratordienstprogramm den UVM-Verschlüsselungstext eingegeben und bestätigt haben.	**Maßnahme**
Wenn Sie neue Benutzer in UVM aufnehmen, ist die Schaltfläche **Weiter** möglicherweise nicht mehr verfügbar, nachdem Sie Ihren UVM-Verschlüsselungstext im Administratordienstprogramm eingegeben und bestätigt haben.	Klicken Sie in der Windows-Taskleiste auf **Informationen**, und fahren Sie mit dem Vorgang fort.
Beim Ändern des öffentlichen Administratorschlüssels wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie den Inhalt des integrierten IBM Sicherheits-Subsystems löschen und anschließend das Schlüsselarchiv wiederherstellen, wird beim Ändern des öffentlichen Administratorschlüssels möglicherweise eine Fehlernachricht angezeigt.	Fügen Sie in UVM die Benutzer hinzu, und fordern Sie ggf. neue Zertifikate an.
Beim Versuch, einen UVM-Verschlüsselungstext wiederherzustellen, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie einen öffentlichen Administratorschlüssel ändern und anschließend versuchen, einen UVM-Verschlüsselungstext für einen Benutzer wiederherzustellen, wird möglicherweise eine Fehlernachricht angezeigt.	Führen Sie einen der folgenden Schritte aus: • Sollte für den Benutzer der UVM-Verschlüsselungstext nicht benötigt werden, ist keine Maßnahme erforderlich. • Wenn der UVM-Verschlüsselungstext für den Benutzer erforderlich ist, müssen Sie ihn in UVM aufnehmen und ggf. neue Zertifikate anfordern.
Beim Versuch, die UVM-Policydatei zu speichern, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie versuchen, eine UVM-Policydatei (globalpolicy.gvm) durch Klicken auf **Übernehmen** oder **Speichern** zu speichern, wird eine Fehlernachricht angezeigt.	Schließen Sie die Fehlernachricht, bearbeiten Sie die UVM-Policydatei erneut, und speichern Sie die Datei.
Beim Versuch, den UVM-Policy-Editor zu öffnen, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn der aktuelle Benutzer, der am Betriebssystem angemeldet ist, nicht in UVM aufgenommen wurde, wird der UVM-Policy-Editor nicht geöffnet.	Nehmen Sie den Benutzer in UVM auf, und öffnen Sie den UVM-Policy-Editor.

Fehlersymptom	Mögliche Lösung
Bei der Verwendung des Administratordienstprogramms wird eine Fehlernachricht angezeigt.	**Maßnahme**
Während Sie das Administratordienstprogramm verwenden, wird möglicherweise die folgende Fehlernachricht angezeigt: Beim Versuch, auf das integrierte IBM Sicherheits-Subsystem zuzugreifen, ist ein Puffer-E/A-Fehler aufgetreten. Der Fehler kann möglicherweise durch einen Warmstart behoben werden.	Schließen Sie die Fehlernachricht, und starten Sie den Computer erneut.
Beim Ändern des Administratorkennworts wird eine Nachricht über die Inaktivierung des Chips angezeigt.	**Maßnahme**
Wenn Sie versuchen, das Administratorkennwort zu ändern, und nach der Eingabe des Bestätigungskennworts die Eingabetaste oder die Tabulatortaste zusammen mit der Eingabetaste drücken, wird die Schaltfläche **Chip inaktivieren** aktiviert, und es wird eine Bestätigungsnachricht für das Inaktivieren des Chips angezeigt.	Gehen Sie wie folgt vor: 1. Schließen Sie das Bestätigungsfenster für die Inaktivierung des Chips. 2. Geben Sie zum Ändern des Administratorkennworts das neue Kennwort ein, geben Sie das Bestätigungskennwort ein, und klicken Sie anschließend auf **Ändern**. Drücken Sie, nachdem Sie das Bestätigungskennwort eingegeben haben, nicht die Eingabetaste oder die Tabulatortaste zusammen mit der Eingabetaste.

Fehlerbehebungsinformationen zum Benutzerkonfigurationsprogramm

Die folgenden Informationen zur Fehlerbehebung können hilfreich sein, wenn bei der Verwendung des Benutzerkonfigurationsprogramms Fehler auftreten.

Fehlersymptom	Mögliche Lösung
Benutzer mit eingeschränkter Berechtigung können gewisse Funktionen des Benutzerkonfigurationsprogramms unter Windows XP Professional nicht ausführen	**Maßnahme**
Benutzer von Windows XP Professional mit eingeschränkter Berechtigung können möglicherweise folgende Tasks im Benutzerkonfigurationsprogramm nicht ausführen: • Den UVM-Verschlüsselungstext ändern • Das mit UVM registrierte Windows-Kennwort aktualisieren • Das Schlüsselarchiv aktualisieren	Dies ist eine bekannte Einschränkung bei Windows XP Professional. Dieser Fehler kann nicht behoben werden.

