EK Certificate Policy

Version 1.0

Oct 9th, 2014

1. Table of Contents

2. TABLE OF FIGURES

No table of figures entries found.

3. INTRODUCTION

3.1 Overview

This document contains the Certificate Policies associated with Intel Corporation's Platform Trust Technology Endorsement Key PKI ("PKI") and its associated EK Certificate Authority ("CA").

The EK PKI was developed and established to support the generation, distribution, revocation and administrator of cryptographic keys and X.509 certificates required by Intel's Platform Trust Technology (PTT). The intent of the PKI is to generate Endorsement Key private keys, and corresponding digital certificates to meet the Trusted Platform Module specifications implemented by Intel's PTT. This document will address all aspects of the CA policies established to support the PKI.

This document will begin by covering the distribution points and publication details of this document. In following sections, the document describes details about identification and authentication processes, certificate life-cycle details including issuance, and revocation of digital certificates. A section on facility, business, technical, and operational controls will describe the security environment surrounding the CA. A section on compliance and legal requirements governing the CA will close out the document.

3.2 Document Name and Identification

The name of this document is EKcertPolicyStatement.pdf.

Policy OID id-intel-ftpm-certPolicy::= 1.2.840.113741.1.5.2.1

3.3 PKI Participants

The following are roles relevant to the administration and operation of CAs under this policy:

3.3.1 PKI Authorities

3.3.1.1 Certification Authority

The CA is the collection of hardware, software and operating personnel that create, sign, and issue public key certificates to PTT enabled devices. The CA is responsible for the issuing and managing certificates including:

- Approving the issuance of all device certificates
- Publication of certificates
- Revocation of certificates
- Generation and destruction of CA signing keys
- Establishing and maintaining the CA system
- Establishing and maintaining the Certificate Policy (CP) & Certification Practice Statement (CPS)
- Ensuring that all aspects of the CA services, operations, and infrastructure related to certificates issued under the CP are performed in accordance with the requirements of the CP

3.3.1.2 Certificate Status Servers

No Online Certificate Status Protocol (OSCP) responders are provided as part of this CA. All certificate status checks must be performed through a published Certificate Revocation List by the verifier.

3.3.2 Registration Authorities

This PKI only issues device certificates for Intel manufactured devices; therefore, the scope of the registration authority (RAs) is limited to:

- Authentication and management of the Intel's authorized organizational representative (AOR) requesting device certificates.
- Verification of the device certificate requests submitted by the AOR.

3.3.3 Trusted Agents

No stipulation

3.3.4 Subscribers

A subscriber is the entity whose name appears as the subject in a certificate. The subscriber asserts that he or she uses the key and certificate in accordance with the certificate policy asserted in the certificate, and does not issue certificates. However, in this case, since the subscriber is an electronic device, an Intel authorized organizational representative (AOR) will be responsible for requesting the EK Certificates.

3.3.5 Relying Parties

A Relying Party is an entity that relies on the validity of the binding of the Subscriber's name to a public key. The Relying Party uses a Subscriber's certificate to verify or establish the identity and status of a system or device. A Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. In the PKI a relying party is a third party component, either software or hardware, or external service wanted to attest the validity of the PTT module.

3.3.6 Other Participants

No stipulation

3.4 Certificate Usage

3.4.1 Appropriate Certificate Uses

Endorsement Key Certificates are generated to provide attestation capabilities for PTT enabled devices. The EK Certificate complies with the Trusted Computing Group's TPM specification, which establishes the use of a cryptographic key to sign the Attestation Identity Keys used in remote attestation, and a corresponding public key certificate to validate the signature.

3.4.2 Prohibited Certificate Uses

No stipulation.

3.5 Policy Administration

3.5.1 Organization Administering the Document

The Policy Authority is responsible for all aspects of this CP.

3.5.2 Contact Person

For any questions related to this policy please contact the Policy Authority at EKPolicy@intel.com.

3.5.3 Person Determining Suitability for the Policy

The Policy Authority shall approve each CA that issues certificates under the policy.

3.5.4 Approval Procedures

CAs issuing under the policy are required to meet all facets of the policy. The Policy Authority shall not issue waivers. The CA must meet all requirements of this policy before commencing operations.

3.5.5 Definitions and Acronyms

See sections 12 and 13**Error! Reference source not found.**. **Error! Reference source not found.**

4. Publication and Repository Responsibilities

4.1 Repositories

All CAs that issue certificates under this policy are obligated to post all CA certificates issued by or to the CA and CRLs issued by the CA in a repository that is publicly accessible through all Uniform Resource Identifier (URI) references asserted in valid certificates issued by that CA. To promote consistent access to certificates and CRLs, the repository shall implement access controls and communication mechanisms to prevent unauthorized modification or deletion of information.

4.2 Publication of Certification Information

4.2.1 Publication of Certificates and Certificate Status

The publicly accessible repository system shall be designed and implemented so as to provide 99% availability overall and limit scheduled down-time to 0.5% annually.

4.2.2 Publication of CA Information

The CP shall be publicly available.

4.3 Time or Frequency of Publication

An updated version of the CP will be made publicly available within 30 days of the incorporation of changes.

4.4 Access Controls on Repositories

The CA shall protect information not intended for public dissemination or modification. CA certificates and CRLs in the repository shall be publicly available through the Internet. Direct and/or remote access to other information in the CA repositories shall be determined by Policy Authority.

5. Identification and Authentication

5.1 Naming

5.1.1 Types of Names

The CA shall not assign a Distinguished Name (DN) to each device EK certificate, instead, it will assign an anonymous subject alternate name as follows:

```
SEQUENCE :
         OBJECT IDENTIFIER : subjectAltName [2.5.29.17]
         BOOLEAN : 'ÿ'
         OCTET STRING :
            SEQUENCE :
               CONTEXT SPECIFIC (4) :
                  SEQUENCE :
                     SET :
                        SEQUENCE :
                           OBJECT IDENTIFIER : tcpa_at_tpmManufacturer [2.23.133.2.1]
                           UTF8 STRING :
                              'id: <ManufactuerID>'
                     SET :
                        SEQUENCE :
                           OBJECT IDENTIFIER : tcpa_at_tpmModel [2.23.133.2.2]
                           UTF8 STRING :
                              '<ModelName>'
                     SET :
                        SEQUENCE :
                           OBJECT IDENTIFIER : tcpa_at_tpmVersion [2.23.133.2.3]
                           UTF8 STRING :
                              'id: :<TPM Version (XXXXYYYY where XXXX is major and YYYY is
                                    minor hex rev)>'
```

5.1.2 Need for Names to Be Meaningful

No stipulation.

5.1.3 Anonymity or Pseudonymity of Subscribers

All EK Certificates issued by the CA shall be anonymous. No information that uniquely identifies the device shall be included in the certificate.

5.1.4 Rules for Interpreting Various Name Forms

No stipulation.

5.1.5 Uniqueness of Names

Name uniqueness is not a requirement of this CA.

5.1.6 Recognition, Authentication, and Role of Trademarks

No stipulation.

5.2 Initial Identity Validation

5.2.1 Method to Prove Possession of Private Key

Key generation and distribution is performed under the CA's direct control and supervision, proof of private key possession is not required to issue device EK Certificate.

5.2.2 Authentication of Organization Identity

No stipulation.

5.2.3 Authentication of Individual Identity

5.2.3.1 Authentication of Human Subscribers

No stipulation.

5.2.3.2 Authentication of Devices

Key generation, distribution, and provisioning is performed under the CA's direct control, device authentication is not required for EK Certificate issuance. Nonetheless, an authorized organizational representative (AOR) must provide identifying information for the device(s) to be certified. The AOR is responsible for providing the following registration information:

- Device platform name and platform parameters
- Device application authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA to communicate with the AOR when required.

The registration information provided by the AOR shall be verified. The identity of the AOR shall be authenticated by:

1) Verify AOR's employment through use of official organization records.

2) Presentation of a handwritten application form including management approval.
3) Establish subscriber's identity by verifying corporate electronic records.

5.2.3.3 Authentication for Role Certificates

No stipulation.

5.2.4 Non-verified Subscriber Information

Information that is not verified shall not be included in certificates.

5.2.5 Validation of Authority

No stipulation.

5.2.6 Criteria for Interoperation

No interoperation between this CA issuing certificates under this policy and other CA(s) is permitted.

5.3 Identification and Authentication for Revocation Request

5.3.1 Identification and Authentication for Routine Re-key

No re-key is currently allowed of any EK Certificate issued by this CA.

5.3.2 Identification and Authentication for Re-key after Revocation

No re-key is currently allowed of any EK Certificate issued by this CA.

5.4 Identification and Authentication for Revocation Request

Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's public key, regardless of whether or not the associated private key has been compromised.

6. Certificate Life-cycle Operational Requirements

6.1 Certificate Application

The Certificate application process must provide sufficient information to:

- Establish the applicant's authorization (by the employing or sponsoring organization) to obtain a device EK certificate.
- Establish and record identity of the applicant.
- Verify the applicant's authorization for petitioning device EK certificate.
- Verify any information requested for inclusion in the certificate.

These steps may be performed in any order that is convenient for the PKI Authority and applicants that does not defeat security, but all must be completed before certificate issuance.

6.1.1 Who Can Submit a Certificate Application

6.1.1.1 CA Certificates

No stipulation.

6.1.1.2 User Certificates

No stipulation.

6.1.1.3 Device Certificates

An application for a device EK certificate shall be submitted by the device AOR.

6.1.2 Enrollment Process and Responsibilities

Any electronic transmission of shared secrets and personally identifiable information shall be protected. Communications may be electronic or out-of-band. Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair shall be used. Out-of-band communications shall protect the confidentiality and integrity of the data. Subscribers are responsible for providing accurate information on their certificate applications.

6.2 Certificate Application Processing

Information in certificate applications must be verified as accurate before certificates are issued. The PKI Authority shall specify procedures to verify information in certificate applications.

6.2.1 Performing Identification and Authentication Functions

The identification and authentication of the subscriber must meet the requirements specified for subscriber authentication as specified in Section 5.2.3.2. The PKI Authority must identify the components of the PKI (e.g., CA or RA) that are responsible for authenticating the subscriber's identity in each case.

6.2.2 Approval or Rejection of Certificate Applications

Any certificate application that is received by a CA under this policy, for which the identity and authorization of the applicant has been validated, will be duly processed. However, the CA must reject any application for which such validation cannot be completed, or when the CA has cause to lack confidence in the application or certification process.

6.2.3 Time to Process Certificate Applications

Certificate applications must be processed and a certificate issued within 30 of identity verification.

