CertiPath X.509 Certificate Policy

Version 4.1

March 24, 2025

Note: The effective date for the inclusion in PMA Member Certificate Policies of the Key Recovery Policy requirements in this Policy is no later than the 2026 Recertification of each PMA Member PKI. Such consolidated Certificate Policy must be the basis for the Annual Third-Party Audit provided for the 2026 Recertification. If a PMA Member elects to maintain a separate Key Recovery Policy in lieu of consolidation, that Key Recovery Policy must be included in the Annual Third-Party Audit provided for the 2026 Recertification.

Signature Page

Judith Spencer - SIG

Digitally signed by Judith Spencer - SIG
Date: 2025.03.28 15:38:26 -04'00'

CertiPath Policy Management Authority

March 28, 2025

DATE

Table of Contents

1 INTRODUCTION

This Certificate Policy (CP) defines several certificate policies to facilitate interoperability among distinct Public Key Infrastructure (PKI) domains. The policies represent the medium-CBP-software[1], medium-CBP-hardware, high-CBP-hardware, medium-device-software, medium-software, medium-device-hardware, medium-hardware, high-hardware, IceCAP-cardAuth, IceCAP-hardware, and IceCAP-contentSigning, assurance levels for public key certificates. The word "assurance" used in this CP means how well a Relying Party can be certain of the identity binding between the public key and the individual whose subject name is cited in the certificate. In addition, it also reflects how well the Relying Party can be certain that the individual whose subject name is cited in the certificate is controlling the use of the private key that corresponds to the public key in the certificate, and how securely the system which was used to produce the certificate and (if appropriate) deliver the private key to the Subscriber performs its task.

This CP assists interoperability among Organizational PKI domains cross certified with the CertiPath Bridge Certification Authority (CBCA) in a peer-to-peer fashion. CertiPath operates the CBCA based on this CP to facilitate interoperation among the Member PKIs. Member PKIs are required to comply with this CP through the use of policy mapping or direct policy assertion.

This CP also covers the CertiPath Common Policy Root CA (CRCA) that certifies Signing Certification Authorities (CAs) of organizations that do not wish to operate their own Root CAs. The CRCA will issue certificates to Enterprise Signing CAs under the certificate policies defined in this document, resulting in the Enterprise Signing CA becoming subordinated to the CRCA. The CRCA will cross certify with the CBCA in order to ensure interoperation among subordinated organizations and other member organizations.

Key recovery is mandatory for all CertiPath Member CAs that issue key management (encryption) certificates. This CP incorporates the requirements for the escrow and key recovery of private decryption key management keys. Member PKIs may either incorporate Key Recovery into their Certificate Policy or establish a separate Key Recovery Policy (KRP) that captures all of the requirements established by this CP. In addition, key recovery practices must be incorporated into the appropriate Certification Practice Statement (CPS) or captured in a dedicated Key Recovery Practice Statement (KRPS).

Any use of or reference to this CP outside the purview of the CertiPath PKI is completely at the using party's risk. A cross-certified Entity shall not assert the OIDs listed in Section 1.2 of this CP in any certificates the Entity CA issues, except in the *policyMappings* extension of certificates issued by the Entity Principal Certification Authority (PCA) to CBCA for the establishment of equivalency between a CertiPath OID and an OID in the Entity CA's CP. Entities subordinated under the CRCA shall assert the OIDs listed in Section 1.2 of this CP directly.

This CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy, and Certification Practice Statement Framework.

---

[1] Note: CBP stands for Commercial Best Practices

1.1 Overview

1.1.1 Certificate Policy (CP)

Certificates issued by CertiPath contain one or more registered certificate policy object identifiers (OID), which may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. Each OID corresponds to a specific level of assurance established by this Certificate Policy (CP), which shall be available to Relying Parties. Certificates issued by CertiPath shall, in the *policyMappings* extension and in whatever other fashion is determined by the CertiPath Policy Management Authority (described in Section 1.3.1.1) to be necessary for interoperability, reflect what mappings exist between this CP and the CertiPath Member PKI CP.

The key recovery requirements included in this CP are based on the principle that all encryption activities using the certificates are performed on behalf of the person or the organization that authorized the issuance of encryption certificates. Therefore, the person or the business has the right to identify the persons authorized to recover the decryption private key in order to maintain the continuity of business operations. In addition, some organizations require that the contents of incoming and/or outgoing email be examined for compliance with the organization's policies. Furthermore, there may be a need to access the information for investigative and law enforcement purposes.

1.1.2 Relationship between this CP & the CBCA CPS and CRCA CPS

This CP states what assurance can be placed in a certificate issued under this policy. The CBCA Certification Practice Statement (CPS) and CRCA CPS state how the respective certification authorities establish that assurance.

1.1.3 Relationship between this CP & the Principal CA (PCA) CP

For CertiPath Member PKIs whose PCAs cross certify with the CBCA, the levels of assurance identified in this CP are mapped by the CertiPath Policy Management Authority (CPMA) to the levels of assurance of the certificates issued by the Member PKI. For a definition and description of PCA, see Section 1.3.1.5. The policy mappings information is placed into the certificates issued by the CBCA, or otherwise published or used by the CertiPath Operational Authority (described in Section 1.3.1.3) so as to facilitate interoperability.

For CertiPath Member PKIs, whose Signing CAs are subordinated to the CRCA, the Member PKI must adopt the CertiPath CP at the levels of assurance agreed upon by the CPMA.[2]

1.1.4 Scope

Figure 1 illustrates the scope of this CP.

[2] For Member Organizations that elect to subordinate to the CRCA, the CertiPath CP becomes the relevant policy document for the Member Organization's CA. This constitutes *adoption* by the Member Organization and contrasts with CBCA cross certification which requires the Member Organization to develop and maintain its own CP and map it to the CBCA.

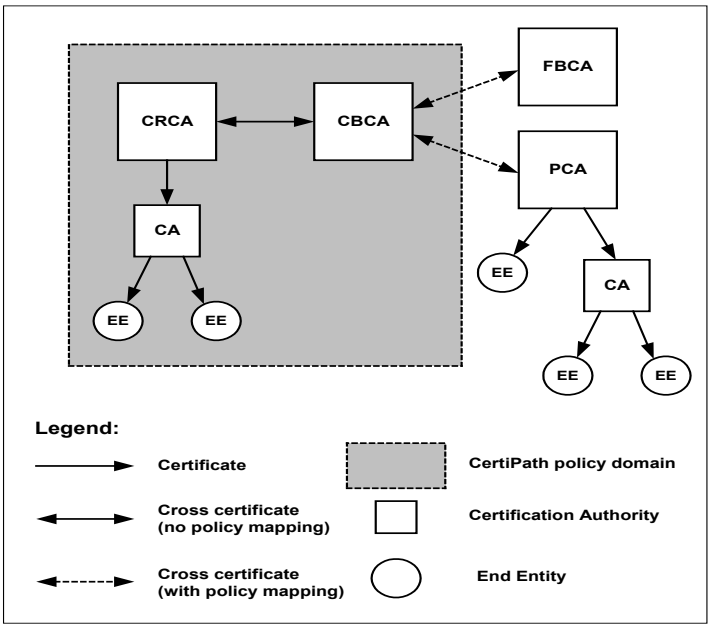

Figure 1 - Scope and Domain of the CertiPath CAs

This CP imposes requirements on all the CertiPath Member CAs involved in issuing certificates. These include the following:

- CertiPath Bridge Certification Authority (CBCA)
- CertiPath Common Policy Root Certification Authority (CRCA)
- Principal CAs (PCA) cross certifying with the CBCA
- Root CAs[3]
- Intermediate and Signing CAs certified by the PCAs
- Signing CAs certified by the intermediate CAs

In addition, Bridge CAs that enter into a relationship with the CertiPath Bridge are required to align with this CP prior to cross certification.