Fehlersymptom	Mögliche Lösung
Benutzer mit eingeschränkter Berechtigung können das Benutzerkonfigurationsprogramm unter Windows XP Home nicht ausführen	**Maßnahme**
Benutzer von Windows XP Home mit eingeschränkter Berechtigung können in den folgenden Fällen das Benutzerkonfigurationsprogramm nicht verwenden: • Client Security ist auf einer Partition im NTFS-Format installiert. • Der Windows-Ordner befindet sich auf einer Partition im NTFS-Format. • Der Archivordner befindet sich auf einer Partition im NTFS-Format.	Dies ist eine bekannte Einschränkung unter Windows XP Home. Dieser Fehler kann nicht behoben werden.

Fehlerbehebungsinformationen zum ThinkPad

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Verwendung von Client Security auf ThinkPads weiterhelfen können.

Fehlersymptom	Mögliche Lösung
Beim Versuch, eine Administratorfunktion von Client Security aufzurufen, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie versuchen, eine Administratorfunktion von Client Security durchzuführen, wird eine Fehlernachricht angezeigt.	Das ThinkPad-Administratorkennwort muss inaktiviert sein, damit Sie bestimmte Administratorfunktionen von Client Security ausführen können. Gehen Sie wie folgt vor, um das Administratorkennwort zu inaktivieren: 1. Rufen Sie mit ″F1″ das Programm ″IBM BIOS Setup Utility″ auf. 2. Geben Sie das aktuelle Administratorkennwort ein. 3. Geben Sie ein leeres neues Administratorkennwort ein, und bestätigen Sie das leere Kennwort. 4. Drücken Sie die Eingabetaste. 5. Drücken Sie die Taste F10, um die Einstellungen zu speichern und das Programm zu beenden.
Ein anderer UVM-Sensor für Fingerabdrücke funktioniert nicht ordnungsgemäß.	**Maßnahme**
Der IBM ThinkPad unterstützt den Wechsel zwischen mehreren UVM-Sensoren für Fingerabdrücke nicht.	Wechseln Sie die Modelle der Sensoren für Fingerabdrücke nicht. Verwenden Sie bei der Arbeit von einem fernen Standort aus stets das gleiche Modell wie bei der Arbeit an einer Andockstation.

Fehlerbehebungsinformationen zu Microsoft-Anwendungen und -Betriebssystemen

Die folgenden Fehlerbehebungstabellen enthalten Informationen zur Fehlerbehebung bei der Verwendung von Client Security mit Microsoft-Anwendungen oder -Betriebssystemen.

Fehlersymptom	**Mögliche Lösung**
Bildschirmschoner wird nur auf lokaler Anzeige angezeigt	**Maßnahme**
Bei Verwendung des erweiterten Windows-Desktop wird der Client Security-Bildschirmschoner nur auf der lokalen Anzeige angezeigt, obwohl der Zugriff auf das System und die Tastatur geschützt wird.	Wenn sensible Informationen angezeigt werden, verkleinern Sie die Fenster auf Ihrem erweiterten Desktop auf Symbolgröße, bevor Sie den Client Security-Bildschirmschoner aufrufen.
Client Security funktioniert für einen in UVM registrierten Benutzer nicht ordnungsgemäß.	**Maßnahme**
Der registrierte Clientbenutzer hat möglicherweise seinen Windows-Benutzernamen geändert. Wenn dies zutrifft, geht die gesamte Funktionalität von Client Security verloren.	Registrieren Sie den neuen Benutzernamen in UVM erneut, und fordern Sie alle neuen Berechtigungsnachweise an.
Anmerkung: Unter Windows XP werden in UVM registrierte Benutzer, deren Windows-Benutzername zuvor geändert wurde, von UVM nicht erkannt. Diese Einschränkung gilt selbst dann, wenn der Windows-Benutzername vor der Installation von Client Security geändert wurde.	
Fehler beim Lesen verschlüsselter E-Mails mit Outlook Express	**Maßnahme**
Verschlüsselte E-Mails können nicht entschlüsselt werden, da sich die Verschlüsselungsgrade der Webbrowser, die vom Sender und vom Empfänger verwendet werden, unterscheiden.	Überprüfen Sie Folgendes: 1. Der Verschlüsselungsgrad des Webbrowsers beim Sender muss mit dem Verschlüsselungsgrad des Webbrowsers des Empfängers kompatibel sein. 2. Der Verschlüsselungsgrad des Webbrowsers muss mit dem Verschlüsselungsgrad der Firmware von Client Security kompatibel sein.
Fehler bei der Verwendung eines Zertifikats von einer Adresse, der mehrere Zertifikate zugeordnet sind	**Maßnahme**
Outlook Express kann mehrere Zertifikate zu einer einzigen E-Mail-Adresse auflisten, und einige dieser Zertifikate können ungültig werden. Ein Zertifikat kann ungültig werden, wenn der private Schlüssel für das Zertifikat im integrierten IBM Sicherheits-Subsystem des Sender-Computers, auf dem das Zertifikat erstellt wurde, nicht mehr existiert.	Bitten Sie den Empfänger, sein digitales Zertifikat erneut zu senden; wählen Sie anschließend dieses Zertifikat im Adressbuch von Outlook Express aus.