6.3 Certificate Issuance

6.3.1 CA Actions during Certificate Issuance

Upon receiving the request, the CA will:

- Verify the identity of the requester.
- Verify the authority of the requester and the integrity of the information in the certificate request.

- Build and sign a certificate if all certificate requirements have been met.
- Make the certificate available to the subscriber.

All authorization and other attribute information received from a prospective subscriber shall be verified before inclusion in a certificate.

6.3.2 Notification to Subscriber by the CA of Issuance of Certificate

CAs operating under this policy shall inform the subscriber (or other certificate subject) of the creation of a certificate. Device certificates must be made available within 30 days through the certificate provisioning protocol.

6.4 Certificate Acceptance

6.4.1 Conduct Constituting Certificate Acceptance

No stipulation.

6.4.2 Publication of the Certificate by the CA

As specified in Section **Error! Reference source not found.** , root and intermediate certificates shall be made available through public distribution points. Device EK certificates shall be made available through the certificate provisioning protocol.

6.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

6.5 Key Pair and Certificate Usage

6.5.1 Subscriber Private Key and Certificate Usage

The intended scope of usage for a private key is limited to the Endorsement Key required by the Trusted Computing Group TPM Family 2.0 Specification, Version 2.0.

6.5.2 Relying Party Public key and Certificate Usage

Certificates may specify restrictions on use through critical certificate extensions, including the basic constraints and key usage extensions. All CAs operating under this policy shall issue CRLs specifying the current status of all unexpired certificates. It is recommended that relying parties process and comply with this information whenever using certificates in a transaction.

6.6 Certificate Renewal

No stipulation.

6.7 Certificate Re-key

No stipulation.

6.8 Certificate Modification

No stipulation.

6.9 Certificate Revocation and Suspension

CAs operating under this policy shall issue CRLs covering all unexpired certificates issued under this policy. CAs operating under this policy shall include the CRL distribution point in the device EK certificate.
Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using the signed certificate to revoke, regardless of whether or not the private key has been compromised**.**
Certificate suspension for CA certificates or end entity certificates is not allowed by this policy.

6.9.1 Circumstances for Revocation

A certificate shall be revoked when the binding between the device and the device's public key defined within the certificate is no longer considered valid. Examples of circumstances that invalidate the binding are:

- There is reason to believe the private key has been compromised.
- The subscriber or other authorized party asks for his/her certificate to be revoked.

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on the CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

6.9.2 Who Can Request Revocation

Within the PKI, a CA may summarily revoke certificates within its domain. The AOR that owns or controls a device can request the revocation of the device's certificate.

6.9.3 Procedure for Revocation Request

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated and authorized (manually signed).

6.9.4 Revocation Request Grace Period

There is no grace period for revocation under this policy.

6.9.5 Time within which CA must Process the Revocation Request

CAs will revoke certificates as quickly as practical upon receipt of a proper revocation request. Revocation requests shall be processed before the next CRL is published.

6.9.6 Revocation Checking Requirements for Relying Parties

No stipulation.

6.9.7 CRL Issuance Frequency

CRLs shall be issued whenever a new certificate or group of certificates has been revoked, periodical CRL issuance is not required. CAs that issue certificates to subscribers or operate on-line must issue CRLs at least 30 days from the date a certificate revocation request is received.

6.9.8 Maximum Latency for CRLs

CRLs shall be published within 7 calendar days of generation.

6.9.9 On-line Revocation/Status Checking Availability

No stipulation.

6.9.10 On-line Revocation Checking Requirements

No stipulation.

6.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

6.9.12 Special Requirements Related To Key Compromise

No stipulation.

6.9.13 Circumstances for Suspension

6.9.13.1 Circumstances for Suspension

For CA certificates, suspension is not permitted. For end entity certificates, suspension is not permitted.

6.9.13.2 Who Can Request Suspension

No stipulation for end entity certificates.

6.9.13.3 Procedure for Suspension Request

No stipulation for end entity certificates.

6.9.13.4 Limits on Suspension Period

No stipulation for end entity certificates.

6.9.13.5 Circumstances for Restoration

No stipulation for end entity certificates.

6.9.13.6 Who Can Request Restoration

No stipulation for end entity certificates.

6.9.13.7 Procedure for Restoration Request

No stipulation for end entity certificates.

6.10 Certificate Status Services

No stipulation.

6.10.1 Operational Characteristics

No stipulation.

6.10.2 Service Availability

No stipulation.

6.10.3 Optional Features

No stipulation.

6.11 End of Subscription

No stipulation.

6.12 Key Escrow and Recovery

6.12.1 Key Escrow and Recovery Policy and Practices

CA private keys and device private keys are never escrowed.

6.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

7. Facility, Management, and Operational Controls

7.1 Physical Controls

All CA equipment, including cryptographic modules, shall be protected from theft, loss, and unauthorized access at all times. Unauthorized use of CA equipment is prohibited. CA equipment shall be dedicated to performing CA functions.

7.1.1 Site Location and Construction

The location and construction of the facility housing the CA equipment, as well as sites housing remote workstations used to administer the CAs, shall be consistent with facilities used to house high-value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, shall provide robust protection against unauthorized access to the CA equipment and records.

7.1.2 Physical Access

Physical access to equipment shall be limited to authorized personnel. The security mechanisms shall be commensurate with the level of threat in the equipment environment.

At a minimum, physical access controls for equipment shall meet the following requirements:

- Ensure that no unauthorized access to the hardware is permitted

- Be manually or electronically monitored for unauthorized intrusion at all times
- Require two-person physical access control. Technical or mechanical mechanisms (e.g., dual locks) shall be used to enforce the two-person physical access control
- Other individuals shall be escorted by two persons. This includes maintenance personnel.

When not in use, removable cryptographic modules, removable media, and any activation information used to access or enable cryptographic modules or equipment, or paper containing sensitive plain-text information shall be securely stored in a manner commensurate with the sensitivity, or value of the information being protected by the certificates issued by the CA. Access to this content shall be restricted to individuals holding CA trusted roles as defined in section 7.2.1.

Cryptographic modules shall only be removed by authorized personnel. No cryptographic module shall be removed from the facility without proper authorization, and shall be destroyed accordingly with Intel's data and equipment disposal policies.

Any activation information used to access or enable the cryptographic modules or equipment shall be stored separately from the associated modules and equipment. Such information shall either be memorized or recorded and stored in a manner commensurate with the security afforded the associated cryptographic module or equipment.

If unattended, the facility housing equipment shall be protected by video surveillance and intrusion detection systems. The video surveillance feed shall be recorded 24 x 7 and reviewed by authorized security personnel as needed. Unauthorized access to the facility shall be monitored automatically and reported immediately to security personnel through automated or electronic means. All ingress and egress points shall be equipped with sensors to detect access and must be monitored by active security system.

7.1.3 Power and Air Conditioning

Power and air conditioning backups shall be supported by Intel's infrastructure.

7.1.4 Water Exposures

CA equipment shall be installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors).

Potential water damage from fire prevention and protection measures (e.g., sprinkler systems) are excluded from this requirement.

7.1.5 Fire Prevention and Protection

The equipment shall be protected from potential fire damage by a gas or water based fire suppression system.

7.1.6 Media Storage

Media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic) and unauthorized physical access. Media not required for daily operation or not required by policy to remain with the CA shall be stored securely in a location separate from the equipment.

Media containing private key material shall be handled, packaged, and stored in a manner compliant with the requirements for the sensitivity level of the information it protects or provides access. Storage protection of private key material shall be consistent with stipulations in Section 7.1.2.

7.1.7 Waste Disposal

Personnel shall remove and destroy normal office waste in accordance with local policy. Media used to collect or transmit privacy information shall be destroyed, such that the information is unrecoverable, prior to disposal. Sensitive media and paper shall be destroyed in accordance with the applicable policy for destruction of such material.

7.1.8 Off-Site Backup

A system backup shall be made when a CA system is activated, and on a daily basis thereafter. Backups shall be stored offsite. Only the latest full backup and incremental backups need to be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA system.

7.2 Procedural Controls

7.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. It is essential that the people selected to fill these roles shall be held accountable to perform designated actions correctly or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust in the CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first approach is to minimize the number of trusted roles and ensure that the people filling those roles are trustworthy and properly trained. The second is to enforce the concept of least privilege and distribute the functions of the roles among several people, so that any malicious activity requires collusion.

Trusted role operations include:

- The validation, authentication, and handling of information in Certificate Applications
- The acceptance, rejection, or other processing of Certificate Applications, revocation requests, renewal requests, or enrollment information
- The issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository
- Access to safe combinations and/or keys to security containers that contain materials supporting production services
- Access to hardware security modules (HSMs), their associated keying material, and the smartcards that protect access to those modules.
- Access to any source code for the digital certificate applications or systems.
- Access to restricted portions of the certificate repository
- The ability to grant physical and/or logical access to the CA equipment

The only mandatory trusted roles defined by this policy are the System Administrator, Operations, Physical Security, Security Auditors, and RA Staff. Multiple people may hold the same trusted role, with collective privileges sufficient to fill the role. Other trusted roles may be defined in other documents, which describe or impose requirements on the CA operation.

The CA shall maintain lists, including names, organizations, contact information, and organizational affiliation for those who act in these roles, and shall make them available during compliance audits.

7.2.1.1 System Administrator

The administrator role shall be responsible for:

- Installation, configuration, and maintenance of the CA
- Establishing and maintaining CA system accounts
- Configuring CA equipment
- Generating and backing up CA keys and audit trails
- Controlling and managing CA cryptographic modules
- System backups and restore

System Administrators do not issue certificates to subscribers.

7.2.1.2 Operations Staff

The Operations Staff role shall be responsible for issuing certificates, that is:

- Verifying the identity of subscribers and accuracy of information included in certificates
- Executing the issuance of certificates
- Executing the revocation of certificates
- Executing revocation of certificates issued to CAs
- Posting Certificates and CRLs

7.2.1.3 Security Auditor

Security Auditors are responsible for auditing CAs and RAs. This sensitive role cannot be combined with any other sensitive role, e.g. the Security Auditor cannot also be part of the Operations Staff.

Performing or overseeing internal audits (independent of formal compliance audits) to ensure that CAs and RAs are operating in accordance with the associated policies.