The CBCA shall issue CA certificates only to the following:

- CAs designated by the CertiPath Member PKI domains as PCAs;
- Bridge CAs approved for cross certification by the CPMA;
- CRCA

The CRCA shall issue CA certificates only to the following:

- CertiPath Member PKI domains that elect to adopt the CertiPath CP and subordinate to the CRCA.
- CBCA

The CBCA and CRCA exist to facilitate trusted communications among CertiPath Member PKI domains. CertiPath member enterprise PKIs operating under their own policy domains shall be issued cross-certificates from the CBCA to their Principal CAs. CertiPath member enterprise PKIs operating under the policy domain defined by this CP shall be issued certificates by the CRCA. The generic term “entity” applies equally to organizations owning or operating PKI domains. As used in this CP, Entity PKI or Entity

[3] Generally a PCA for an Enterprise PKI is also the Root CA for the Enterprise PKI, but this may not always be true.

CA may refer to an organization's PKI, a PKI provided by a commercial service, or a bridge CA serving a community of interest.

Within this document, the term CA, when used without qualifier, shall refer to any certification authority subject to the requirements of this certificate policy, including the CBCA, CRCA, PCAs, and intermediate and signing CAs. The term CertiPath CA shall be used for requirements that pertain to both the CBCA and CRCA. Requirements that apply to a specific CA type will be denoted by specifying the CA type, e.g., CBCA, CRCA, PCA, Root CA, etc.

The scope of this CP in terms of subscriber (i.e., end entity) certificate types is limited to those listed in Section 10 and repeated here: identity, signature, encryption, web server, code signing, role signature, and role encryption.

1.2 Document Identification

There are multiple levels of assurance in this Certificate Policy, which are defined in subsequent sections. Each level of assurance has an OID, to be asserted in certificates issued by the CBCA, CRCA and the CAs subordinate to the CRCA, which comply with the policy stipulations herein.

The OIDs are registered under the CertiPath arc as follows:

id-certipath	::= {1.3.6.1.4.1.24019}
id-security	::= { id-certipath 1}
id-pki	::= { id-security 1}
certipath-certificate-policies	::= { id-pki 1}
id-mediumSoftware	::= {certipath-certificate-policies 1}
id-mediumHardware	::= {certipath-certificate-policies 2}
id-highHardware	::= {certipath-certificate-policies 3}
id-mediumCBPSoftware	::= {certipath-certificate-policies 4}
id-mediumCBPHardware	::= {certipath-certificate-policies 5}
id-highCBPHardware	::= {certipath-certificate-policies 6}
id- IceCAP-hardware	::= {certipath-certificate-policies 7}
id-IceCAP-cardAuth	::= {certipath-certificate-policies 8}
id-IceCAP-contentSigning	::= {certipath-certificate-policies 9}
id-medium-device-software	::= {certipath-certificate-policies 23}
id-medium-device-hardware	::= {certipath-certificate-policies 24}

Unless otherwise stated, a requirement stated in this CP applies to all assurance levels.

The requirements associated with CBP (commercial best practice) assurance levels are identical to the corresponding non-CBP assurance level with the exception of trusted role personnel citizenship requirements (see section 5.3.1).

The requirements associated with the "id-medium-device. . ." policies are identical to those defined for other medium assurance policies with the exception of identity proofing, backup and activation data. The use of these policies is restricted to devices and systems (e.g., software applications and hardware devices). Certificates issued to end-entity devices shall assert one or both of the following policies: id-medium-device-software, id-medium-device-hardware. Other devices (such as content signers, OCSP responders, etc.) may assert appropriate policy OIDs.

Upon Entity PKI request, the CBCA may assert certificate policy OIDs not listed above in an Entity cross-certificate. These policy OIDs are called "pass-through" policy OIDs.

Unless otherwise stated, a requirement stated for medium hardware assurance level also applies to all three IceCAP assurance levels. In addition, the IceCAP-contentSigning policy is reserved for certificates used by the Card Management System (CMS) to sign the IceCAP card security objects.

Figure 2 below illustrates the partially ordered hierarchy of some of these policies.

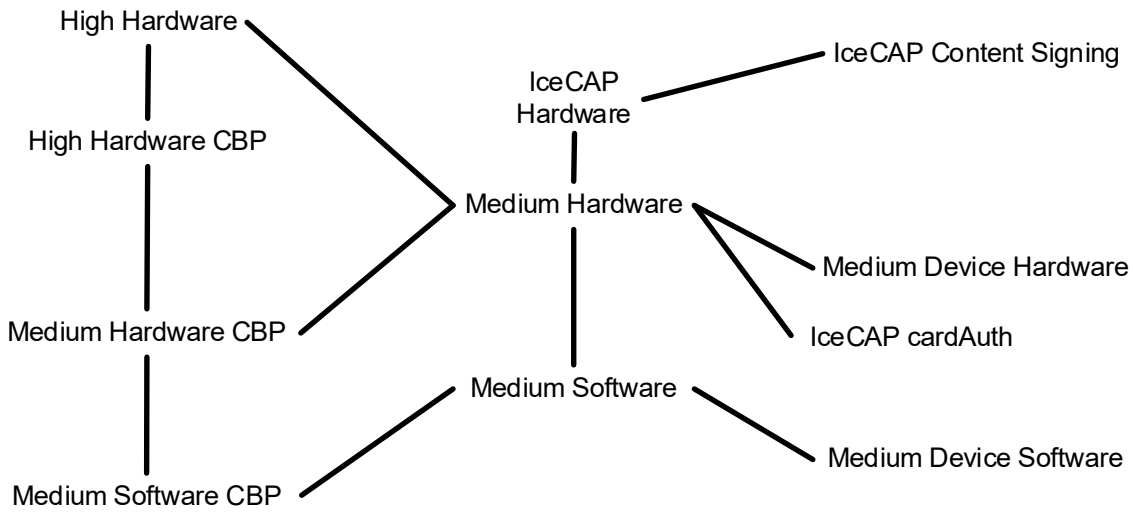

Figure 2 – Hierarchy of CertiPath Certificate Policies

1.3 PKI Participants

This section contains a description of the roles relevant to the administration and operation of the CBCA and CRCA. The PKI components identified in Sections 1.3.1.5 through 1.3.2 and their sub-components comprise the security-relevant components of the PKI and must adhere to the security, audit and archive requirements of Sections 5 and 6.

1.3.1 PKI Authorities

1.3.1.1 CertiPath PMA (CPMA)

The CPMA is responsible for:

- Approval of the CertiPath CP, including all CP Change Requests,
- Accepting and processing applications from Entities desiring to cross-certify with the CBCA or subordinate to the CRCA,

- Approval of the mappings between certificates issued by applicant Entity CAs and the levels of assurance set forth in the CertiPath CP (which will include objective and subjective evaluation of the respective CP contents, and any other facts deemed relevant by the CPMA),
- Providing notification of changes that have the potential to affect their operational environments to cross certified entities at least two (2) weeks prior to implementation, and
- After an Entity is authorized to interoperate using the CBCA, ensuring continued conformance of that Entity with applicable requirements as a condition for allowing continued interoperability using the CBCA or CRCA.

A complete description of CPMA roles and responsibilities are provided in the CPMA Charter.

CertiPath will enter into an agreement with a Member Entity setting forth the respective responsibilities and obligations of both parties, and the mappings between the certificate levels of assurance contained in this CP and those in the Entity CP. CertiPath will consult with the CPMA chair prior to entering into any such agreement. The stylized term AGREEMENT as used in this CP shall always refer to the agreement cited in this paragraph.