Fehlersymptom	Mögliche Lösung
Beim Versuch, eine E-Mail digital zu signieren, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn der Verfasser einer E-Mail versucht, eine E-Mail digital zu signieren, jedoch seinem E-Mail-Account noch kein Zertifikat zugeordnet ist, wird eine Fehlernachricht angezeigt.	Verwenden Sie die Sicherheitseinstellungen in Outlook Express, um ein Zertifikat anzugeben, das dem Benutzeraccount zugeordnet werden soll. Weitere Informationen hierzu finden Sie in der Dokumentation zu Outlook Express.
Outlook Express (128 Bit) verschlüsselt E-Mails nur mit dem 3DES-Algorithmus.	**Maßnahme**
Beim Senden verschlüsselter E-Mails zwischen Clients, die Outlook Express mit der 128-Bit-Version von Internet Explorer 4.0 oder 5.0 verwenden, kann nur der 3DES-Algorithmus verwendet werden.	Aktuelle Informationen zu den Verschlüsselungsalgorithmen, die mit Outlook Express verwendet werden, erhalten Sie bei Microsoft.
Outlook Express-Clients senden E-Mails mit einem anderen Algorithmus zurück.	**Maßnahme**
Eine mit dem RC2(40)-, RC2(64)- oder RC2(128)-Algorithmus verschlüsselte E-Mail wird von einem Client mit Netscape Messenger an einen Client mit Outlook Express (128 Bit) gesendet. Eine vom Outlook Express-Client zurückgesendete E-Mail wird mit dem Algorithmus RC2(40) verschlüsselt.	Es ist keine Maßnahme erforderlich. Eine Verschlüsselungsanforderung gemäß RC2(40), RC2(64) oder RC2(128) von einem Netscape-Client an einen Outlook Express-Client (128 Bit) wird an den Netscape-Client immer mit dem RC2(40)-Algorithmus zurückgesendet. Aktuelle Informationen zu den Verschlüsselungsalgorithmen, die mit den verschiedenen Versionen von Outlook Express verwendet werden, erhalten Sie von Microsoft.
Bei der Verwendung eines Zertifikats in Outlook Express wird nach dem Ausfall eines Festplattenlaufwerks eine Fehlernachricht angezeigt.	**Maßnahme**
Zertifikate können im Administratordienstprogramm mit der Wiederherstellungsfunktion für Schlüssel wiederhergestellt werden. Möglicherweise sind einige Zertifikate, wie z. B. die kostenfreien Zertifikate von VeriSign, nach einer Schlüsselwiederherstellung nicht wiederhergestellt.	Führen Sie nach der Wiederherstellung der Schlüssel einen der folgenden Schritte aus: • Fordern Sie neue Zertifikate an. • Registrieren Sie die Zertifizierungsinstanz erneut in Outlook Express.
Outlook Express aktualisiert den dem Zertifikat zugeordneten Verschlüsselungsgrad nicht.	**Maßnahme**
Wenn ein Sender den Verschlüsselungsgrad in Netscape auswählt und eine signierte E-Mail an einen Outlook Express-Client mit Internet Explorer 4.0 (128 Bit) sendet, stimmt möglicherweise der Verschlüsselungsgrad der zurückgesendeten E-Mail nicht überein.	Löschen Sie das zugeordnete Zertifikat aus dem Adressbuch von Outlook Express. Öffnen Sie die signierte E-Mail erneut, und fügen Sie dem Adressbuch von Outlook Express das Zertifikat hinzu.

Fehlersymptom	Mögliche Lösung
In Outlook Express wird eine Nachricht über Entschlüsselungsfehler angezeigt.	**Maßnahme**
Sie können in Outlook Express eine Nachricht öffnen, indem Sie doppelt darauf klicken. Wenn Sie zu schnell auf eine verschlüsselte Nachricht klicken, wird in einigen Fällen eine Nachricht über Entschlüsselungsfehler angezeigt.	Schließen Sie die Nachricht, und öffnen Sie die verschlüsselte E-Mail erneut.
Darüber hinaus wird möglicherweise in der Voranzeige eine Fehlernachricht angezeigt, wenn Sie eine verschlüsselte Nachricht auswählen.	Wenn in der Voranzeige eine Fehlernachricht angezeigt wird, ist keine Maßnahme erforderlich.
Wenn Sie bei verschlüsselten E-Mails zwei Mal auf die Schaltfläche "Senden" klicken, wird eine Fehlernachricht angezeigt	**Maßnahme**
Wenn Sie in Outlook Express zweimal auf die Schaltfläche zum Senden klicken, um eine verschlüsselte E-Mail zu senden, wird eine Fehlernachricht darüber angezeigt, dass die Nachricht nicht gesendet werden konnte.	Schließen Sie die Fehlernachricht, und klicken Sie einmal auf **Senden**.
Beim Anfordern eines Zertifikats wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie Internet Explorer verwenden, wird Ihnen bei der Anforderung eines Zertifikats, das das CSP-Modul des integrierten IBM Sicherheits-Subsystems verwendet, möglicherweise eine Fehlernachricht angezeigt.	Fordern Sie das digitale Zertifikat erneut an.

Fehlerbehebungsinformationen zu Netscape-Anwendungen

Die folgenden Fehlerbehebungstabellen enthalten Informationen zur Fehlerbehebung bei der Verwendung von Client Security mit Netscape-Anwendungen.