7.2.1.4 RA Staff

RA Staff are the individuals that operate and manage RA processes. RA Staff is responsible for the following:

- Registering new subscriber and requesting the issuance of certificates
- Verifying the identity of subscribers
- Managing requests for revocation of certificates

7.2.2 Number of Persons Required per Task

Where multi-party control is required, all participants shall hold a trusted role. Multi-party control shall not be achieved using personnel that serve in a Security Auditor role with the exception of audit functions. The following tasks shall require two or more persons:

- Generation, and activation of CA keys
- Generation of device keys and certificates
- Performance of CA administration or maintenance tasks
- Physical access to CA equipment

- Access to any copy of the CA cryptographic module

7.2.3 Identification and Authentication for Each Role

Individuals holding trusted roles shall identify themselves and be authenticated by the CA before being permitted to perform any actions set forth above for that role or identity. CA equipment shall require, at a minimum, strong authenticated access control using multi-factor authentication. Examples of multi factor authentication include use of a password or PIN along with a smartcard that enforce a policy of what a user has and what a user knows. CA equipment shall require, at a minimum, authenticated access control (e.g., strong passwords) for local multi-party access.

7.2.3.1 Authentication: Passwords and Accounts

When the authentication mechanism uses operator selectable passwords, strong passwords shall be employed. Passwords for CA authentication shall be different from non-CA systems.

7.2.4 Roles Requiring Separation of Duties

Individuals serving as Security Auditors shall not perform or hold any other trusted role.

An individual that holds any Operations Staff role shall not be an RA except that CA Operations Staff may perform RA functions when issuing CA Certificates.

Only an individual serving in a Security Auditor role may perform internal auditing functions, with the exception of those security audit functions (e.g., configuring, archiving, deleting) that require multi-person control.

An individual that performs any trusted role shall only have one identity when accessing CA equipment.

7.3 Personnel Controls

Personnel Security plays a critical role in the CA facility's overall security system. Personnel Security shall be designed to prevent both unauthorized access to the CA facility and CA systems and compromise of sensitive CA operations by CA personnel.

Inadequate personnel security procedures or negligent enforcement of personnel security policies can pose potentially devastating threats to security. These threats can include unauthorized access, data loss and corruption, denial of service, and even facility sabotage and terrorism. Such events can erode or destroy customer confidence in the CA.

7.3.1 Qualifications, Experience, and Clearance Requirements

Personnel seeking to become Trusted Persons shall present proof of the requisite background, qualifications and experience needed to perform their prospective job responsibilities competently and satisfactorily.

Individuals appointed to any trusted role shall meet the following:

- Be employees of or contractor/vendor of the CA and bound by terms of employment or contract
- Have successfully completed the appropriate training
- Have demonstrated the ability to perform their duties

- Have no other duties that would interfere or conflict with their responsibilities as defined in Section 7.2.1

7.3.2 Background Check Procedures

CAs shall adhere to Intel Corporation's background check policies.

7.3.3 Training Requirements

All personnel performing duties with respect to the operation of the CA shall receive training associated with all PKI duties they are expected to perform.

7.3.4 Retraining Frequency and Requirements

All individuals responsible for PKI Trusted Roles shall be made aware of changes in the operation. Any significant change to the operations shall require the necessary training for the roles impacted.

7.3.5 Job Rotation Frequency and Sequence

No stipulation.

7.3.6 Sanctions for Unauthorized Actions

Appropriate administrative and disciplinary actions as documented in organization policy shall be taken against personnel who perform unauthorized actions involving the CA's systems, security systems, and the repository.

7.3.7 Independent Contractor Requirements

Contractor personnel filling trusted roles shall be subject to all requirements stipulated in this document. Independent contractors and consultants who have not completed or passed the background check procedures specified above shall be permitted access to the CA's secure facilities only to the extent they are escorted and directly supervised by a person holding trusted role at all times.

7.3.8 Documentation Supplied to Personnel

Documentation sufficient to operate the CA shall be provided to the appropriate personnel.

7.4 Audit Logging Procedures

Audit log files shall be generated for all events relating to the security of the CA. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

7.4.1 Types of Events Recorded

All security auditing capabilities of the operating system and applications shall be enabled during installation. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event;
- The date and time the event occurred;

- Success or failure where appropriate, and
- The identity of the entity and/or operator that caused the event.

The CA shall record the events identified in the list below. Where these events cannot be electronically logged, the CA shall supplement electronic audit logs with physical logs as necessary.

- IDENTIFICATION AND AUTHENTICATION:
  - Successful and unsuccessful attempts to assume a role
  - Addition and deletion of user accounts
  - Attempts to set passwords
  - Attempts to modify passwords
  - Logon attempts to applications
- LOCAL DATA ENTRY:
  - All security-relevant data that is entered in the application
- DATA EXPORT AND OUTPUT:
  - All export and output of confidential and security-relevant information from the CA application
- KEY GENERATION:
  - Whenever the CA generates a key
- PRIVATE KEY LOAD AND STORAGE:
  - The loading of Component private keys
- TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE:
  - All changes to the trusted public keys, including additions and deletions
- SECRET KEY STORAGE:
  - The generation and storage of private keys
- PRIVATE AND SECRET KEY EXPORT:
  - The export of private and secret keys
- CERTIFICATE REGISTRATION:
  - All certificate requests
- CERTIFICATE REVOCATION:
  - All certificate revocation requests
- CA CONFIGURATION:
  - Installation of the CA
  - Installing cryptographic modules
  - Removing cryptographic modules
  - Re-key of the CA

    - Destruction of cryptographic modules
    - System startup
    - Any security-relevant changes to the configuration of the CA
- ACCOUNT ADMINISTRATION:
    - Roles and users are added or deleted
    - The access control privileges of a user account or a role are modified
    - Appointment of an individual to a trusted role
    - Designation of personnel for multi-party control
- CERTIFICATE PROFILE MANAGEMENT:
    - All changes to the certificate profile
- REVOCATION PROFILE MANAGEMENT:
    - All changes to the revocation profile
- CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT:
    - All changes to the certificate revocation list profile
- MISCELLANEOUS:
    - Backing up CA internal database
    - Restoring CA internal database
- Configuration changes to the CA server involving:
    - Hardware
    - Software
    - Operating system
    - Patches
    - Security profiles
- PHYSICAL ACCESS / SITE SECURITY:
    - Personnel access to room housing CA
    - Access to the CA server
    - Known or suspected violations of physical security
    - Any removal or addition of equipment to the CA enclosure.
- ANOMALIES:
    - Software error conditions
    - Receipt of improper input
    - Operating system errors

7.4.2 Frequency of Processing Log

No predefined frequency of review is defined by this policy. All significant events shall be explained in an audit log summary. Reviews involve briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Real-time automated analysis tools should be used when possible. All critical alerts generated by such a systems shall be analyzed.

7.4.3 Retention Period for Audit Log

Audit logs generated by the CA application shall be retained for 5 years.

7.4.4 Protection of Audit Log

The security audit data shall not be open for reading or modification by any human, or by any automated process, other than those authorized.

Electronic logs within the CA application shall be protected to prevent alteration and detect tampering. Examples include keyed hashing of audit records to detect modifications.

Physical logbooks shall implement controls to allow for the detection of the removal of pages or deletion of entries.

CA system configuration and procedures must be implemented together to ensure that only authorized people archive CA application data.

7.4.5 Audit Log Backup Procedures

CA application audit logs and audit summaries shall be backed up at least every 1 day. A copy of the audit log shall be sent off-site every 1 day.

7.4.6 Audit Collection System (Internal vs. External)

The audit log collection system may or may not be external to the system. Automated audit processes shall be invoked at system or application startup, and cease only at system or application shutdown. Audit collection systems shall be configured such that security audit data is protected against loss (e.g., overwriting or overflow of automated log files). Should it become apparent that an automated audit system has failed; CA operations shall be suspended until the security audit capability can be restored.

7.4.7 Notification to Event-Causing Subject

There is no requirement to notify a subject that an event was audited. Real-time alerts are neither required nor prohibited by this policy.

7.4.8 Vulnerability Assessments

No stipulation.

7.5 Records Archival

7.5.1 Types of Events Archived

CA archive records shall be sufficiently detailed to determine the proper operation of the CA and the validity of any certificate (including those revoked or expired) issued by the CA. At a minimum, the following data shall be recorded for archive:

- Certificate policy
- Contractual obligations
- All Necessary Audit logs
- Compliance Auditor reports
- Documentation related to the operation of the CA equipment

Many other relevant CA operations events are recorded in the audit logs, and archived with those logs.

7.5.2 Retention Period for Archive

Archive records must be kept for a minimum of 5 years.

7.5.3 Protection of Archive

No unauthorized user shall be permitted to write to, modify, or delete the archive.

7.5.4 Archive Backup Procedures

No stipulation.

7.5.5 Requirements for Time-Stamping of Records

No stipulation.

7.5.6 Archive Collection System (Internal or External)

No stipulation.

7.5.7 Procedures to Obtain and Verify Archive Information

No stipulation.

7.6 Key Changeover

No stipulation.

7.7 Compromise and Disaster Recovery

7.7.1 Incident and Compromise Handling Procedures

If compromise of a CA is suspected an investigation shall be performed in order to determine the nature and the degree of damage. Certificates issued off that CA shall be stopped immediately upon detection of a compromise. If a CA private signing key is suspected of compromise, the procedures outlined in

Section 7.7.3 shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA private key needs to be declared compromised.

The personnel shall notify the Policy Authority in the case of a root CA or notify the superior CA in the case of a subordinate CA if any of the following occur:

- Suspected or detected compromise of any CA system or subsystem
- Physical or electronic penetration of any CA system or subsystem
- Successful denial of service attacks on any CA system or subsystem
- Any incident preventing a CA from issuing and publishing a CRL that violates sections 6.9.7.

7.7.2 Computing Resources, Software, and/or Data Are Corrupted

When computing resources, software, and/or data are corrupted, CAs operating under this policy shall respond as follows:

- Ensure that the system's integrity has been restored prior to returning to operation and determine the extent of loss of data since the last point of backup.
- If the CA signing keys are not destroyed, the integrity of the system has been restored, and the risk is deemed negligible, reestablish CA operations, giving priority to the ability to generate certificate status information within the CRL issuance schedule.
- If the CA signing keys are destroyed, the integrity of the system cannot be restored, or the risk is deemed substantial, reestablish CA operations as quickly as possible, giving priority to the generation of a new CA signing key pair.

7.7.3 Entity (CA) Private Key Compromise Procedures

7.7.3.1 Root CA Compromise Procedures

In the case of the Root CA compromise, the CA shall notify the relying parties, of the Root CA compromise so that they can remove the trusted self-signed certificate from their trust stores. Notification shall be made in an authenticated and trusted manner. Initiation of notification to the relying parties shall be made at the earliest feasible time and shall not exceed 72 hours beyond determination of compromise or loss unless otherwise required by law enforcement.