1.3.1.2 CertiPath Policy Working Group (CPWG)

The CertiPath Policy Working Group (CPWG) reports to the CPMA. The CPWG is responsible for the following:

- Compliance analysis and approval of the CBCA CPS and CRCA CPS,
- Review of CP change requests and recommendations to the CPMA for approval or rejection by the CPMA, and
- Conducting Applicant CP mapping and interoperability testing and providing recommendations to the CPMA for approval or rejection by the CPMA.

1.3.1.3 CertiPath Operational Authority (OA)

The CertiPath Operational Authority reports to the CertiPath corporate management. The CertiPath Operational Authority is the organization that operates the CBCA and the CRCA. This includes drafting the CBCA CPS and CRCA CPS, issuing certificates when directed by the CPMA Chair, posting those certificates and CRLs into the CertiPath PKI Repository, and ensuring the continued availability of the PKI Repository to all users.

1.3.1.4 CertiPath Operational Authority Manager

The CertiPath Operational Authority Manager is the individual within CertiPath corporate management who has principal responsibility for overseeing the proper operation of the CertiPath CAs including the CertiPath PKI Repository, and who oversees appointment of the Operational Authority Staff.

1.3.1.5 Entity Principal Certification Authority (PCA)

The Principal CA is a CA within a PKI that has been designated to interoperate directly with the CBCA (i.e., through the exchange of cross-certificates). It should be noted that an Entity may request that the CBCA interoperate with more than one CA within the Entity; that is, an Entity may have more than one Principal CA. A PCA may or may not be a Root CA (trust anchor) for its PKI Enterprise.

1.3.1.6 Root CA

A Root CA is a trust anchor for Subscribers of a PKI domain when the Subscribers act as a relying party.

The CRCA is a PCA and Root CA that cross-certifies with the CBCA.

1.3.1.7 Intermediate CA

An Intermediate CA is a CA that is not a Root CA and whose primary function is to issue certificates to other CAs. Intermediate CAs may or may not issue some end entity certificates. An Intermediate CA may function as a PCA.

1.3.1.8 Signing CA

A Signing CA is a CA whose primary function is to issue certificates to end entities. A Signing CA may function as a PCA. In addition, an Entity Signing CA may be subordinated to the CRCA.

1.3.1.9 CertiPath Bridge Certification Authority (CBCA)

The CBCA is the Bridge CA operated by the Operational Authority. The CBCA issues and revokes PCA cross certificates based on the CPMA authorization. As operated by the Operational Authority, the CBCA is responsible for all aspects of the issuance and management of a certificate including:

- Control over the registration process,
- The identification and authentication process,
- The certificate manufacturing process,
- Publication of certificates,
- Revocation of certificates,
- Re-key of CBCA signing material, and
- Ensuring that all aspects of the services, operations and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

1.3.1.10 CertiPath Root Certification Authority (CRCA)

The CRCA is the Root CA operated by the Operational Authority. The CRCA issues and revokes certificates to Enterprise Signing CAs upon authorization by the CPMA. As operated by the Operational Authority, the CRCA is responsible for all aspects of the issuance and management of a certificate including:

- Control over the registration process,
- The identification and authentication process,
- The certificate manufacturing process,
- Publication of certificates,
- Revocation of certificates,
- Re-key of CRCA signing material, and
- Ensuring that all aspects of the services, operations and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

1.3.1.11 Certificate Status Authority (CSA)

A CSA is an authority that provides status of certificates or certification paths. A CSA can be operated in conjunction with an Entity's CAs or independent of the CAs. Examples of CSA are:

- OCSP Responders that provide revocation status of certificates.

- Simple Certificate Validation Protocol (SCVP) Servers that validate certifications paths or provide revocation status checking services[4].

OCSP Responders that are keyless and simply repeat responses signed by other Responders and SCVP Servers that do not provide certificate validation services adhere to the same security requirements as repositories.

CAs that issue end-entity certificates at any of the IceCAP levels of assurance must provide OCSP Responder. Furthermore, the OCSP Responders shall be issued CA-delegated certificates(s) in order to ensure interoperability with cross certified partners.

1.3.1.12 Card Management System (CMS)

The Card Management System is responsible for managing smart card token content. In the context of this CP, the CMS requirements are mandatory for the IceCAP policies and optional for other certificate policies. CAs issuing IceCAP certificates are responsible for ensuring that all CMSs meet the requirements described in this document. In addition, the CMS shall not be issued any certificates that express the IceCAP-hardware or IceCAP-cardAuth policy OID.

1.3.1.13 Key Recovery System (KRS)

The Key Recovery System consists of the information system (or systems) and operations personnel used to provide key escrow and key recovery services.

The KRS consists of the Key Escrow Database (KED) and Key Recovery Workstation and may include one or more Data Decryption Servers (DDS). KRS personnel include the Key Recovery Agents (KRA) and, optionally, Key Recovery Officers (KRO).

The applicable requirements for physical, personnel, and procedural security controls, technical security controls and Compliance Audit apply as follows:

- CA requirements apply to the KED and to the DDS.
- RA requirements apply to the KRA and KRA automated systems.
- RA requirements apply to the KRO and KRO automated systems, when the KRO has privileged access to the KED.

1.3.1.13.1 Key Escrow Database (KED)

The Key Escrow Database is the function, system, or subsystem that maintains the key escrow repository and responds to key registration requests. The KED also responds to key recovery requests from two or more key recovery trusted role personnel (e.g., KRAs) or self-recovery by a current Subscriber.

Practice Note:
In some cases, the CMS may incorporate key escrow services. If so, the CMS must include the provision for preserving the enforcement of two-person integrity of key recovery operations.

---

[4] There are three types of SCVP Servers: path development, path validation with revocation checking, and path validation without revocation checking. The path development servers are not considered within the scope of this policy since the corruption of these servers does not adversely impact security and hence they need not be subject of a CP.

1.3.1.13.2 Key Recovery Workstation

Key Recovery Workstations are used by the key recovery trusted role personnel to securely communicate with the KED for the recovery of escrowed keys.

1.3.1.13.3 Data Decryption Server (DDS)

Also known as a Key Server, the Data Decryption Server is an automated system that obtains subscriber private keys or session keys from the KED or from another Key Server for data monitoring or other purposes (e.g., email inspection). A DDS does not provide keys to Subscribers or other Third-Party Requestors. A DDS must adhere to physical, personnel, procedural and technical security requirements of the KED.

The use of a DDS is optional and is based on organizational needs. Where a DDS is not implemented by an organization, this section and any subsequent references to the DDS may be omitted from the CP.

1.3.1.14 Administration Workstation

Administration Workstations may be used to administer CA, KED, DDS, CMS, and CSA equipment and/or the associated HSMs from a specific secure location inside or outside the security perimeter of the CA, KED, DDS, CMS, and CSA. In essence, the secure location housing the Administration Workstation is a logical extension of the secure enclave in which the CA, KED, DDS, CMS, and CSA equipment reside.

1.3.2 Registration Authority (RA)

A Registration Authority (RA) is comprised of the systems, procedures and personnel that collect and verify each Subscriber's proof of identity and the subject information that is to be entered into the associated public key certificate. The RA interacts with the CA to enter and approve the subscriber certificate request information. There may be multiple RA personnel and systems associated with a single CA.

The CertiPath Operational Authority acts as the RA for the CertiPath CAs and performs its function in accordance with the CBCA CPS and CRCA CPS.

An RA may assume the duties of a Key Recovery Agent or Key Recovery Officer for the recovery of escrowed private decryption keys on behalf of Subscribers and third-party requestors or these roles may be assigned to separate personnel:

1.3.2.1 Key Recovery Agent (KRA)

A Key Recovery Agent is an individual who, using a two-party control procedure with a second KRS trusted role individual, is authorized to interact with the KED in order to recover an escrowed key. Because KRAs can recover large numbers of keys, the number and location of KRAs should be closely controlled. KRAs are considered Trusted Role personnel.