Fehlersymptom	Mögliche Lösung
Fehler beim Lesen verschlüsselter E-Mails	**Maßnahme**
Verschlüsselte E-Mails können nicht entschlüsselt werden, da sich die Verschlüsselungsgrade der Webbrowser, die vom Sender und vom Empfänger verwendet werden, unterscheiden.	Überprüfen Sie Folgendes: 1. Der Verschlüsselungsgrad des vom Sender verwendeten Webbrowsers ist mit dem Verschlüsselungsgrad des vom Empfänger verwendeten Webbrowsers kompatibel. 2. Der Verschlüsselungsgrad des Webbrowsers ist mit dem Verschlüsselungsgrad kompatibel, der von der Firmware von Client Security bereitgestellt wird.

Fehlersymptom	Mögliche Lösung
Beim Versuch, eine E-Mail digital zu signieren, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn das Zertifikat des integrierten IBM Sicherheits-Subsystems in Netscape Messenger nicht ausgewählt wurde und der Verfasser der E-Mail versucht, diese mit dem Zertifikat zu signieren, wird eine Fehlernachricht angezeigt.	Verwenden Sie zur Auswahl des Zertifikats die Sicherheitseinstellungen in Netscape Messenger. Wenn Netscape Messenger geöffnet ist, klicken Sie in der Symbolleiste auf das Sicherheitssymbol. Das Fenster mit den Sicherheitsinformationen wird geöffnet. Klicken Sie im linken Teilfenster auf **Netscape Messenger**, und wählen Sie anschließend **Zertifikat des integrierten IBM Security Chips** aus. Weitere Informationen hierzu finden Sie in der Dokumentation von Netscape.
Eine E-Mail wird mit einem anderen Algorithmus an den Client zurückgesendet.	**Maßnahme**
Eine mit dem RC2(40)-, RC2(64)- oder RC2(128)-Algorithmus verschlüsselte E-Mail wird von einem Client mit Netscape Messenger an einen Client mit Outlook Express (128 Bit) gesendet. Eine vom Outlook Express-Client zurückgesendete E-Mail wird mit dem Algorithmus RC2(40) verschlüsselt.	Es ist keine Maßnahme erforderlich. Eine Verschlüsselungsanforderung gemäß RC2(40), RC2(64) oder RC2(128) von einem Netscape-Client an einen Outlook Express-Client (128 Bit) wird an den Netscape-Client immer mit dem RC2(40)-Algorithmus zurückgesendet. Aktuelle Informationen zu den Verschlüsselungsalgorithmen, die mit den verschiedenen Versionen von Outlook Express verwendet werden, erhalten Sie von Microsoft.
Ein digitales Zertifikat, das vom integrierten IBM Sicherheits-Subsystem generiert wurde, kann nicht verwendet werden.	**Maßnahme**
Das digitale Zertifikat, das vom integrierten IBM Sicherheits-Subsystem erstellt wurde, kann nicht verwendet werden.	Überprüfen Sie, ob Sie beim Öffnen von Netscape den richtigen UVM-Verschlüsselungstext eingegeben haben. Wenn Sie den falschen UVM-Verschlüsselungstext eingeben, wird eine Fehlernachricht über einen Authentifizierungsfehler angezeigt. Wenn Sie auf **OK** klicken, wird Netscape zwar geöffnet, Sie können aber das vom integrierten IBM Sicherheits-Subsystem generierte Zertifikat nicht verwenden. Sie müssen Netscape verlassen und erneut öffnen und anschließend den richtigen UVM-Verschlüsselungstext eingeben.
Neue digitale Zertifikate vom selben Sender werden innerhalb von Netscape nicht ausgetauscht.	**Maßnahme**
Wenn eine digital signierte E-Mail vom selben Sender mehrmals empfangen wird, wird das erste digitale Zertifikat, das der E-Mail zugeordnet ist, nicht überschrieben.	Wenn Sie mehrere E-Mail-Zertifikate empfangen, ist das einzige Zertifikat das Standardzertifikat. Löschen Sie mit den Sicherheitseinrichtungen in Netscape das erste Zertifikat, und öffnen Sie anschließend das zweite Zertifikat erneut, oder bitten Sie den Sender, eine weitere signierte E-Mail zu senden.

Fehlersymptom	Mögliche Lösung
Das Zertifikat des integrierten IBM Sicherheits-Subsystems kann nicht exportiert werden.	**Maßnahme**
Das Zertifikat des integrierten IBM Sicherheits-Subsystems kann in Netscape nicht exportiert werden. Die Exportfunktion in Netscape können Sie zum Sichern von Zertifikaten verwenden.	Rufen Sie das Administratordienstprogramm oder Benutzerkonfigurationsprogramm auf, um das Schlüsselarchiv zu aktualisieren. Wenn Sie das Schlüsselarchiv aktualisieren, werden Kopien von allen Zertifikaten des integrierten IBM Sicherheits-Subsystems erstellt.
Beim Versuch, ein wiederhergestelltes Zertifikat nach dem Ausfall eines Festplattenlaufwerks zu verwenden, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Zertifikate können im Administratordienstprogramm mit der Wiederherstellungsfunktion für Schlüssel wiederhergestellt werden. Möglicherweise sind einige Zertifikate, wie z. B. die kostenfreien Zertifikate von VeriSign, nach einer Schlüsselwiederherstellung nicht wiederhergestellt.	Fordern Sie nach dem Wiederherstellen der Schlüssel ein neues Zertifikat an.
Der Netscape-Agent wird geöffnet und verursacht einen Fehler in Netscape.	**Maßnahme**
Das Öffnen des Netscape-Agenten führt zum Schließen von Netscape.	Schalten Sie den Netscape-Agenten aus.
Netscape wird mit zeitlicher Verzögerung geöffnet.	**Maßnahme**
Wenn Sie das PKCS #11-Modul des integrierten IBM Sicherheits-Subsystems hinzufügen und anschließend Netscape öffnen, kommt es zu einer kurzen zeitlichen Verzögerung, bevor Netscape geöffnet werden kann.	Es ist keine Maßnahme erforderlich. Dies dient lediglich zu Ihrer Information.