Initiation of notification to relying parties and subscribers may be made after mediations are in place to ensure continued operation of applications and services. If the cause of the compromise can be adequately addressed, and it is determined that the PKI can be securely re-established, the vendors shall then generate a new Root CA certificate, solicit requests and issue new Subordinate CA certificates, securely distribute the new Root CA certificate, and re-establish any cross certificates.

7.7.3.2 Intermediate or Subordinate CA Compromise Procedures

In the event of an Intermediate or Subordinate CA key compromise, the CA vendor shall notify the Superior CA. The superior CA shall revoke that CA's certificate, and the revocation information shall be published immediately in the most expedient, authenticated, and trusted manner but within 72 hours after the notification. The Compromised CA shall also investigate and report to the Superior CA what caused the compromise or loss, and what measures have been taken to preclude recurrence. If the cause of the compromise can be adequately addressed and it is determined that the CA can be securely re-established, then, the CA shall be re-established. Upon re-establishment of the CA, new device certificates shall be requested and issued.

For Subordinate CAs, when a Subscriber certificate is revoked because of compromise, suspected compromise, or loss of the private key, a CRL shall be published at the earliest feasible time by the supporting CA, but in no case more than 30 days after notification.

7.7.3.3 CSS Compromise Procedures

No stipulation.

7.7.3.4 RA Compromise Procedures

No stipulation.

7.7.4 Business Continuity Capabilities after a Disaster

CAs shall be required to maintain a Disaster Recovery Plan.

In the case of a disaster in which the CA equipment is damaged and inoperative, the CA operations shall be re-established as quickly as possible, giving priority to the ability to revoke device certificates, followed by generation of device certificates. The CA shall decide whether to declare the CA private signing key as compromised and re-establish the CA keys and certificates, or allow additional time for reestablishment of the CA's revocation capability.

In the case of a disaster whereby a CA installation is physically damaged and all copies of the CA signing functionality has been destroyed, the CA functions shall be migrated to the Disaster Recovery facility, where priority will be given to device certificate revocation and generation. The CA installation shall then be completely rebuilt by re-establishing the CA equipment, and restoring private and public keys.

7.8 CA Termination

Termination of the CA shall be approved by the Policy Authority team. When a CA operating under this policy terminates operations before all certificates have expired, Entities will be given as much advance notice as circumstances permit. In addition:

- The CA shall issue a CRL revoking all unexpired certificates prior to termination
- The CA shall archive all audit logs and other records prior to termination
- The CA shall destroy all its private keys upon termination
- If a Root CA is terminated, the Root CA shall use secure means to notify the subscribers to delete all trust anchors representing the terminated CA

8. TECHNICAL SECURITY CONTROLS

8.1 Key Pair Generation and Installation

8.1.1 Key Pair Generation

8.1.1.1 CA Key Pair Generation

Cryptographic keying material used by CAs to sign certificates, CRLs or status information shall be generated in FIPS 140 Level 2 validated cryptographic modules. Multiparty control is required for CA key pair generation, as specified in section 8.2.2.

CA key pair generation must create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure must be detailed enough to show that appropriate role separation was used.

8.1.1.2 Device Key Pair Generation

Device key pair generation shall be performed exclusively by the CA. Since the CA generates the device key pairs, the requirements for key pair delivery specified in section 8.1.2 must be met.
FIPS 140 validated software or hardware cryptographic modules shall be used to generate all device key pairs, as well as pseudo-random numbers and parameters used in key pair generation.

8.1.1.3 CSS Key Pair Generation

No stipulation.

8.1.2 Private Key Delivery to Subscriber

The device private keys must be delivered securely to the device. Private keys shall be delivered electronically using encryption to protect during storage and transit of the keys. In all cases, the following requirements must be met:

- The CA shall not retain any copy of the key after delivery of the private key to the device.
- The private key(s) must be protected from activation, compromise, or modification during the delivery process.
- The AOR shall acknowledge receipt of the private key(s).
- Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct devices.
    - For electronic delivery of private keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data shall be delivered using a separate secure channel.

8.1.3 Public Key Delivery to Certificate Issuer

No stipulation.

8.1.4 CA Public Key Delivery to Relying Parties

The public key of a root CA shall be provided to the subscribers acting as relying parties in a secure manner so that it is not vulnerable to modification or substitution. Examples of acceptable methods for delivery of the public key include secure distribution of self-signed certificates through secure out-of-band mechanisms.

8.1.5 Key Sizes

This CP requires use of RSA PKCS #1 or ECDSA signatures; additional restrictions on key sizes and hash algorithms are detailed below. Certificates issued under this policy shall contain RSA or elliptic curve public keys.
Root CA and intermediate certificates that expire on or after January 1, 2031 shall contain subject public keys of at least 256 or 384 bits for elliptic curve, and be signed with the corresponding private key. CAs that generate certificates and CRLs under this policy shall use the SHA-256, or SHA-384 hash algorithm when generating digital signatures. ECDSA signatures on certificates and CRLs shall be generated using SHA-256 or SHA-384, as appropriate for the key length.

8.1.6 Public Key Parameters Generation and Quality Checking

Elliptic Curve public key parameters shall always be selected from the set specified in section 9.1.3.

8.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The use of a specific key is constrained by the key usage extension in the X.509 certificate. All certificates, shall include a key usage extension.
Public keys that are bound into CA certificates shall be used only for signing certificates and status information (e.g., CRLs). CA certificates whose subject public key is to be used to verify other certificates shall assert the *keyCertSign* bit. CA certificates whose subject public key is to be used to verify CRLs shall assert the *cRLSign* bit.
Public keys that are bound into device certificates shall assert the digitalSign bit, keyEncipherment bit, and the keyAgreement bit.

8.2 Private Key Protection and Cryptographic Module Engineering Controls

8.2.1 Cryptographic Module Standards and Controls

CAs shall use a FIPS 140 Level 2 or higher validated cryptographic modules for signing operations.

8.2.2 Private Key (n out of m) Multi-Person Control

A single person shall not be permitted to activate or access any cryptographic module that contains the complete CA private signing key. CA signature keys may be backed up by one person, but it must be protected with 2 out of m tokens. Access to CA signing keys backed up for disaster recovery shall be under at least two-person control.

8.2.3 Private Key Escrow

CA private keys are never escrowed. No device private key escrow is provided.

8.2.4 Private Key Backup

8.2.4.1 Backup of CA Private Signature Key

The CA private signature keys backups shall be protected under the same multiperson control as the original signature key. At least one copy of the private signature key shall be stored off-site. All copies of the CA private signature key shall be accounted for and protected in the same manner as the original.

8.2.4.2 Backup of Human Subscriber Private Keys

No stipulation, no subscriber private keys are managed or stored by the CA.

8.2.4.3 Backup of CSS Private Key

No stipulation.

8.2.4.4 Backup of Device Private Keys

No stipulation. Copies of device private keys are not retained after distribution.

8.2.5 Private Key Archival

CA private signature keys shall not be archived.

8.2.6 Private Key Transfer into or from a Cryptographic Module

CA private keys may be exported from the cryptographic module only to perform CA key backup procedures as described in section 8.2.4.1. At no time shall the CA private key exist in plaintext outside the cryptographic module.
All other keys shall be generated by and in a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport; private keys must never exist in plaintext form outside the cryptographic module boundary. Private or symmetric keys used to encrypt other private keys for transport must be protected from disclosure.

8.2.7 Private Key Storage on Cryptographic Module

No stipulation beyond that specified in FIPS 140.

8.2.8 Method of Activating Private Key

A device shall be configured to activate its private key without requiring its authorized administrator to authenticate to the cryptographic token, provided that appropriate physical and logical access controls are implemented for the device and its cryptographic token. The strength of the security controls shall be commensurate with the level of threat in the device's environment, and shall protect the device's hardware, software, and the cryptographic token and its activation data from compromise.

8.2.9 Method of Deactivating Private Key

Cryptographic modules that have been activated shall not be available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure or automatically after a period of inactivity. CA cryptographic modules shall be removed and stored in a secure container when not in use.

8.2.10 Method of Destroying Private Key

Individuals in trusted roles shall destroy CA private signature keys when they are no longer needed. Physical destruction of cryptographic modules is required.

8.2.11 Cryptographic Module Rating

See section 8.2.1.

8.3 Other Aspects of Key Pair Management

8.3.1 Public Key Archival

No stipulation.

8.3.2 Certificate Operational Periods and Key Usage Periods

The usage period for the CA key pair is a maximum of 35 years. All certificates signed by a specific CA key pair must expire before the end of that key pair's usage period. The private keys corresponding to the public keys in the device certificates have a maximum usage period of 35 years.

8.4 Activation Data

8.4.1 Activation Data Generation and Installation

CA activation data may be user-selected (by each of the multiple parties holding that activation data). If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module. The strength of the activation data shall meet or exceed the requirements for authentication mechanisms stipulated for Level 2 in FIPS 140-2.

8.4.2 Activation Data Protection

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms.

8.4.3 Other Aspects of Activation Data

No stipulation.

8.5 Computer Security Controls

8.5.1 Specific Computer Security Technical Requirements

8.5.1.1 Access Control

Access to information such as sensitive details about customer accounts, passwords, and, ultimately, CA-related private keys shall be carefully guarded, along with the machines housing such information.

8.5.1.1.1 Access Control Policy and Procedures

The CA shall document roles and responsibilities for each employee job function. The CA shall create and maintain a mapping of these roles to specific employees.

8.5.1.1.2 Account Management

Information system account management features shall ensure that users access only that functionality permitted by their role or function. All account types with access to information system shall be documented along with procedures to follow in creating a new account. Conditions under which membership to a group or role is granted shall be justified based upon business need. Accounts shall be removed when a user no longer requires an account, their business role changes, or the user is terminated or transferred. Accounts and role membership should be removed as part of the last day of office procedures.

For off-line systems, account administration activities shall be logged, with a report available for security personnel to review when the systems are running. Account administration activities that shall be audited include account creation, modification, enabling, disabling, group or role changes, and removal actions

8.5.1.1.3 Access Enforcement

For some actions, defined in Section 7.2.2, dual authorization is required. The underlying access control systems shall support requiring two or more users to access certain sensitive data (such as particularly sensitive private keys) or to invoke certain functionality (such as batch approval and signing of large numbers of certificates).