Two KRS trusted role individuals are required for a successful key recovery.

In addition, KRAs may conduct requestor identity verification and authorization validation when KROs are not used.

1.3.2.2 Key Recovery Officer (KRO)

An Entity may choose to use the services of a Key Recovery Officer (KRO) to perform identity verification and authorization validation tasks in support of key recovery. KROs authenticate the identity of the Key Recovery Requestor. KROs that do not belong to the organization maintaining the KRS shall be able to participate in the recovery of keys of Subscribers from the KROs' Organization/Enterprise only.

KROs perform their duties from a workstation that securely communicates with the KRA. A KRO performs the following:

- Authentication of the requestor;
- Validation of the requestor's authorization;
- Secure transmission of key recovery requests to a KRA.

When KROs are not used, authentication of the requestor and validation of the requestor's authorization to recover keys are the responsibility of the KRA.

1.3.3 Subscribers

A Subscriber is the entity whose name appears as the subject in an end-entity certificate, agrees to use its key and certificate in accordance with the certificate policy asserted in the certificate, and does not itself issue certificates. CertiPath CA Subscribers include only CertiPath Operational Authority personnel and, when determined by the CPMA, certain network or hardware devices such as firewalls, web servers, and routers when needed for infrastructure protection. CAs are sometimes technically considered "Subscribers" in a PKI. However, the term "Subscriber" as used in this document refers only to those entities who request certificates for uses other than signing and issuing certificates or certificate status information.

1.3.3.1 Affiliated Organizations

Subscriber certificates may be issued in conjunction with an organization that has a relationship with the Subscriber; this is termed affiliation. The organizational affiliation shall be indicated in a relative distinguished name in the subject field in the certificate, and the certificate shall be revoked in accordance with Section 4.9.1 when affiliation is terminated.

1.3.3.2 Key Recovery Requestor

A Key Recovery Requestor is the person who requests the recovery of a decryption private key. A Requestor is generally the Subscriber itself (for self-recovery) or a third-party (e.g., supervisor, corporate officer, or law enforcement officer) who is authorized to request recovery of a Subscriber's escrowed key. Any individual who can demonstrate verifiable authority and a need to obtain a recovered key can be considered a Key Recovery Requestor.

1.3.3.2.1 Internal Third-party Requestor

An Internal Third-party Requestor is any Requestor who is in the Subscriber's supervisory chain or otherwise authorized to obtain the Subscriber's key for the Organization/Enterprise. The Subscribers' Organization/Enterprise shall appoint authorized Internal Key Recovery Requestors, and the PKI shall implement key recovery such that the existing Organization/Enterprise Policy regarding access and release of sensitive information is met.

1.3.3.2.2 External Third-party Requestor

An External Third-party Requestor is someone outside the Subscribers' Organization/Enterprise with authorization from the Organization's legal department to obtain the decryption private key of the Subscriber. An External Key Recovery Requestor must work with an Internal Key Recovery Requestor unless the law requires the Entity to release the Subscriber's private key without approval of the Subscriber's Organization/Enterprise. Nothing in this document is intended to change the current

procedures of the Organization/Enterprise for obtaining information about individuals in connection with such requests.

Practice Note: The authorization process is determined by the organization and may include the requirement for authorized court orders or other demonstrable legal rights to the information, and requests from customer organizations.

1.3.4 Relying Parties

A Relying Party is the entity that relies on the validity of the binding of the Subscriber's name to a public key. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The Relying Party can use the certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate. A Relying Party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

1.3.5 Other Participants

1.3.5.1 Related Authorities

The CertiPath CAs and Entity CAs operating under this CP will require the services of other security, community, and application authorities, such as compliance auditors and attribute authorities.

The CBCA CPS and CRCA CPS shall identify the parties responsible for providing such services to CertiPath, and the mechanisms used to support these services.

The Entity CPS shall identify the parties responsible for providing such services to the Entity, and the mechanisms used to support these services.

1.3.5.2 Trusted Agent

A Trusted Agent is appointed by PKI Operational Authority personnel and may collect and verify Subscriber identity and information on behalf of an RA.

Information shall be verified in accordance with Section 3.2 and communicated to the RA in a secure manner. A Trusted Agent shall not have privileged access to the CA to enter or approve subscriber information.

When Trusted Agents are used, the CPS must include any criteria associated with the appointment of the Trusted Agent, to include vetting and training or certification (e.g. notary public). Identity proofing artifacts produced by a Trusted Agent must be traceable to the individual that produced them.

1.3.6 Applicability

The sensitivity of the information processed or protected using certificates issued by CertiPath CAs or an Entity CA will vary significantly. Relying Party Entities must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is performed by each Entity for each application and is not controlled by this CP.

To provide sufficient granularity, this CP specifies security requirements for the assurance levels listed in Section 1.2.

The certificate levels of assurance contained in this CP are set forth below, as well as a brief and non-binding description of the applicability for applications suited to each level.

Assurance Level	Applicability
Medium-software or Medium-CBP-software	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud or involving access to private information where the likelihood of malicious access is substantial. Subscriber private keys are stored in software at this assurance level.
IceCAP-cardAuth	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include contactless smart card readers where use of an activation pin is not practical.
Medium-hardware or Medium-CBP-hardware	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud or involving access to private information where the likelihood of malicious access is substantial. Subscriber private keys are stored in hardware at this assurance level.
IceCAP-hardware, or IceCAP-contentSigning	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud or involving access to private information where the likelihood of malicious access is substantial. Subscriber private keys are stored in hardware at this assurance level.
High-hardware or High-CBP-hardware	This level is relevant to environments where risks and consequences of data compromise are high. This may include transactions having high monetary value or risk of fraud or involving access to private information where the likelihood of malicious access is high. Subscriber private keys are stored in hardware at this assurance level.

1.3.6.1 Factors in Determining Usage

The Relying Party must first determine the level of assurance required for an application, and then select the certificate appropriate for meeting the needs of that application. This will be determined by evaluating various risk factors including the value of the information, the threat environment, and the existing protection of the information environment. These determinations are made by the Relying Party and are not controlled by the CPMA or the CertiPath Operational Authority. Nonetheless, this CP contains some helpful guidance, set forth herein, which Relying Parties may consider in making their decisions.

1.3.6.2 Obtaining Certificates

This CP requires publication and access to CA certificates and CRLs. This CP imposes no requirements in terms of publication and access to end entity (i.e., Subscriber) certificates. The relying party applications must make their own agreements for obtaining the subscriber certificates. This could be trivially done for signature applications by including the signer certificate in the application protocol. For encryption applications, the relying party must develop a means to access subscriber certificates. Use of X.500 and LDAP Repositories is one way to achieve this, but this CP does not mandate which mechanism a Relying Party must use.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

None beyond those specified in Section 1.3.6.

1.4.2 Prohibited Certificate Uses

Certificates that map to id-IceCAP-cardAuth are used only to authenticate the hardware token containing the associated private key and shall not be interpreted as authenticating the presenter or holder of the token..

1.5 Policy Administration

1.5.1 Organization administering the document

The CPMA is responsible for all aspects of this CP.

1.5.2 Contact Person

Questions regarding this CP shall be directed to the Chair of the CPMA. The current CPMA Chair can be found at https://certipath.com/services/federated-trust/policy-management-authority/

1.5.3 Person Determining Certification Practice Statement Suitability for the Policy

The CPWG shall approve the CBCA CPS and CRCA CPS. Entities are responsible for determining whether their CPSs conform to their CPs, and in particular, properly adhere to any policy mappings approved by the CPMA between this CP and the Entity CP. Entities will be required to attest to such compliance periodically as established by the CPMA. Further, the CPMA reserves the right to audit Entity compliance as set forth in this CP and in the AGREEMENT between CertiPath and the Entity.