Fehlerbehebungsinformationen zu digitalen Zertifikaten

Die folgenden Informationen zur Fehlerbehebung können hilfreich sein, wenn bei der Anforderung eines digitalen Zertifikats Fehler auftreten.

Fehlersymptom	**Mögliche Lösung**
Das Fenster "UVM-Verschlüsselungstext" oder das Fenster für die Authentifizierung über Fingerabdrücke wird bei der Anforderung eines digitalen Zertifikats mehrmals angezeigt.	**Maßnahme**
In der UVM-Sicherheits-Policy ist festgelegt, dass ein Benutzer sich mit einem UVM-Verschlüsselungstext oder über Fingerabdrücke authentifizieren muss, bevor er ein digitales Zertifikat erhalten kann. Wenn der Benutzer versucht, ein Zertifikat zu erhalten, wird das Authentifizierungsfenster, in dem er aufgefordert wird, den UVM-Verschlüsselungstext anzugeben oder die Fingerabdrücke abtasten zu lassen, mehrmals angezeigt.	Geben Sie bei jedem Öffnen des Authentifizierungsfensters den UVM-Verschlüsselungstext ein bzw. lassen Sie ihre Fingerabdrücke abtasten.
Eine Nachricht über einen VBScript- oder JavaScript-Fehler wird angezeigt.	**Maßnahme**
Wenn Sie ein digitales Zertifikat anfordern, wird möglicherweise eine Fehlernachricht angezeigt, die sich auf VBScript oder JavaScript bezieht.	Starten Sie den Computer erneut, und beziehen Sie das Zertifikat erneut.

Fehlerbehebungsinformationen zu Tivoli Access Manager

Die folgenden Informationen zur Fehlerbehebung können hilfreich sein, wenn bei der Verwendung von Tivoli Access Manager in Verbindung mit Client Security Fehler auftreten.

Fehlersymptom	**Mögliche Lösung**
Die lokalen Policy-Einstellungen entsprechen nicht denen auf dem Server.	**Maßnahme**
Tivoli Access Manager lässt bestimmte Bit-Konfigurationen zu, die von UVM nicht unterstützt werden. Folglich können lokale Policy-Anforderungen Einstellungen überschreiben, die ein Administrator bei der Konfiguration eines PD-Servers vorgenommen hat.	Dies ist eine bekannte Einschränkung.
Kein Zugriff auf die Konfigurationseinstellungen von Tivoli Access Manager	**Maßnahme**
Im Administratordienstprogramm kann auf der Seite zur Policy-Installation weder auf die Konfigurationseinstellungen von Tivoli Access Manager noch auf die entsprechenden Einstellungen zur lokalen Cache-Einrichtung zugegriffen werden.	Installieren Sie Tivoli Access Manager Runtime Environment. Wenn die Laufzeitumgebung (Runtime Environment) auf dem IBM Client nicht installiert ist, sind auf der Seite zur Policy-Installation auch keine Einstellungen für Tivoli Access Manager verfügbar.
Eine Benutzersteuerung gilt sowohl für den Benutzer als auch für die Gruppe.	**Maßnahme**
Wenn Sie beim Konfigurieren des Tivoli Access Manager-Servers einen Benutzer für eine Gruppe definieren, gilt die Benutzersteuerung sowohl für den Benutzer als auch für die Gruppe, wenn die Option **Traverse-bit** aktiviert wurde.	Es ist keine Maßnahme erforderlich.

Fehlerbehebungsinformationen zu Lotus Notes

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Verwendung von Lotus Notes mit Client Security weiterhelfen können.

Fehlersymptom	**Mögliche Lösung**
Nach dem Aktivieren des UVM-Schutzes für Lotus Notes kann Lotus Notes die Konfiguration nicht fertig stellen.	**Maßnahme**
Lotus Notes kann nach dem Aktivieren des UVM-Schutzes mit dem Administratordienstprogramm die Konfiguration nicht fertig stellen.	Dies ist eine bekannte Einschränkung. Lotus Notes muss konfiguriert werden und aktiv sein, bevor die Lotus Notes-Unterstützung im Administratordienstprogramm aktiviert wird.
Beim Versuch, das Notes-Kennwort zu ändern, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie das Notes-Kennwort bei Verwendung von Client Security ändern, wird dies in einer Fehlernachricht angezeigt.	Wiederholen Sie die Kennwortänderung. Wurde der Fehler dadurch nicht behoben, starten Sie den Client neu.
Nach dem Festlegen eines Kennworts per Zufallsgenerator wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie folgende Vorgänge ausführen, wird möglicherweise eine Fehlernachricht angezeigt: • Verwenden des Tools zur Lotus Notes-Konfiguration zur Einstellung des UVM-Schutzes für eine Notes-ID • Öffnen von Notes und Verwenden der Notes-Funktion zur Kennwortänderung für die Datei mit der Notes-ID • Schließen von Notes sofort nach der Kennwortänderung	Klicken Sie auf **OK**, um die Fehlernachricht zu schließen. Es ist keine weitere Maßnahme erforderlich. Entgegen der Fehlernachricht wurde das Kennwort geändert. Das neue Kennwort wurde von Client Security per Zufallsgenerator festgelegt. Die Datei mit der Notes-ID wird nun mit dem per Zufallsgenerator festgelegten Kennwort verschlüsselt, und der Benutzer benötigt keine neue Benutzer-ID-Datei. Wenn der Endbenutzer das Kennwort erneut ändert, generiert UVM ein neues, per Zufallsgenerator festgelegtes Kennwort für die Notes-ID.