8.5.1.1.4 Least Privilege

In granting rights to accounts and groups, the CA shall employ the principle of least privilege, allowing only authorized access for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. The CA shall explicitly authorize access to accounts and groups for controlling security functions and security-relevant information. The CA shall authorize access to privileged commands and features of information systems only for specific, organization-defined compelling operational needs.

8.5.1.1.5 Previous Logon (Access) Notification

No stipulation.

8.5.1.1.6 Permitted Actions without Identification or Authentication

No stipulation.

8.5.1.2 System Integrity

8.5.1.2.1 System Isolation and Partitioning

CA systems shall be configured, operated, and maintained so as to ensure the continuous logical separation (isolation) of processes (and their assigned resources). This separation shall be enforced by

- physical and/or logical isolation mechanisms, such as dedicated systems or virtualization
- protecting an active process and any assigned resources from access by or interference from another process
- protecting an inactive process and any assigned resources from access by or interference from an active process
- ensuring that any exception condition raised by one process will have no lasting detrimental effect on the operation or assigned resources of another process

All trusted components should be logically separated from each other, and shall be logically separated from any untrusted components of the CA system. Security critical processes shall be isolated from processes that have external interfaces. For example the CA signing processes shall be isolated from registration processes. The CA shall develop and document controlled procedures for transferring software updates, configuration files, certificate requests, and other data files between trusted components.

8.5.1.2.2 Malicious Code Protection

CA system components running standard operating systems that are not air-gapped from the Internet shall employ host-based anti-malware tools to detect and prevent the execution of known malicious code.
Anti-malware tools employed by a CA shall be properly maintained and updated by the CA. Anti-malware tools on networked systems shall be updated automatically as updates become available, or CA system administrators shall push updates to system components on a monthly basis. Anti-malware tools shall alert system administrators of any malware detected by the tools.
On system components that do not implement host-based anti-malware tools, the CA shall identify and employ other malicious code protection mechanisms to prevent the execution of malicious code, detect infected files or executables, and remediate infected systems.

8.5.1.2.3 Software and Firmware Integrity

The CA shall employ technical and operational controls to prevent unauthorized changes to firmware and software on CA systems. Access control mechanisms and configuration management processes shall ensure that only authorized system administrators are capable of installing or modifying firmware and software on CA systems.

8.5.1.2.4 Information Protection

The CA shall protect the confidentiality of integrity of sensitive information stored or processed on CA systems that could lead to abuse or fraud. For example, the CA shall protect customer data that could allow an attacker to impersonate a customer. The CA shall employ technical mechanisms to prevent unauthorized changes or accesses to this information, such as access control mechanisms that limit which users are authorized to view or modify files. Sensitive information stored on devices that are not physically protected from potential attackers shall be stored in an encrypted format, using a NIST-approved encryption algorithm and mode of operation.

8.5.2 Computer Security Rating

No Stipulation.

8.6 Life Cycle Technical Controls

8.6.1 System Development Controls

The system development controls address various aspects related to the development and change of the CA system through aspects of its life-cycle.

The CA system shall be implemented and tested in a non-production environment prior to implementation in a production environment. No change shall be made to the production environment unless the change has gone through the change control process.

In order to prevent incorrect or improper changes to the CA system, the CA system shall require authorized personnel credentials when changes are made. All accesses and authentication information associated with access control shall be logged. All data input to CA system components from users or other system components shall be validated prior to consumption by the receiving entity. Validating the syntax and semantics of system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match the expected definitions for format and content.

8.6.2 Security Management Controls

A list of acceptable products and their versions for each individual component in the CA system shall be maintained and kept up-to-date. Mechanisms and/or procedures shall be in operation designed to prevent the installation and execution of unauthorized software. To reduce the available attack surface of a CA system, only those ports, protocols, and services that are necessary to the CA system architecture are permitted to be installed or operating.

8.6.3 Life Cycle Security Controls

8.6.3.1 Flaw Remediation

Each vulnerability found shall be entered into an issue tracking database, along with the date and time of location, implementation of the remediation shall depend on the severity of the flaw.

CAs shall have a plan for receiving notification of software and firmware updates, for evaluating the updates, for deciding when to install them, and finally for installing them without undue disruption. A log shall be kept of the update patches applied and the data of such application.

From time to time, the CA may discover errors in configuration files, either because of human error, source data error, or changes in the environment which have made an entry erroneous. The CA shall correct such errors within a reasonable timeframe, and shall document the reason for the error, and the associated correction.

The CA shall also keep abreast of industry developments (e.g., computer, network), and plan to remain resistant to attack.

In no case should a remediation cause unavailability of revocation information.

8.7 Network Security Controls

The various components of a CA are, for the most part, connected to each other and their customers via various forms of networks. While it is necessary for connections to customers and administrative systems, care shall be taken to ensure those connections do not adversely impact the security of those components. Guidelines for effective CA networking security are discussed in the following sections.

8.7.1 Isolation of Networked Systems

The components of a CA with direct network connection shall be minimized. Those networked components shall be protected from attacks through the use of firewalls to filter unwanted protocols (utilizing access rules, whitelists, blacklists, protocol checkers, etc., as necessary).
Any administrator attempting to access these systems shall be required to pass strong authentication before being granted privileged access. All such administrative accesses shall be over secured channels, such as SSH, and the actions taken therein shall be irrevocably logged by the affected system.

8.7.2 Boundary Protection

Boundary protection is discussed in the context of four zone types. The zones are not assumed to be nested. They may be interconnected, but are independent. Zone boundaries are defined by limits of authority over the security of the data processed within the boundary. Interconnection of two zones, even at the same protection level, must be done in a way that respects the different authorities of the two zones. The zones are:

- Special Access Zone (SAZ) - highly controlled network area for processing and storage of especially high value data. It should be assumed that a network in this zone is not interconnected to a network in a lower security zone.
- Restricted Zone (RZ) - controlled network area for sensitive data processing and storage.
- Operations Zone (OZ) - network area containing systems for routine business operations.
- Public Zone (PZ) - any network area that is not behind a protective boundary controlled by the organization. Includes the public Internet and the public telephone network. Since there is no presumed control over the Public Zone, there are no requirements for boundary protection.

8.7.2.1 PKI Network Zones Overview

Root and intermediate CAs are expected to reside in a Special Access Zone with no network connection to any network in a lower security zone. The following sections describe the boundary of each zone type in the context of an extended CA (that is, including connections to systems that support but are not part of the CA).

8.7.2.2 Special Access Zone Boundary

An SAZ has no physical nor logical interconnection to networks in a lower security zone.

- Physical boundary protection measures shall include checks for network elements (cables, routers, wireless equipment) that indicate interconnection.
- Network interface software shall be configured to maintain network isolation. Configuration shall be monitored for modification.
- Incoming communications is limited to certificate signing requests, and system maintenance data.
- Outgoing communications is limited to signed certificates and CRLs, and any data related to monitoring and audit.
- Communication to and from a lower security zone shall be by means of removable media.
- Auditing functions shall be enabled on systems in the SAZ, according to the requirements in Section 7.4.
- Systems shall be physically isolated to separate platform instances and uniquely identified on each subnet with managed interfaces.

8.7.2.3 Restricted Zone Boundary

No secure component of this CA shall exist in the Restricted Zone Boundary, all highly sensitive data, including signing and encryption keys, and secure operations shall remain within the Special Access Zone Boundary.

8.7.2.4 Operational Zone Boundary

An OZ has physical interconnections to other OZs, and the PZ.

- Physical boundary protection measures shall include checks for network elements (cables, routers, wireless equipment) that indicate unauthorized interconnection.
- Physical boundary protection devices shall fail securely in the event of an operational failure.
- Connections with other OZs may be simple firewalled router interconnections that maintain the security posture of each OZ.

- Connections with the PZ must be limited to specific protocols, and connections digitally authenticated.
- Confidentiality of any interconnection shall be provided depending on the sensitivity of the information transferred and the route of the connection.
- Firewalls shall allow only those protocols necessary to perform a function, and only from recognized network origins, deny network traffic by default, and allow network traffic by exception (i.e., deny all, permit by exception).
- All communications shall be source authenticated.
- Incoming and outgoing communications shall be limited to data related to the business of the organization, system maintenance data, and any data related to monitoring and audit.
- Indications that boundary protections have failed must be dealt with promptly (see Section 7.7).
- No interconnection shall exist between the OZ and the SAZ. Data transfers between the OZ and the SAZ shall occur only through sanitized digital media as described in section 8.7.2.2. These are limited to certificate signing request, signed certificates, CRLs, and audit data.

8.7.3 Availability

Certificate request/issuing and revocation services need to be available, but can tolerate some down time. The advertisement of revoked certificates and distribution of device certificates, need to be highly available. If revocation information is not available, or if revocation information is inaccurate, then a Relying Party could be easily convinced to trust a revoked certificate.

8.7.3.1 Denial of Service Protection

CA systems shall be configured, operated, and maintained to maximize uptime and availability. CAs shall document the methods to request revocation.

8.7.3.2 Public Access Protections

No stipulation.

8.7.4 Communications Security

8.7.4.1 Transmission Integrity

Source authentication and integrity mechanisms shall be employed to all certificate request, manufacture, and issuance communications, including all related services irrespective of whether those services are hosted on the same or different platform than the CA workstation.

8.7.4.2 Transmission Confidentiality

Intra-CA communications that cross the physical protection barrier of the certificate-signing portion of the CA system shall be confidentiality-protected. Services used by the CA system that are not administered by the CA administrative staff shall provide protection commensurate with any applicable CP.

8.7.4.3 Network Disconnect

No stipulation.

8.7.4.4 *Cryptographic Key Establishment and Management*

Cryptographic key management includes all aspects of cryptographic key life cycle: key generation, distribution, storage, access and destruction, for all types of keys, both symmetric and asymmetric. Key

generation and management shall be performed in FIPS-140-2 Level 2 validated modules. Keys that are backed up for business continuity shall have protection comparable to the operational key.

Cryptographic key management includes all aspects of cryptographic key life cycle (key generation, distribution, storage, access and destruction) for all types of keys (symmetric and asymmetric). The CA service shall employ key protection mechanisms implemented in a FIPS 140-2 level 2 validated modules.

8.7.4.5 Cryptographic Protection

Cryptographic mechanisms implemented in a FIPS 140-2 level 1 (or higher) cryptographic module shall be employed to detect changes to sensitive information during transmission of Intra-CA communications.

8.7.4.6 Session Authenticity

No stipulation.

8.7.5 Network Monitoring

No stipulation.

8.7.5.1 Events and Transactions to be Monitored

No stipulation.