In each case, the determination of suitability shall be based on an independent compliance assessor's results and recommendations. The compliance assessor shall be independent from the entity being audited. The compliance assessor may not be the author of the subject CPS. The CPMA shall determine whether a compliance assessor meets these requirements (See Section 8 for complete assessor requirements).

1.5.4 CPS Approval Procedures

The term CPS is defined in the Internet RFC 3647, X.509 Public Key Infrastructure Certificate Policy and Certificate Practices Framework as: "A statement of the practices which a Certification Authority employs in issuing certificates." It is a comprehensive description of such details as the precise implementation of service offerings and detailed procedures of certificate life-cycle management. It shall be more detailed than the corresponding certificate policy described above. The CBCA CPS and CRCA CPS which are drafted by the CertiPath Operational Authority and approved by the CPWG, specify how this CP and any AGREEMENTS that the CPMA has approved will be implemented to ensure compliance with their provisions.

1.5.5 Waivers

There shall be no waivers to this CP.

2 PUBLICATION & PKI REPOSITORY RESPONSIBILITIES

2.1 PKI Repositories

Entities that interoperate with the CertiPath CAs shall make their PKI Repositories available over the Internet to the CertiPath relying parties. The PKI Repositories shall contain the information necessary to support interoperation of the Entity PKI domains that employ the CertiPath CAs for this purpose.
Entities and the CertiPath Operational Authority may use a variety of mechanisms for posting information into their respective repositories as required by this CP. These mechanisms at a minimum shall include:

- Availability of the information as required by the certificate information posting and retrieval stipulations of this CP, and
- Access control mechanisms when needed to protect repository information as described in later sections.

The PKI Repositories containing certificates and certificate status information shall be deployed so as to provide 24 hour per day/365 day per year availability. CertiPath shall implement features to provide high levels of PKI Repository reliability (99% availability or better).

2.2 Publication of Certificate Information

2.2.1 Publication of CA Information

The Operational Authority shall publish information concerning the CertiPath CAs necessary to support their use and operation.

Entities shall publish information pertaining to their CAs in the Entities' interoperable PKI Repositories.

All CA certificates valid through the CBCA shall be posted in publicly accessible HTTP URIs.

- With the exception of self-signed certificates, all CA certificates issued *to* the CA shall be published in a file available via a publicly accessible HTTP URI. This URI must be asserted in the Authority Information Access (AIA) extension in all certificates issued *by* the CA.
- With the exception of self-signed certificates and those CA certificates with the Basic Constraints path length constraint set to zero, after February 21, 2023, all new CA certificates issued *by* the CA shall be published in a second file available via a publicly accessible HTTP URI. This URI must be asserted in the Subject Information Access (SIA) extension in all certificates issued *to* the CA.

In both cases, the file must be a certs-only Cryptographic Message Syntax file that has an extension of .p7c.

The latest CRL covering all unexpired certificates shall be posted as a file available via a publicly accessible HTTP URI until such time as all issued certificates have expired.

This URI shall be asserted in the CRL distribution point extension of all certificates issued by that CA, with the exception of OCSP responder certificates that include the *id-pkix-ocsp-nocheck* extension.

CAs that provide OCSP must do so in the form of a publicly accessible delegated OCSP service, as described in Section 2.6 of RFC 6960. OCSP services must be

designed and implemented to provide 99% availability or better, with resources sufficient to provide a response time of ten (10) seconds or less under normal operating conditions.

Practice Note:
Internet disruptions may impact the response time experienced by the relying party.

2.2.2 Certificate Policy Publication

This CP and the Annual Audit Opinion Letter for the CertiPath Bridge CA are publicly available on https://certipath.com/services/federated-trust/policy-management-authority/.

Entity Certificate Policies must be available in publicly accessible internet locations.

2.3 Time or Frequency of Publication

Certificate Policy updates (revisions) must be made publicly available within thirty (30) days of approval.

Certificates and certificate status information shall be published as specified in this CP in Section 4.

2.4 Access Controls on PKI Repositories

Any PKI Repository information not intended for public dissemination or modification shall be protected.

IceCAP certificates that contain the UUID in the subject alternative name extension shall not be distributed via publicly accessible repositories (e.g., HTTP, LDAP, etc.).

Public keys and certificate status information in the CertiPath PKI Repository shall be publicly available through the Internet.

Access to information in Entity PKI Repositories shall be determined by the Entity pursuant to the rules and statutes that apply to that entity.

3 IDENTIFICATION & AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

CAs shall generate and sign certificates containing an X.500 Distinguished Name (DN) in the Issuer and in Subject fields; the X.500 DN may contain domain component elements. Subject Alternative Name may also be used, if marked non-critical.

3.1.1.1 Subject Names

For certificates issued to human Subscribers, the subject DN shall either contain the value “Unaffiliated” in the last organizational unit (ou) attribute or shall contain the affiliated organization name in an appropriate relative distinguished name attribute (e.g., organization (o), organizational unit (ou), or domain component (dc) attribute).

IceCAP-contentSigning certificates shall clearly indicate the organization administering the CMS.

IceCAP-cardAuth certificates subject DN shall not contain the common name. Instead, the DN shall populate the *serialNumber* attribute with the Universally Unique Identifier (UUID) associated with the card.

For IceCAP certificates with the exception of the IceCAP-contentSigning certificate, the subject DN shall either contain the value “Unaffiliated” in the last organizational unit (ou) attribute or shall contain the affiliated organization name in an appropriate relative distinguished name attribute (e.g., organization (o), organizational unit (ou), or domain component (dc) attribute). If the subject DN includes the value ou = “Unaffiliated”, the value ou = <Issuing CA CN> shall also be present.

For certificates issued to devices, the subject DN must contain a unique name for the device that does not take the form of a Human Subscriber name.

3.1.1.2 Subject Alternative Names

Subscriber certificates that contain an EKU value of id-kp-emailProtection shall include a rfc822Name in the Subject Alternative Name extension.

For Device Subscriber certificates that assert serverAuth in the Extended Key Usage:

- Wildcard domain names are permitted in the dNSName values only if all sub-domains covered by the wildcard fall within the same application, cloud service, or system boundary within the scope of the sponsoring organization.
- Wildcards shall not be used in subdomains that host more than one distinct application platform.

IceCAP-hardware and IceCAP-cardAuth certificates shall include a Subject Alternative Name extension containing a UUID value encoded as a URI.

IceCAP-cardAuth certificates shall not include any name other than the UUID value in the Subject Alternative Name extension.

3.1.2 Need for Names to be Meaningful

The certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates can be understood and used by Relying Parties. Names used in the certificates must identify the person or object to which they are assigned in a meaningful way.

All DNs shall accurately reflect organizational structures. The Subject Name in a CA certificate must match the Issuer Name in certificates it issues.

When DNs are used, it is preferable that the common name represents the Subscriber in a way that is easily understandable for humans. For people, this will typically be a legal name. For equipment, this may be a model name and serial number, or an application process (e.g., Organization X Mail List or Organization Y Multifunction Interpreter).

3.1.3 Anonymity or Pseudonymity of Subscribers

CA certificates shall not contain anonymous or pseudonymous identities.

DNs in certificates issued to Subscribers may contain a pseudonym to meet local privacy regulations provided name space uniqueness requirements are met, and such name is traceable to the specific Subscriber.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting name forms shall be contained in the applicable certificate profile. The authority responsible for Entity CA name space control shall be identified in the respective CP.

Rules for interpreting UUID are specified in RFC 4122.