Fehlerbehebungsinformationen zur Verschlüsselung

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Verschlüsselung von Dateien unter Verwendung von Client Security ab Version 3.0 weiterhelfen können.

Fehlersymptom	**Mögliche Lösung**
Bereits verschlüsselte Dateien werden nicht entschlüsselt.	**Maßnahme**
Dateien, die mit früheren Versionen von Client Security verschlüsselt wurden, werden nach dem Upgrade auf Client Security ab Version 3.0 nicht entschlüsselt.	Dies ist eine bekannte Einschränkung. Sie müssen alle mit früheren Versionen von Client Security verschlüsselten Dateien entschlüsseln, *bevor* Sie Client Security ab Version 3.0 installieren. Client Security 3.0 kann Dateien, die von früheren Versionen von Client Security verschlüsselt wurden, nicht entschlüsseln, da in dieser Version die Implementierung der Dateiverschlüsselung geändert wurde.

Fehlerbehebungsinformationen zu UVM-sensitiven Einheiten

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Verwendung UVM-sensitiver Einheiten weiterhelfen können.

Fehlersymptom	**Mögliche Lösung**
Eine UVM-sensitive Einheit funktioniert nicht mehr ordnungsgemäß.	**Maßnahme**
Eine UVM-sensitive Sicherheitseinheit, wie z. B. eine Smartcard, ein Kartenlesegerät für Smartcards oder ein Lesegerät für Fingerabdrücke, funktioniert nicht ordnungsgemäß.	Überprüfen Sie, ob die Einheit ordnungsgemäß vom System konfiguriert wurde. Nachdem die Einheit konfiguriert wurde, müssen Sie möglicherweise das System erneut starten, damit der Service richtig ausgeführt wird. Weitere Informationen zur Fehlerbehebung finden Sie auch in der Dokumentation zu der entsprechenden Einheit. Sie können sich auch die Verkaufsstelle wenden, bei der Sie die Einheit erworben haben.
Eine UVM-sensitive Einheit funktioniert nicht mehr ordnungsgemäß.	**Maßnahme**
Wenn Sie eine UVM-sensitive Einheit vom USB-Anschluss (Universal Serial Bus) trennen und die Einheit danach erneut am USB-Anschluss anschließen, funktioniert die Einheit möglicherweise nicht ordnungsgemäß.	Starten Sie nach dem erneuten Anschluss der Einheit an den USB-Anschluss den Computer erneut.

Anhang A. Informationen zu Kennwörtern und Verschlüsselungstexten

Dieser Anhang enthält Informationen zu Kennwörtern und Verschlüsselungstexten.

Regeln für Kennwörter und Verschlüsselungstexte

Bei einem gesicherten System wird eine Vielzahl verschiedener Kennwörter und Verschlüsselungstexte verwendet. Für unterschiedliche Kennwörter gelten unterschiedliche Regeln. Dieser Abschnitt enthält Informationen zum Administratorkennwort und zum UVM-Verschlüsselungstext.

Regeln für Administratorkennwörter

Die Regeln für das Administratorkennwort können nicht von einem Sicherheitsadministrator geändert werden.

Für Administratorkennwörter gelten folgende Regeln:

Länge Das Kennwort muss genau acht Zeichen lang sein.

Zeichen
Das Kennwort darf nur alphanumerische Zeichen enthalten. Die Kombination von Buchstaben und Ziffern ist zulässig. Es sind keine speziellen Zeichen wie das Leerzeichen und die Zeichen !, ?, % zulässig.

Merkmale
Sie können das Administratorkennwort festlegen, um den integrierten IBM Security Chip im Computer zu aktivieren. Dieses Kennwort müssen Sie bei jedem Zugriff auf das Administratordienstprogramm oder die Administratorkonsole eingeben.

Fehlversuche
Wenn Sie das Kennwort zehnmal falsch eingegebenen haben, wird der Computer 1 Stunde und 17 Minuten lang gesperrt. Wenn Sie nach diesem Zeitraum das Kennwort zehn weitere Male falsch eingeben, wird der Computer 2 Stunden und 34 Minuten lang gesperrt. Die Dauer der Computersperrung verdoppelt sich jedes Mal, wenn Sie das Kennwort zehnmal falsch eingeben.