8.7.5.2 Monitoring devices

A CA shall deploy intrusion detection tools or other monitoring devices strategically within the CA to collect the essential information; and at ad hoc locations within the system to track specific types of transactions of interest to the organization.

8.7.5.3 Monitoring of Security Alerts, Advisories, and Directives

A CA shall monitor information system security alerts, advisories, and directives on an ongoing basis. The CA shall generate and disseminate internal security alerts, advisories, and directives as deemed necessary.

8.7.6 Remote Access/External Information Systems

8.7.6.1 Remote Access

No stipulation.

8.7.6.2 Bastion Host

No stipulation.

8.7.6.3 Documentation

No stipulation.

8.7.6.4 Logging

No stipulation.

8.7.6.5 Automated Monitoring

No stipulation.

8.7.6.6 Security of Remote Management System

No stipulation.

8.7.6.7 Authentication

No stipulation.

8.7.6.8 Communications Security for Remote Access

No stipulation.

8.7.7 Penetration Testing

No stipulation.

8.8 Time-Stamping

No stipulation.

9. Certificate, CRL, and OCSP Profiles

9.1 Certificate Profile

Intermediate certificates issued by a CA under this policy shall conform to the following ASN.1 profile:

```
SEQUENCE :
  SEQUENCE :
    CONTEXT SPECIFIC (0) :
      INTEGER : 2
    INTEGER :
      <SHA1 (Public Key) &0x7F (top byte only)>
    SEQUENCE :
      OBJECT IDENTIFIER :  [1.2.840.10045.4.3.2]
    SEQUENCE :
      SET :
        SEQUENCE :
          OBJECT IDENTIFIER : countryName [2.5.4.6]
          UTF8 STRING : 'US'
      SET :
        SEQUENCE :
          OBJECT IDENTIFIER : stateOrProvinceName [2.5.4.8]
          UTF8 STRING : 'CA'
      SET :
        SEQUENCE :
          OBJECT IDENTIFIER : localityName [2.5.4.7]
          UTF8 STRING :
            'Santa Clara'
      SET :
        SEQUENCE :
          OBJECT IDENTIFIER : organizationName [2.5.4.10]
          UTF8 STRING :
            'Intel Corporation'
      SET :
```

```
      SEQUENCE :
        OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]
        UTF8 STRING :
          'TPM EK root cert signing'
    SET :
      SEQUENCE :
        OBJECT IDENTIFIER : commonName [2.5.4.3]
        UTF8 STRING :
          'www.intel.com'
  SEQUENCE :
    UTC TIME : '<Initial Create Date and time> Zulu UTC TIME'
    UTC TIME : 'Dec 31, 2049, 23:59:59 Zulu UTC TIME'
  SEQUENCE :
    SET :
      SEQUENCE :
        OBJECT IDENTIFIER : countryName [2.5.4.6]
        UTF8 STRING : 'US'
    SET :
      SEQUENCE :
        OBJECT IDENTIFIER : stateOrProvinceName [2.5.4.8]
        UTF8 STRING : 'CA'
    SET :
      SEQUENCE :
        OBJECT IDENTIFIER : localityName [2.5.4.7]
        UTF8 STRING :
          'Santa Clara'
    SET :
      SEQUENCE :
        OBJECT IDENTIFIER : organizationName [2.5.4.10]
        UTF8 STRING :
          'Intel Corporation'
    SET :
      SEQUENCE :
        OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]
        UTF8 STRING :
          'TPM EK intermediate for Chipset 501 EPID1.'
          '1B EK RND'
    SET :
      SEQUENCE :
        OBJECT IDENTIFIER : commonName [2.5.4.3]
        UTF8 STRING :
          'www.intel.com'
  SEQUENCE :
    SEQUENCE :
      OBJECT IDENTIFIER : ecPublicKey [1.2.840.10045.2.1]
      OBJECT IDENTIFIER :  [1.2.840.10045.3.1.7]
    BIT STRING UnusedBits:0 :
      <04 | Public Key C | Public Key D>
  CONTEXT SPECIFIC (3) :
    SEQUENCE :
      SEQUENCE :
        OBJECT IDENTIFIER : authorityKeyIdentifier [2.5.29.35]
        OCTET STRING :
          SEQUENCE :
            CONTEXT SPECIFIC (0) :
```

```
        <Hash of signing public key>}
SEQUENCE :
  OBJECT IDENTIFIER : subjectKeyIdentifier [2.5.29.14]
  OCTET STRING :
    OCTET STRING :
      <Hash of platform public key>
SEQUENCE :
  OBJECT IDENTIFIER : basicConstraints [2.5.29.19]
  BOOLEAN : True
  OCTET STRING :
    SEQUENCE :
      BOOLEAN : True
      INTEGER : 0
SEQUENCE :
  OBJECT IDENTIFIER : keyUsage [2.5.29.15]
  BOOLEAN : True
  OCTET STRING :
    BIT STRING UnusedBits:1 :
      <keyCertSign(5), crlSign(6)>
SEQUENCE :
  OBJECT IDENTIFIER : extKeyUsage [2.5.29.37]
  BOOLEAN : True
  OCTET STRING :
    SEQUENCE :
      OBJECT IDENTIFIER :  [2.23.133.8.1]
SEQUENCE :
  OBJECT IDENTIFIER : certificatePolicies [2.5.29.32]
  BOOLEAN : True
  OCTET STRING :
    SEQUENCE :
      SEQUENCE :
        OBJECT IDENTIFIER :  [1.2.840.113741.1.5.2.1]
        SEQUENCE :
          SEQUENCE :
            OBJECT IDENTIFIER : cps [1.3.6.1.5.5.7.2.1]
            IA5 STRING :
              'http://upgrades.intel.com/c'
              'ontent/CRL/ekcert/EKcertPol'
              'icyStatement.pdf'
SEQUENCE :
  OBJECT IDENTIFIER : authorityInfoAccess [1.3.6.1.5.5.7.1.1]
  OCTET STRING :
    SEQUENCE :
      SEQUENCE :
        OBJECT IDENTIFIER : caIssuers [1.3.6.1.5.5.7.48.2]
        CONTEXT SPECIFIC (6) :
          'http://upgrades.intel.com/content'
          '/CRL/ekcert/EKRootPublicKey.cer'
SEQUENCE :
  OBJECT IDENTIFIER : cRLDistributionPoints [2.5.29.31]
  OCTET STRING : ''
    SEQUENCE : ''
      SEQUENCE : ''
        CONTEXT SPECIFIC (0) :
          CONTEXT SPECIFIC (0) :
```

```
                CONTEXT SPECIFIC (6) :
                  'http://upgrades.intel.com/c'
                  'ontent/CRL/ekcert/EK_Platfo'
                  'rm.crl'
  SEQUENCE :
    OBJECT IDENTIFIER :  [1.2.840.10045.4.3.2]
  BIT STRING UnusedBits:0 :
    SEQUENCE :
      INTEGER :
        <Hex R value>
      INTEGER :
        <Hex S value>
```