3.1.5 Uniqueness of Names

Name uniqueness across the CertiPath domains, including cross-certified domains shall be enforced. The CAs and RAs shall enforce name uniqueness within the X.500 name space, which they have been authorized.

The CertiPath Operational Authority Manager shall be responsible for ensuring name uniqueness in certificates issued by the CertiPath CAs.

Entity CAs shall identify the authority that is responsible for ensuring name uniqueness in certificates issued by the entity CA.

It is good practice for Entities to include the following information in their CPS:

- What name forms shall be used, and
- How they will allocate names within the Subscriber community to guarantee name uniqueness among current and past Subscribers (e.g., if “Joe Smith” leaves a CA’s community of Subscribers, and a new, different “Joe Smith” enters the community of Subscribers, how will these two people be provided unique names?).

3.1.6 Recognition, Authentication & Role of Trademarks

CertiPath will not knowingly use trademarks in names unless the subject has the rights to use that name.

Entity Certificate Policies shall identify the use and role of trademarks within their PKI environments.

3.1.7 Name Claim Dispute Resolution Procedure

The CPMA shall resolve any name collisions brought to its attention that may affect interoperability.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

In all cases where the party named in a certificate generates its own keys that party shall be required to prove possession of the private key, which corresponds to the public key in the certificate request. For signature keys, this may be done by the entity using its private key to sign a value and providing that value to the issuing CA. The CA shall then validate the signature using the party's public key. The CPMA may allow other mechanisms that are at least as secure as those cited here.

3.2.2 Authentication of Organization Identity

Requests for cross certificates shall include the CA name, address, and documentation of the existence of the CA. Before issuing cross certificates, the issuing CA shall verify the information provided, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the CA.

The existence of an affiliated organization shall be verified prior to issuing any end user certificates on its behalf. In addition, the RA shall verify the authenticity of the requesting representative and the representative's authorization to act in the name of the organization.

Requests for end-user certificates other than unaffiliated Subscribers shall include the name of the organization and shall be verified with the identified affiliated organization.

3.2.3 Authentication of Individual Identity

The CA must authenticate the identity of the individual requestor for each certificate issued.

In addition to the processes described below, Subscriber certificates may be issued on the basis of an electronically authenticated request using a valid signature or authentication certificate and associated private key, with the following restrictions:

- The assurance level of the new certificate shall be the same or lower than the assurance level of the certificate used to authenticate the request.
- Identity information in the new certificate must match the identity information in the certificate used to authenticate the request.
- The expiration date of the new certificate shall not exceed the next required initial identity authentication date associated with the certificate used to authenticate the request.
- The next initial identity authentication date remains unchanged in the event of a new certificate issuance based on electronic authentication.

This electronic authentication process does not remove the requirement for in-person identity proofing.

3.2.3.1 Authentication of Human Subscriber Identity

IceCAP-hardware certificates shall be issued to human Subscribers only.

Identity shall be established by in-person or supervised remote[5] identity proofing before the RA, Trusted Agent, or an entity certified by a State or Federal Entity as being authorized to confirm identities; information provided shall be verified to ensure legitimacy. Requirements for authentication of individual identity using an in-person antecedent are listed in Section 3.2.3.4.

The applicant shall present one valid National Government-issued photo ID, one valid U.S. State REAL ID Act-compliant picture ID[6] or two valid non-National Government IDs, one of which shall be a recent photo ID.

The CA or an RA shall ensure that the applicant's identity information is verified and checked in accordance with the applicable CP and CPS. The CA or an RA shall ensure that the applicant's identity information and public key are properly bound. Additionally, the CA or the RA shall record the process that was followed for issuance of each certificate. Process information shall depend upon the certificate level of assurance and shall be addressed in the applicable CPS. The process documentation shall include the following:

- The identity of the person performing the identity verification and either;
    - A signed declaration by that person that the identity of the applicant was verified as required by the applicable certificate policy which may be met by establishing how the applicant is known to the verifier as required by this certificate policy, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law; The signature on the declaration may be either a handwritten or digital signature using a certificate that is of equal or higher level of assurance as the credential being issued; or
    - An auditable record linking the authentication of the person performing the identification to the verification of each Applicant.
- Unique identifying numbers from the ID of the verifier and from an ID of the applicant or, in the case of electronic authentication, the serial number, subject key identifier, public key or other unique identifier from the certificate used to authenticate the request;
- The date and time of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature or appropriate digital signature (see Practice Note) and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

Practice Note:
In those cases in which the individual is in possession of a valid digital signature credential of equal or higher level of assurance or the signature certificate is generated immediately upon authentication of the applicant's identity, the applicant may sign the declaration of identity and certificate of acceptance using the digital credential. In the latter case, if the applicant fails to sign the declaration of identity, then the certificate must be revoked.

---

[5] Supervised Remote Identity proofing must be implemented in a manner that conforms to Section 5.3.3.2 of NIST SP 800-63A *Digital Identity Guidelines: Enrollment and Identity Proofing,* dated June 2017. Future changes to NIST SP 800-63A will be reviewed for consideration by the CertiPath PMA.

[6] REAL ID Act-compliant IDs are identified by the presence of the U.S. Department of Homeland Security REAL ID star.

At the IceCAP-hardware and IceCAP-cardAuth assurance levels, the following additional requirements shall apply:

- In-person antecedent method shall not be used.
- Identity proofing shall be performed by an RA or a Trusted Agent only.
- The applicant shall present two identity source documents in original form. The identity source documents shall come from the list of acceptable documents included in *FIPS 201-3, Section 2.7* (see Section 12).
- Two electronic fingerprints shall be collected and stored on the card for automated authentication during card usage (See Section 12 for additional requirements).
- An electronic facial image shall be collected. The facial image shall be printed on the card and stored on the card for visual authentication during card usage. A new facial image shall be collected each time a card is issued (See Section 12 for additional requirements).
- The identity proofing, registration and issuance process shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a credential without the cooperation of another authorized person.

In the event an applicant is denied a credential based on the results of the identity proofing process, the applicant shall be given an opportunity to provide additional identity documentation prior to final rejection.

3.2.3.2 Authentication of Device Identities

Some computing and communications devices (routers, firewalls, servers, etc.) will be named as certificate subjects. In such cases, the device shall have a human PKI Sponsor. The PKI Sponsor should have been issued a credential that is equal to or higher assurance level than the credential being sponsored. The PKI sponsor shall be responsible for the security of the private key and for providing the following registration information:

- Equipment identification (e.g., serial number) or service name (e.g., DNS name) or unique software application name
- Equipment or software application public keys
- Equipment or software application authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or RA to communicate with the sponsor when required.

The registration information provided by the human sponsor shall be verified to an assurance level commensurate with the certificate assurance level being requested. Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

- Verification of digitally signed messages sent from the sponsor (using certificates of equivalent or greater assurance than that being requested).
- In person registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of Section 3.2.3.1

In the event a human sponsor is changed, the new sponsor shall review the status of each sponsored device to ensure it is still authorized to receive certificates. The CPS shall describe procedures to ensure that certificate accountability is maintained.

3.2.3.3 Human Subscriber Re-Authentication following loss, damage, or key compromise

If human subscriber credentials containing the private keys associated with the public key certificates are lost, damaged, or stolen, the Subscriber may be issued new certificates using the process described in this section. However, the validity period of the certificates issued using this process shall not exceed the identity-reproofing requirements in Section 3.3.1. Alternatively, the Subscriber can undergo an initial identity proofing process described in Section 3.2.3.1.

The Subscriber shall present one valid National Government-issued photo ID or valid non-National Government issued photo ID (e.g., Driver's License, Passport). In addition and where applicable, the RA shall match a good fingerprint or other adequate biometric from the Subscriber with the biometric stored in an authoritative trusted database. This database shall be protected as stipulated in Section 4.3 of this CP.