Regeln für UVM-Verschlüsselungstexte

IBM Client Security bietet Sicherheitsadministratoren die Möglichkeit, Regeln für die UVM-Verschlüsselungstexte von Benutzern festzulegen. Die Sicherheit wird dadurch erhöht, dass der UVM-Verschlüsselungstext länger und eindeutiger ist als ein herkömmliches Kennwort. Die Policy für den UVM-Verschlüsselungstext wird über das Administratordienstprogramm gesteuert.

Das Fenster "Policy für UVM-Verschlüsselungstext" des Administratordienstprogramms stellt Sicherheitsadministratoren eine einfache Schnittstelle zur Steuerung von Kriterien für Verschlüsselungstexte bereit.

Über das Fenster ″Policy für UVM-Verschlüsselungstext″ kann der Administrator folgende Regeln für Verschlüsselungstexte festlegen:

Anmerkung: Die Standardeinstellung für jedes Kriterium ist unten in Klammern angegeben.

- ob eine Mindestanzahl an alphanumerischen Zeichen festgelegt werden soll (ja, 6)

  Wenn z. B. der Wert ″6″ festgelegt ist, ist der Verschlüsselungstext `1234567xxx` ungültig.
- ob eine Mindestanzahl an Ziffern festgelegt werden soll (ja, 1)

  Wenn z. B. der Wert ″1″ festgelegt ist, ist der Verschlüsselungstext `thisismypassword` ungültig.
- ob eine Mindestanzahl an Leerzeichen festgelegt werden soll (keine Mindestanzahl)

  Wenn z. B. der Wert ″2″ festgelegt ist, ist der Verschlüsselungstext `i am not here` ungültig.
- ob der Verschlüsselungstext mit einer Ziffer beginnen darf (nein)

  Standardmäßig ist z. B. der Verschlüsselungstext `1password` ungültig.
- ob der Verschlüsselungstext mit einer Ziffer enden darf (nein)

  Standardmäßig ist z. B. der Verschlüsselungstext `password8` ungültig.
- ob der Verschlüsselungstext eine Benutzer-ID enthalten darf (nein)

  Standardmäßig ist z. B. der Verschlüsselungstext `UserName` ungültig, wobei es sich bei `UserName` um eine Benutzer-ID handelt.
- ob der neue Verschlüsselungstext sich von den letzten x Verschlüsselungstexten unterscheiden muss (ja, 3)

  Standardmäßig ist z. B. der Verschlüsselungstext `mypassword` ungültig, wenn einer der drei vorherigen Verschlüsselungstexte `mypassword` war.
- ob der Verschlüsselungstext mehr als drei identische aufeinander folgende Zeichen des letzten Kennworts enthalten darf (nein)

  Standardmäßig ist z. B. der Verschlüsselungstext `password` ungültig, wenn der vorherige Verschlüsselungstext `pass` oder `word` war.

Das Fenster ″Policy für UVM-Verschlüsselungstext″ des Administratordienstprogramms ermöglicht Sicherheitsadministratoren zudem eine Steuerung des Ablaufs der Verschlüsselungstexte. Über das Fenster ″Policy für UVM-Verschlüsselungstext″ kann der Administrator aus den folgenden Regeln für Verschlüsselungstexte auswählen:

- Verschlüsselungstext ist nicht mehr gültig nach (ja, 184).

  Standardmäßig läuft der Verschlüsselungstext z. B. nach 184 Tagen ab. Der neue Verschlüsselungstext muss der vorhandenen Policy für den Verschlüsselungstext entsprechen.
- Entscheiden, ob der Verschlüsselungstext nie ablaufen soll (ja).

  Wenn diese Option ausgewählt ist, läuft der Verschlüsselungstext nie ab.

Die Policy für den Verschlüsselungstext wird vom Administratordienstprogramm bei der Registrierung des Benutzers und bei der Änderung des Verschlüsselungstextes durch den Benutzer über das Clientdienstprogramm überprüft. Die beiden Benutzereinstellungen zum vorherigen Kennwort werden zurückgesetzt, und Protokolle zum Verschlüsselungstext werden entfernt.

Folgende allgemeine Regeln gelten für UVM-Verschlüsselungstexte:

Länge Der Verschlüsselungstext kann bis zu 256 Zeichen lang sein.

Zeichen
Der Verschlüsselungstext kann eine beliebige Kombination aus Zeichen enthalten, die über die Tastatur eingegeben werden können, einschließlich Leerzeichen und nicht-alphanumerische Zeichen.

Merkmale
Der UVM-Verschlüsselungstext unterscheidet sich von einem Kennwort, das Sie zur Anmeldung am Betriebssystem verwenden können. Der UVM-Verschlüsselungstext kann in Verbindung mit anderen Authentifizierungseinheiten verwendet werden, z. B. mit einem UVM-Sensor für Fingerabdrücke.

Fehlversuche
Wenn der UVM-Verschlüsselungstext mehrere Male während einer Sitzung falsch eingegeben wird, führt der Computer eine Reihe entsprechender Verzögerungsaktionen durch. Diese Aktionen werden im folgenden Abschnitt beschrieben.