Device certificates issued by this CA shall conform to the following profile:

```
SEQUENCE :
  SEQUENCE :
    CONTEXT SPECIFIC (0) :
      INTEGER : 2
    INTEGER : <PAVP Unique Key ID>
    SEQUENCE :
      OBJECT IDENTIFIER :  [1.2.840.10045.4.3.2]
    SEQUENCE :
      SET :
        SEQUENCE :
          OBJECT IDENTIFIER : countryName [2.5.4.6]
          UTF8 STRING : 'US'
      SET :
        SEQUENCE :
          OBJECT IDENTIFIER : stateOrProvinceName [2.5.4.8]
          UTF8 STRING : 'CA'
      SET :
        SEQUENCE :
          OBJECT IDENTIFIER : localityName [2.5.4.7]
          UTF8 STRING :
            'Santa Clara'
      SET :
        SEQUENCE :
          OBJECT IDENTIFIER : organizationName [2.5.4.10]
          UTF8 STRING :
            'Intel Corporation'
      SET :
        SEQUENCE :
          OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]
          UTF8 STRING :
            'TPM EK intermediate for <PlatformName>'
      SET :
        SEQUENCE :
          OBJECT IDENTIFIER : commonName [2.5.4.3]
          UTF8 STRING :
            'www.intel.com'
```

```
SEQUENCE :
  UTC TIME : <Create Date and time Zulu  UTC TIME>
  UTC TIME : Dec 31, 2049, 23:59:59 Zulu UTC TIME
SEQUENCE : ''
SEQUENCE :
  SEQUENCE :
    OBJECT IDENTIFIER : rsaEncryption [1.2.840.113549.1.1.1]
    NULL : ''
  BIT STRING UnusedBits:0 :
    SEQUENCE :
      INTEGER : <Public Key N Value>
      INTEGER : 65537
CONTEXT SPECIFIC (3) :
  SEQUENCE :
    SEQUENCE :
      OBJECT IDENTIFIER : basicConstraints [2.5.29.19]
      BOOLEAN : True
      OCTET STRING :
        SEQUENCE :
          BOOLEAN : False
    SEQUENCE :
      OBJECT IDENTIFIER : keyUsage [2.5.29.15]
      BOOLEAN : True
      OCTET STRING :
        BIT STRING UnusedBits:1 :
          <digitalSig(0), keyEncipherment(2), keyAgreement(4)>
    SEQUENCE :
      OBJECT IDENTIFIER : extKeyUsage [2.5.29.37]
      OCTET STRING :
        SEQUENCE :
          OBJECT IDENTIFIER :  [2.23.133.8.1]
    SEQUENCE :
      OBJECT IDENTIFIER : subjectDirectoryAttributes [2.5.29.9]
      BOOLEAN : False
      OCTET STRING :
        SEQUENCE :
          SEQUENCE :
            OBJECT IDENTIFIER :  [2.23.133.2.16]
            SET :
              SEQUENCE :
                UTF8 STRING :
                  '<FamilyName>'
                INTEGER : <Level>
                INTEGER : <Revision>
          SEQUENCE :
            OBJECT IDENTIFIER :  [2.23.133.2.17]
            SET :
              SEQUENCE :
```

```
            SEQUENCE :
              INTEGER : <Major Version>
              INTEGER : <Minor Version>
              INTEGER : <Revision>
            OCTET STRING :
              '<Platform Class>'
SEQUENCE :
  OBJECT IDENTIFIER : subjectAltName [2.5.29.17]
  BOOLEAN : True
  OCTET STRING :
    SEQUENCE :
      CONTEXT SPECIFIC (4) :
        SEQUENCE :
          SET :
            SEQUENCE :
              OBJECT IDENTIFIER : tcpa_at_tpmManufacturer [2.23.133.2.1]
              UTF8 STRING :
                'id:<ManufactuerID>'
          SET :
            SEQUENCE :
              OBJECT IDENTIFIER : tcpa_at_tpmModel [2.23.133.2.2]
              UTF8 STRING :
                '<ModelName>'
          SET :
            SEQUENCE :
              OBJECT IDENTIFIER : tcpa_at_tpmVersion [2.23.133.2.3]
              UTF8 STRING :
                'id:<TPM Version (XXXXYYYY where XXXX is major and YYYY is minor hex rev)>'
      CONTEXT SPECIFIC (4) :
        SEQUENCE :
          SET :
            SEQUENCE :
              OBJECT IDENTIFIER : tcpa_at_platformManufacturer [2.23.133.2.4]
              UTF8 STRING :
                '<Platform Manufacturer>'
          SET :
            SEQUENCE :
              OBJECT IDENTIFIER : tcpa_at_platformModel [2.23.133.2.5]
              UTF8 STRING :
                '<Platform Model>'
      CONTEXT SPECIFIC (4) :
        SEQUENCE :
          SET :
            SEQUENCE :
              OBJECT IDENTIFIER : countryName [2.5.4.6]
              UTF8 STRING :
                'US'
          SET :
```

```
            SEQUENCE :
              OBJECT IDENTIFIER : stateOrProvinceName [2.5.4.8]
              UTF8 STRING :
                'CA'
            SET :
              SEQUENCE :
                OBJECT IDENTIFIER : localityName [2.5.4.7]
                UTF8 STRING :
                  'Santa Clara'
            SET :
              SEQUENCE :
                OBJECT IDENTIFIER : organizationName [2.5.4.10]
                UTF8 STRING :
                  'Intel Corporation'
            SET :
              SEQUENCE :
                OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]
                UTF8 STRING :
                  'TPM EK Device'
            SET :
              SEQUENCE :
                OBJECT IDENTIFIER : commonName [2.5.4.3]
                UTF8 STRING :
                  'www.intel.com'
SEQUENCE :
  OBJECT IDENTIFIER : authorityKeyIdentifier [2.5.29.35]
  OCTET STRING :
    SEQUENCE :
      CONTEXT SPECIFIC (0) :
        <Hash of signing public key>
SEQUENCE :
  OBJECT IDENTIFIER : cRLDistributionPoints [2.5.29.31]
  OCTET STRING : ''
    SEQUENCE : ''
      SEQUENCE : ''
        CONTEXT SPECIFIC (0) :
          CONTEXT SPECIFIC (0) :
            CONTEXT SPECIFIC (6) :
              'http://upgrades.intel.com/c'
              'ontent/CRL/ekcert/EK_Device'
              '.crl'
SEQUENCE :
  OBJECT IDENTIFIER : authorityInfoAccess [1.3.6.1.5.5.7.1.1]
  OCTET STRING :
    SEQUENCE :
      SEQUENCE :
        OBJECT IDENTIFIER : caIssuers [1.3.6.1.5.5.7.48.2]
        CONTEXT SPECIFIC (6) :
```

```
            'http://upgrades.intel.com/content'
            '/CRL/ekcert/<ShortenedPlatformName>_EK_Platform_Public_Key.cer'
      SEQUENCE :
        OBJECT IDENTIFIER : certificatePolicies [2.5.29.32]
        OCTET STRING :
          SEQUENCE :
            SEQUENCE :
              OBJECT IDENTIFIER :  [1.2.840.113741.1.5.2.1]
              SEQUENCE :
                SEQUENCE :
                  OBJECT IDENTIFIER : cps [1.3.6.1.5.5.7.2.1]
                  IA5 STRING :
                    'http://upgrades.intel.com/c'
                    'ontent/CRL/ekcert/EKcertPol'
                    'icyStatement.pdf'
                SEQUENCE :
                  OBJECT IDENTIFIER : unotice [1.3.6.1.5.5.7.2.2]
                  SEQUENCE :
                    UTF8 STRING :
                      'TCPA Trusted Platform Mo'
                      'dule Endorsement'
SEQUENCE :
  OBJECT IDENTIFIER :  [1.2.840.10045.4.3.2]
BIT STRING UnusedBits:0 :
  SEQUENCE :
    INTEGER :
      <Hex R value>
    INTEGER :
      <Hex S value>
```

9.1.1 Version Number(s)

The CA shall issue X.509 v3 certificates (populate version field with integer “2”).

9.1.2 Certificate Extensions

Extensions are defined in section 9.1.

9.1.3 Algorithm Object Identifiers

Certificates issued under this CP shall use the following OIDs for signatures:

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
ecdsa-with-Sha256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2}

Certificates issued under this CP shall use the following OIDs to identify the algorithm associated with the subject key:

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1}

Where the certificate contains an elliptic curve public key, the parameters shall be specified as one of the following named curves:

ansip256r1	{iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7}

9.1.4 Name Forms

Refer to section 9.1 for the subjectAltName and Issuer field definitions. An empty subject field is used for the device certificates.

9.1.5 Name Constraints

The CAs may assert name constraints in CA certificates.

9.1.6 Certificate Policy Object Identifier

Certificates issued under this CP shall assert the following OID:

id-intel-ftpm-certPolicy::= 1.2.840.113741.1.5.2.1

9.1.7 Usage of Policy Constraints Extension

The CAs may assert policy constraints in CA certificates.

9.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under this CP shall not contain policy qualifiers.

9.1.9 Processing Semantics for the Critical Certificate Policies Extension

Certificates issued under this policy shall contain a critical certificate policies extension.

9.2 CRL Profile

Intermediate CRLs issued by a CA under this policy shall conform to the CRL profile:

Certificate {
tbsCertificateList
Version (1)
signatureAlgorithm (`sha256ECDSA`)
Issuer (UTF8 Strings) CommonName = www.intel.com OrganizationUnitName = TPM EK root cert signing OrganizationName = Intel Corporation Locality = Santa Clara State = CA Country = US
thisUpdate <Current Date and time> UTCTime
nextUpdate Dec 31 2049 23:59:59 Zulu UTCTime
RevokedCertificates (0 or more entries of the below) Serial Number = INTEGER <revoked serial number> Revocation Date = <revocation Date Time> Zulu UTC
Extensions

AuthorityKeyIdentifier KeyIdentifier Octet String (SHA1(Root Px || Root Py))
CRLNumber Octet String INTEGER <unique ID the certificate>
AlgorithmIdentifier (sha256ECDSA)
SignatureValue (BIT String)
}

Device CRLs issued by a CA under this policy shall conform to the CRL profile:

Certificate {
tbsCertificateList
Version (1)
signatureAlgorithm (sha256ECDSA)
Issuer (UTF8 Strings) CommonName = www.intel.com OrganizationUnitName = TPM EK root cert signing OrganizationName = Intel Corporation Locality = Santa Clara State = CA Country = US
thisUpdate <Current Date and time> UTCTime
nextUpdate Dec 31 2049 23:59:59 Zulu UTCTime
RevokedCertificates (0 or more entries of the below) Serial Number = INTEGER <revoked serial number> Revocation Date = <revocation Date Time> Zulu UTC
Extensions
AuthorityKeyIdentifier KeyIdentifier Octet String (SHA1(Intermediate Px || Intermediate Py))
CRLNumber Octet String INTEGER <unique ID the certificate>
AlgorithmIdentifier (sha256ECDSA)
SignatureValue (BIT String)
}

9.2.1 Version Number(s)

The CAs shall issue X.509 Version two (2) CRLs.

9.2.2 CRL and CRL Entry Extensions

Section 9.2 covers the CRL and CRL Entry extensions.

9.3 OCSP Profile

No stipulation.

10. Compliance Audit and Other Assessments

CAs shall have a compliance audit mechanism in place to ensure that the requirements of their policy are being implemented and enforced. This specification does not impose a requirement for any particular assessment methodology.

10.1 Frequency of Circumstances of Assessment

CAs shall be subject to a periodic compliance audit at least once every two years.

10.2 Qualification of Assessor

The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the CA's practices and this CP. The compliance auditor must perform such compliance audits as a regular ongoing business activity. In addition to the previous requirements, the auditor must be a certified information system auditor (CISA) or IT security specialist, who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

10.3 Assessor's Relationship to Assessed Entity

The compliance auditor either shall be a private firm that is independent from the entities being audited, or it shall be sufficiently organizationally separated from those entities to provide an unbiased, independent evaluation. To insure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining the entity's CA Facility or certificate practices statement. The Policy Authority shall determine whether a compliance auditor meets this requirement.

10.4 Topics Covered by Assessment

The purpose of a compliance audit shall be to verify that a CA and its recognized RAs comply with all the requirements of the current version of this CP. All aspects of the CA operation shall be subject to compliance audit inspections.

10.5 Actions Taken as a Result of Deficiency

When the compliance auditor finds a discrepancy between the requirements of this CP and the design, operation, or maintenance of the PKI Authorities, the following actions shall be performed:

- The compliance auditor shall note the discrepancy
- The compliance auditor shall notify the parties identified in section 10.6 of the discrepancy
- The party responsible for correcting the discrepancy will propose a remedy, including expected time for completion, to the Policy Authority

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the Policy Authority may decide to temporarily halt operation of the CA, to revoke a certificate issued to the CA, or take other actions it deems appropriate. The Policy Authority will develop procedures for making and implementing such determinations.

10.6 Communication of Results

An Audit Compliance Report shall be provided to the entity responsible for CA operations. The Audit Compliance Report and identification of corrective measures shall be provided to Policy Authority within 60 days of completion. A special compliance audit may be required to confirm the implementation and effectiveness of the remedy.

11. Other Business and Legal Matters

11.1 Fees

11.1.1 Certificate Issuance or Renewal Fees

No stipulation.

11.1.2 Certificate Access Fees

CAs operating under this policy must not charge additional fees for access to this information.

11.1.3 Revocation or Status Information Access Fees

CAs operating under this policy must not charge additional fees for access to CRLs information.

11.1.4 Fees for other Services

No stipulation.

11.1.5 Refund Policy

No stipulation.

11.2 Financial Responsibility

This CP contains no limits on the use of certificates issued by CAs under the policy. Rather, entities, acting as relying parties, shall determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction.

11.2.1 Insurance Coverage

No stipulation.

11.2.2 Other Assets

No stipulation.

11.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

11.3 Confidentiality of Business Information

The CA shall protect the confidentiality of sensitive business information stored or processed on CA systems. CA information not requiring protection may be made publicly available. Public access to organizational information shall be determined by the respective organization.