The CA or an RA shall ensure that the Subscriber's identity information and public key are properly bound. Additionally, the CA or the RA shall record the process that was followed for issuance of each certificate. Process information shall depend upon the certificate level of assurance and shall be addressed in the applicable CPS. The process documentation shall include the following:

- The identity of the person performing the identity verification;
- A signed declaration by that person that the identity of the Subscriber was verified as required by the applicable certificate policy which may be met by establishing how the Subscriber is known to the verifier as required by this certificate policy;
- Unique identifying numbers from the Identifier (ID) of the verifier and from the ID of the Subscriber;
- The date and time of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature or appropriate digital signature and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

In addition, if the credentials are lost, stolen or otherwise unaccounted for, all certificates associated with the private keys on the credentials shall be revoked for the reason of key compromise. This CP also requires that when a certificate is revoked for the reason of key compromise, the derivative certificates (i.e., certificates issued on the basis of the compromised certificate) also be revoked.

3.2.3.4 Human Subscriber Initial Identity Proofing Via Antecedent Relationship

The following requirements shall apply when human subscriber identity is verified using antecedent relationship with a Sponsor:

1. The Sponsor shall have an established relationship with the Entity PKI.
2. The Sponsor shall have an established on-going working[7] relationship with the Subscriber sufficient enough to enable the RA to, with a high degree of certainty,

[7] One example of "established on-going working relationship" is the person is employed by or reports to the Certificate Sponsor. Another example is the person is a member of a professional organization which is acting as the Sponsor.

verify that the Human Subscriber is the same person that was identity proofed by the Sponsor;

3. Initial contact information for the Human Subscriber shall be provided by the Sponsor (e.g., name, email address, phone number, etc.).
4. The Sponsor shall provide a signed statement to the RA containing the following information:
    a) Date of original identity proofing event
    b) A description of the ID documents provided during the antecedent identity proofing process. These documents must satisfy the requirements in Section 3.2.3.1 of this CP.
    c) Historical artifacts associated with the Antecedent event, if any.
    d) The name, date of birth, and other personal information that bind the individual to the identity.
5. Exchange of information between the Sponsor, the Subscriber and the RA directly pertaining to the antecedent issuance process shall be secure, and the information shall be validated, protected, and securely exchanged.
6. The RA shall use the Subscriber information provided by the Sponsor to establish contact with the Subscriber.
7. The Human Subscriber shall present a valid Sponsor-issued photo ID that matches information provided by the Sponsor as proof of identity.
8. The Human Subscriber shall sign a declaration of identity using a handwritten signature or appropriate digital signature using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

3.2.3.5 Authentication of Human Subscriber for Role Certificates

Subscribers may be issued role certificates. A role certificate shall identify a specific role title on behalf of which the Subscriber is authorized to act rather than the Subscriber's name. A role certificate can be used in situations where non-repudiation is desired. A role certificate shall not be a substitute for an individual subscriber certificate. Multiple Subscribers can be assigned to a role at the same time; however, the signature key pair shall be unique to each role certificate issued to each individual; the encryption key pair and encryption certificate may be shared by the individuals assigned the role.

Subscribers issued role certificates shall protect the corresponding role credentials in the same manner as individual credentials.

The procedures for issuing role certificates shall comply with all other stipulations of this CP (e.g., subscriber identity proofing, validation of organization affiliation, key generation, private key protection, and Subscriber obligations). For the role signature certificate, the individual assigned the role or the role sponsor may act on behalf of the certificate subject for certificate management activities such as renewal, re-key and revocation. Issuance and modification of role signature certificate shall require the approval of the role sponsor. Rekey and renewal of role signature certificate shall require the approval of the role sponsor if the validity period is extended beyond that already approved by the role sponsor. For the role encryption certificate, only the role sponsor may act on behalf of the certificate subject for certificate management activities such as issuance, renewal, re-key, modification, and revocation.

The CA or the RA shall record the information identified in Section 3.2.3 for a sponsor associated with the role before issuing a role certificate. The role sponsor shall hold an individual certificate issued by the same CA at the same or higher assurance level as the

role certificate. The CA or the RA shall validate from the role sponsor that the individual Subscriber has been approved for the role certificate.

The role sponsor (which is not a trusted role) shall be responsible for:

1. Authorizing individuals for a role certificate;
2. Recovery of the private decryption key
3. Revocation of individual role certificates;
4. Always maintaining a current up-to-date list of individuals who are assigned the role; and
5. Always maintaining a current up-to-date list of individuals who have been provided the decryption private key for the role.

Practice Note:
When determining whether a role certificate is warranted, consider whether the role carries inherent authority beyond the job title. Role certificates may also be used for individuals on temporary assignment, where the temporary assignment carries an authority not shared by the individuals in their usual occupation, for example: "*Chair PKI Process Action Team*".

3.2.4 Non-verified Subscriber Information

Subscriber information that is not verified shall not be included in Certificates.

3.2.5 Validation of Authority

An Issuer CA shall validate the subject CA certificate requestor's authorization to act in the name of the Subject CA prior to issuing a cross certificate or subordinate certificate. In addition, the CertiPath CAs shall obtain the CPMA approval prior to issuing CA certificates. In the case of the CBCA, the certificate issuance shall be based on successful mapping of the Subject CA CP with this CP. In the case of the CRCA, certificate issuance shall be based on successful CPS compliance analysis and CPMA approval.

Certificates that contain explicit or implicit organizational affiliation shall be issued only after ascertaining the applicant has the authorization to act on behalf of the organization in the asserted capacity.

3.2.6 Criteria for Interoperation

A PCA or a Bridge CA shall adhere to the following requirements:

- Have a CP mapped to, and determined by the CPMA to be in conformance with this CP;
- Operate a PKI that has undergone a successful compliance audit pursuant to Section 8 of this CP and as set forth in the Subject CA CP;
- Issue certificates compliant with the profiles described in this CP, and make certificate status information available in compliance with this CP; and
- Provide CA certificate and certificate status information to the relying parties.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-key

CA and subscriber re-key requests shall be authenticated using their existing private key to sign a subscriber request or establish a client authenticated TLS session, and validated using the associated, currently valid public key certificate. Alternatively,

authentication shall be accomplished using the initial identity-proofing process as described in Section 3.2.

For high-hardware and high-CBP-hardware assurance certificates, identity shall be established through the initial identity-proofing process at least once every three years. For medium-software, medium-hardware, medium-device-software, medium-device-hardware, medium-CBP-software, and medium-CBP-hardware assurance certificates, identity shall be established through the initial identity-proofing process at least once every twelve years. For CAs, as required in Section 3.2, identity shall be re-established through the initial registration process at least once every three years, see Section 3.2.2.

When a current public key certificate is used for identification and authentication purposes, the expiration date of the new certificate shall not cause the certificate subject to exceed the initial identity-proofing time frames specified in the paragraph above; and the assurance level of the new certificate shall not exceed the assurance level of the certificate being used for identification and authentication purposes.

3.3.2 Identification and Authentication for Re-key after Revocation

If a certificate has been revoked, the certificate subject shall be authenticated using the initial identity-proofing process as described in Section 3.2. Alternatively, human subscriber identity may be verified through the use of biometrics retained in the IDMS as part of the original identity proofing process.

3.4 Identification and Authentication for Revocation Request

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

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

Communication among the CA, RA, Trusted Agent, other parties confirming identities, and Subscribers shall have requisite security services (i.e., source authentication, integrity, non-repudiation, or confidentiality) applied to them commensurate with the assurance level of the certificate being managed. For example, packages secured and transported in a tamper-evident manner by a certified mail carrier meet the integrity and confidentiality requirements for the High Hardware assurance level. When cryptography is used, the mechanism shall be at least as strong as the certificates being managed. For example, a web site secured using a TLS certificate issued under medium-software policy and set up with appropriate algorithms and key sizes satisfies integrity and confidentiality requirements for medium-software certificate management.