Anzahl der Fehlversuche auf TCPA-Systemen und anderen Systemen

In der folgenden Tabelle sind die Einstellungen für die Verzögerungsaktionen in einem TCPA-System dargestellt:

Versuche	Verzögerung beim nächsten Fehlversuch
15	1,1 Minuten
31	2,2 Minuten
47	4,4 Minuten
63	8,8 Minuten
79	17,6 Minuten
95	35,2 Minuten
111	1,2 Stunden
127	2,3 Stunden
143	4,7 Stunden

Auf TCPA-Systemen findet keine Unterscheidung zwischen Benutzerverschlüsselungstexten und Administratorkennwort statt. Alle Authentifizierungsmethoden unter Verwendung des integrierten IBM Security Chips richten sich nach derselben Policy. Die maximale Zeitsperre beträgt 4,7 Stunden. TCPA-Systeme führen keine Verzögerungsaktionen durch, die länger als 4,7 Stunden dauern.

Bei anderen Systemen findet eine Unterscheidung zwischen Administratorkennwort und Benutzerverschlüsselungstexten statt. Auf diesen Systemen wird für das Administratorkennwort nach 10 fehlgeschlagenen Versuchen eine Verzögerungsaktion von 77 Minuten ausgeführt. Für Benutzerkennwörter gilt nur eine einminütige Verzögerung nach 32 fehlgeschlagenen Versuchen. Nach weiteren 32 fehlgeschlagenen Versuchen wird die Sperrzeit jeweils verdoppelt.

Verschlüsselungstext zurücksetzen

Wenn ein Benutzer seinen Verschlüsselungstext vergisst, kann der Administrator den Benutzer dazu berechtigen, seinen Verschlüsselungstext zurückzusetzen.

Verschlüsselungstext über Remotezugriff zurücksetzen

Gehen Sie wie folgt vor, um ein Kennwort über Remotezugriff zurückzusetzen:

- **Administrator**

  Ein Administrator sollte über Remotezugriff wie folgt vorgehen:

  1. Erstellen Sie ein neues Kennwort zur einmaligen Verwendung für den Benutzer, und teilen Sie es dem Benutzer mit.
  2. Senden Sie eine Datendatei an den Benutzer.

     Sie können dem Benutzer diese Datendatei per E-Mail senden, auf einen austauschbaren Datenträger (wie z. B. eine Diskette) kopieren oder sie direkt in die Archivdatei des Benutzers schreiben (vorausgesetzt, der Benutzer verfügt über einen Zugriff auf dieses System). Diese verschlüsselte Datei ist zum Abgleich mit dem neuen Kennwort für eine einmalige Verwendung erforderlich.

- **Benutzer**

  Der Benutzer muss wie folgt vorgehen:

  1. Melden Sie sich auf dem Computer an.
  2. Wenn die Aufforderung zur Eingabe eines Verschlüsselungstextes angezeigt wird, aktivieren Sie das Markierungsfeld "Verschlüsselungstext vergessen".
  3. Geben Sie das Kennwort ein, das Ihnen der Administrator zur einmaligen Verwendung mitgeteilt hat, und geben Sie die Position der Datei an, die Sie vom Administrator erhalten haben.

     Nachdem UVM bestätigt hat, dass die Informationen in der Datei mit dem eingegebenen Kennwort übereinstimmen, erhält der Benutzer die Zugriffsberechtigung. Der Benutzer wird daraufhin sofort aufgefordert, seinen Verschlüsselungstext zu ändern.

Hierbei handelt es sich um die empfohlene Vorgehensweise zum Zurücksetzen eines verloren gegangenen Verschlüsselungstextes.

Verschlüsselungstext manuell zurücksetzen

Wenn der Administrator direkt auf das System des Benutzers, der seinen Verschlüsselungstext vergessen hat, zugreifen kann, kann er sich am System des Benutzers als Administrator anmelden, im Administratordienstprogramm den privaten Administratorschlüssel angeben und manuell den Verschlüsselungstext des Benutzers ändern. Zum Ändern des Verschlüsselungstextes ist es nicht erforderlich, dass der Administrator den alten Verschlüsselungstext des Benutzers kennt.

Anhang B. Bemerkungen und Marken

Dieser Anhang enthält rechtliche Hinweise zu IBM Produkten und Informationen zu Marken.

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in diesem Dokument beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Dienstleistungen von IBM verwendet werden können. Anstelle der Produkte, Programme oder Dienstleistungen können auch andere, ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen oder andere Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremddienstleistungen liegt beim Kunden.

Für in diesen Dokument beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder IBM Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanfragen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Europe
Director of Licensing
92066 Paris
La Defense Cedex
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekannt gegeben. IBM kann jederzeit ohne Vorankündigung Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängigen, erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse: IBM Corporation, Department 80D, P.O. Box 12195, 3039 Cornwallis, Research Triangle Park, NC 27709, U.S.A. Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesem Dokument aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der Allgemeinen Geschäftsbedingungen der IBM, der Internationalen Nutzungsbedingungen der IBM für Programmpakete oder einer äquivalenten Vereinbarung.

Marken

IBM und SecureWay sind in gewissen Ländern Marken der IBM Corporation.

Tivoli ist in gewissen Ländern eine Marke von Tivoli Systems Inc.

Microsoft, Windows und Windows NT sind in gewissen Ländern Marken der Microsoft Corporation.

Andere Namen von Unternehmen, Produkten und Dienstleistungen können Marken oder Dienstleistungsmarken anderer Unternehmen sein.