11.3.1 Scope of Confidential Information

No stipulation.

11.3.2 Information not within the Scope of Confidential Information

No stipulation.

11.3.3 Responsibility to Protect Confidential Information

No stipulation.

11.4 Privacy of Personal Information

11.4.1 Privacy Plan

The CA shall adhere to Intel Corporation's privacy policy.

11.4.2 Information Treated as Private

CAs shall protect all personally identifying information pursuant to Intel Corporation's privacy policy.

11.4.3 Information not Deemed Private

Information included in certificates is not subject to protections outlined in section 11.4.2.

11.4.4 Responsibility to Protect Private Information

Sensitive information must be stored securely, and may be released only in accordance with other stipulations in section 11.4.

11.4.5 Notice and Consent to Use Private Information

No stipulation.

11.4.6 Disclosure Pursuant to Judicial or Administrative Process

The CA shall not disclose private information to any third party unless authorized by this policy, required by law, government rule or regulation, or order of a court of competent jurisdiction.

11.4.7 Other Information Disclosure Circumstances

None.

11.5 Intellectual Property Rights

The CA will not knowingly violate intellectual property rights held by others.

11.6 Participant Requirements

The Policy Authority shall—

- Approve the practices for each CA that issues certificates under this policy;
- Review periodic compliance audits to ensure that CAs are operating in compliance;
- Revise this CP to maintain the level of assurance and operational practicality;

- Publicly distribute this CP; and
- Coordinate modifications to this CP to ensure continued compliance.

11.6.1 CA Requirements

A CA that issues certificates that assert a policy defined in this document shall conform to the stipulations of this document, including—

- Maintaining its operations in conformance to the stipulations of this CP.
- Ensuring that registration information is accepted only from approved RAs.
- Including only valid and appropriate information in certificates, and maintaining evidence that due diligence was exercised in validating the information contained in the certificates.
- Operating or providing for the services of an on-line repository, and informing the repository service provider of their obligations if applicable.

11.6.2 RA Requirements

No stipulation

11.6.3 Subscriber Requirements

A subscriber (or human sponsor for device certificates) shall be informed of the requirements the subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate.
Subscribers shall—

- Accurately represent themselves in all communications with the PKI authorities.
- Protect their private key(s) at all times, in accordance with this policy.
- Promptly notify the appropriate CA upon suspicion of loss or compromise of their private key(s).
- Abide by all the terms, conditions, and restrictions levied on the use of their private key(s) and certificate(s).

11.6.4 Relying Parties Requirements

This CP does not specify the steps a relying party should take to determine whether to rely upon a certificate. The relying party decides, pursuant to its own policies, what steps to take. The CA merely provides the tools (i.e., certificates and CRLs) needed to perform the trust path creation, validation, and CP mappings that the relying party may wish to employ in its determination.

11.6.5 Other Participants

None.

11.7 Limitations of Liabilities

No stipulation.

11.8 Indemnities

No stipulation.

11.9 Term and Termination

11.9.1 Term

The CP shall document the term for which the CP is effective.

11.9.2 Termination

The CP shall document under what conditions the CP may be terminated.

11.9.3 Effect of Termination and Survival

The requirements of this CP remain in effect through the end of the archive period for the last certificate issued.

11.10 Individual Notices and Communications with Participants

No stipulation

11.11 Amendments

11.11.1 Procedure for Amendment

The Policy Authority shall review this CP at least once every year. Corrections, updates, or changes to this CP shall be publicly available. Suggested changes to this CP shall be communicated to the contact in section 3.5.2; such communication must include a description of the change, a change justification, and contact information for the person requesting the change.

11.11.2 Notification Mechanism and Period

No stipulation.

11.11.3 Circumstances under which OID must be Changed

OIDs should be changed if there is a change in the CP that reduces the level of assurance provided.

11.12 Dispute Resolution Provisions

The Policy Authority shall facilitate the resolution between entities when conflicts arise as a result of the use of certificates issued under this policy.

11.13 Governing Law

No stipulation.

11.14 Compliance with Applicable Law

All CAs operating under this policy are required to comply with applicable law.

11.15 Miscellaneous Provisions

11.15.1 Entire Agreement

No stipulation.

11.15.2 Assignment

No stipulation.

11.15.3 Severability

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in section 11.11.

11.15.4 Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation.

11.15.5 Force Majeure

No stipulation.

11.16 Other Provisions

No stipulation.

12. Acronyms and Abbreviations

AIA	Authority Information Access
AOR	Authorized Operational Representative
CA	Certification Authority
COMSEC	Communications Security
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Objects Registry
CSR	Certificate Signing Request

CSS	Certificate Status Server
DN	Distinguished Name
ECDSA	Elliptic Curve Digital Signature Algorithm
EK	Endorsement Key
FIPS PUB	(US) Federal Information Processing Standards Publication
FPKI	Federal Public Key Infrastructure
HTTP	Hypertext Transfer Protocol
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IS	Information System
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
ISO	International Organization for Standardization
ITU-T	International Telecommunications Union – Telecommunications Sector
NIST	National Institute of Standards and Technology
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OZ	Operations Zone
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PSS	Probabilistic Signature Scheme
PZ	Public Zone

RA	Registration Authority
RZ	Restricted Zone
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
RSASSA	RSA Signature Scheme with Appendix
SHA	Secure Hash Algorithm
S/MIME	Secure/Multipurpose Internet Mail Extensions
SAZ	Special Access Zone
SP	Special Publication
SSP-REP	Shared Service Provider Repository Service Requirements
TAM	Trust Anchor Manager
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
U.S.C.	United States Code
UUID	Universal Unique Identifier
VPN	Virtual Private Network
WAP	Wireless Access Point
WWW	World Wide Web

13. GLOSSARY

Access	Ability to make use of any information system (IS) resource. [NS4009]
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Applicant	The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]

Archive	Long-term, physically separate storage.
Attribute Authority	An entity, recognized by the FPKIPA or comparable body as having the authority to verify the association of attributes to an identity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
Backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
Bastion Host	A special purpose computer on a network specifically designed and configured to withstand attacks.
Binding	Process of associating two related elements of information. [NS4009]
Biometric	A physical or behavioral characteristic of a human being.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]. As used in this CP, the term “certificate” refers to X.509 certificates that expressly reference the OID of this CP in the certificatePolicies extension.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 public key certificates and CRLs.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a certification authority to perform certificate issuance and revocation.
CA Operating Staff	CA components are operated and managed by individuals holding trusted, sensitive roles.
Certificate Policy (CP)	A certificate policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A certificate policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).
CPS Summary	A publically releasable version of the CPS.

Certificate-Related Information	Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.
Certificate Revocation List (CRL)	A list maintained by a certification authority of the certificates that it has issued that are revoked prior to their stated expiration date.
Certificate Status Server (CSS)	A trusted entity that provides on-line verification to a relying party of a subject certificate's revocation status, and may also provide additional attribute information for the subject certificate.
Client (application)	A system entity, usually a computer process acting on behalf of a human user that makes use of a service provided by a server.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by the National Institute of Standards and Technology.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
Cross-Certificate	A certificate used to establish a trust relationship between two certification authorities.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS 140-2]
Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a relying party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.
End Entity Certificate	A certificate in which the subject is not a CA.
Firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]
Key Exchange	The process of exchanging public keys in order to establish secure communications.
Key Management Key	Key exchange, key agreement, key transport

Key Pair	Two mathematically related keys having the properties that (1) one (public) key can be used to encrypt a message that can only be decrypted using the other (private) key, and (2) even knowing the public key, it is computationally infeasible to discover the private key.
Modification (of a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] Technical non-repudiation refers to the assurance a relying party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization, the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the Federal PKI, OIDS are used to uniquely identify certificate policies and cryptographic algorithms.
Online Certificate Status Protocol	Protocol which provides on-line status information for certificates.
Operations Zone (OZ)	Network area containing systems for routine business operations.
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring on-line).
Policy Authority (PA)	Body established to oversee the creation and update of certificate policies, review certification practice statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.
Privacy	Restricting access to subscriber or relying party information in accordance with Federal law.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is normally made publicly available in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public/private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Public Zone (PZ)	Network area that is not behind a protective boundary controlled by the organization.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a

	registration authority is delegated certain tasks on behalf of an authorized CA).
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate that contains the new public key.
Relying Party	A person or entity who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
Restricted Zone (RZ)	Controlled network area for sensitive data processing and storage
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Role Sponsor	Non-trusted role responsible for authorizing individuals for a role certificate, recovery of the private description key, revocation of individuals who are assigned the role, and always maintaining a current up to date list of individuals who have been provided a decryption private key for the role
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Security Auditor	An individual (e.g. employee, contractor, consultant, 3rd party) who is responsible for auditing the security of CAs or Registration Authorities (RAs), including performing or overseeing internal audits of CAs or RAs. A single individual may audit both CAs and RAs. Security Auditor is an internal role that is designated as trusted.
Server	A system entity that provides a service in response to requests from clients.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Special Access Zone (SAZ)	Highly controlled network area for processing and storage of especially high value data.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).
Subscriber	A subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual, an application or network device.
Superior CA	In a hierarchical PKI, a CA that has certified the certificate signature key of another CA, and that constrains the activities of that CA. (See subordinate CA).
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]

Trust List	Collection of Trusted Certificates used by relying parties to authenticate other certificates.
Trust Zone	The level of security controls in a network segment.
Trusted Agent	Entity authorized to act as a representative of a CA in confirming subscriber identification during the registration process. Trusted agents do not have automated interfaces with certification authorities.
Trust Anchor Manager	Authorities who manage a repository of trusted Root CA Certificates. They act on behalf of relying parties, basing their decisions on which CAs to trust on the results of compliance audits. A TAM sets requirements for inclusion of a CA's root public key in their store. These requirements are based on both security and business needs. The TAM has a duty to enforce compliance with these requirements, for example, requirements around the supply of audit results, on initial acceptance of a root, and on an ongoing basis. TAMs will follow their normal practice of requiring CAs to submit an annual audit report.
Trusted Certificate	A certificate that is trusted by the relying party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".
Two-Person Control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements. [NS4009]
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS 140-2]
Zone Boundary	The limit of authority over the security of the data processed within the boundary.

14. Document Revisions

Date	Change Description	Release #	Owner
4/7/2014	Created document	0.1	E. Cabre
6/3/2014	Released first draft	0.2	E. Cabre
10/09/2014	Released second draft	0.3	E. Cabre