The content of the communication shall dictate if some, all, or none of the security services are required.

4.1 Certificate Application

This paragraph applies to entities seeking cross certificates for their Principal CAs from the CBCA or subordinate certificates for their Signing CAs from the CRCA. The CPMA establishes procedures for entities to use in applying for a certificate from a CertiPath CA and publishes those procedures. CertiPath, based on CPMA recommendation, shall enter into an AGREEMENT with the applicant Entity, and shall instruct the Operational Authority to issue the certificate to the Entity. The Entity CA (PCA or Signing CA) shall have a unique distinguished name that shall be placed in the Subject field of the certificate with the common name as the official name of the CA.

The CBCA may issue end-entity certificates to trusted personnel where necessary for the internal operations of the CBCA. The CBCA shall not issue end-entity certificates for any other reasons.

Requests by a CA for a CA certificate from one of the CertiPath CAs shall be submitted to the CPMA using a procedure and application form developed by the CPMA. The CPMA shall make the procedures and application form available to all entities. The application shall be accompanied by a CP and/or a CPS written to the format of the *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* [RFC3647]. Additionally, the application shall propose a mapping between the levels of assurance expressed in the Entity's CP, and those in this CP.

The CPMA shall evaluate the application in accordance with the CertiPath Criteria and Methodology and make a determination regarding whether or not to issue the requested certificate(s), and what policy mappings to express in the certificate(s), if applicable[8]. CertiPath, based on CPMA recommendation, and the applicant CA shall then enter into an AGREEMENT setting forth their respective responsibilities. The CPMA Chair shall direct the Operational Authority to issue the certificate(s). Upon issuance, each certificate issued by a CertiPath CA shall be manually checked to ensure each field and extension is properly populated with the correct information, before the certificate is delivered to the Subject CA.

[8] Note that Signing CA certificates issued by the CRCA do not require policy mapping; nor do cross certificates between the CRCA and CBCA.

4.1.1 Submission of Certificate Application

For certificate applications to a CertiPath CA, an authorized representative of the Subject CA shall submit the application to the CPMA.

For submission of certificate applications to an Entity CA, the Entity CA CP shall describe the submission process for its CAs and Subscribers.

4.1.2 Enrollment Process and Responsibilities

Applicants for public key certificates shall be responsible for providing accurate information in their applications.

For Entity CAs as Issuers, the applicable CP shall describe the enrollment process for its subordinate or cross-certified CAs and Subscribers.

All communications supporting the certificate application and issuance process shall be authenticated and protected from modification. Cryptographic mechanisms commensurate with the strength of the private key shall be used to protect electronic communications between the RA and CA.

4.2 Certificate Application Processing

It is the responsibility of the CA and RA to verify that the information in certificate applications is accurate. The applicable CP or CPS shall specify procedures to verify information in certificate applications.

4.2.1 Performing Identification and Authentication Functions

For the CertiPath CAs, the CertiPath Operational Authority shall perform the identity-proofing of applicant CAs and other Subscribers.

For Entity CAs, the identity-proofing of subordinate CAs and Subscribers shall meet the requirements specified in the respective CP. To allow cross-certification, those requirements shall also meet the provisions for Subscriber identity-proofing and authentication as specified in this CP at the applicable levels of assurance. The Entity CP shall identify the components of the Entity PKI that are responsible for proofing or authenticating the Subscriber's identity in each case.

4.2.2 Approval or Rejection of Certificate Applications

For Entity CAs seeking to cross certify or subordinate to the CertiPath CAs, the CPMA may approve or reject a certificate application.

For Entity CAs as issuers, the Entity CP shall identify the person or an organizational body that may accept or reject a certificate application.

4.2.3 Time to Process Certificate Applications

Certificate application processing from the time the request/application is posted on the CA or RA system to certificate issuance shall not exceed 90 days.

4.3 Certificate Issuance

Upon receiving a request for a certificate, the CA or RA shall respond in accordance with the requirements set forth in the applicable CP and CPS.

The certificate request may contain an already built ("to-be-signed") certificate. This certificate will not be signed until the process set forth in the CP and CPS has been met.

While the Subscriber may do most of the data entry for a certificate, it is still the responsibility of the CA and the RA to verify that the information is correct and accurate. This may be accomplished through a system approach linking trusted databases containing personnel information, other equivalent authenticated mechanisms, or through personal contact with the Subscriber's sponsoring organization. If databases are used to confirm Subscriber information, then these databases must be protected from unauthorized modification to a level commensurate with the level of assurance of the certificate being sought. Specifically, the databases shall be protected using physical security controls, personnel security controls, cryptographic security controls, computer security controls, and network security controls specified for the RA elsewhere in this CP.

4.3.1 CA Actions during Certificate Issuance

The CA shall:

- Verify the identity and authority of the requestor;
- Verify the information in the request before inclusion in the certificate;
- Generate and sign the certificate;
- Check the certificate to ensure that all fields and extensions are properly populated; and
- Post the certificate as set forth in its respective CP, after formal subscriber acceptance (see Section 9.6.3).

4.3.2 Notification to Subscriber of Certificate Issuance

The CA shall notify the subject (CA or End Entity Subscriber) of certificate issuance. When a key management (encryption) certificate is issued, the Subscriber shall be notified that the associated private decryption keys will be escrowed.

4.4 Certificate Acceptance

The AGREEMENT shall be executed setting forth the responsibilities of all parties before the CPMA Chair authorizes issuance of a CA certificate by a CertiPath CA. Once a CA certificate has been issued, its acceptance by the Entity shall commence interoperability with the CertiPath PKI and triggers the Subject CA's obligations under the AGREEMENT and this CP.

End-entity Subscribers shall accept the responsibilities defined in Section 9.6.3 by signing the Subscriber agreement during certificate issuance.

4.4.1 Conduct Constituting Certificate Acceptance

For certificates issued by a CertiPath CA, certificate acceptance shall be governed by the AGREEMENT.

For certificates issued by an Entity CA, certificate acceptance shall be governed by the Entity CP.

4.4.2 Publication of the Certificate by the CA

All CA certificates shall be published in a PKI Repository accessible over the Internet.

Subscriber certificates containing policy OIDs cross-certified with IceCAP-hardware and IceCAP cardAuth shall not be published in a public repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The CertiPath OA shall inform the CPMA of any certificate issuance to a CA by a CertiPath CA.

When a PCA issues a certificate to the CBCA, the PCA shall notify the CPMA and CertiPath Operational Authority of the successful certificate issuance.

Notification of certificate issuance by the CBCA shall be provided to all cross-certified entities.

For Entity CAs, the CPMA shall be notified upon issuance of new CA certificates. In addition, the new CA certificate(s) shall be provided to the CPMA.

In the event a CA renews, rekeys or modifies a certificate without interaction with the RA system involved in the existing certificate's issuance, the CA must notify the RA of the action taken.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers and CAs shall protect their private keys from access by any other party.

Subscribers and CAs shall use their private keys for the purposes intended as constrained by the extensions (such as key usage, extended key usage, certificate policies, etc.) in the certificates issued to them.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties should accept public key certificates and associated public keys for the purposes intended as constrained by the extensions (such as key usage, extended key usage, certificate policies, etc.) in the certificates. In addition, relying parties should perform certificate validation in conformance with the full set of requirements specified in X.509.

4.6 Certificate Renewal

Renewing a certificate means creating a new certificate with a new serial number where all certificate subject information, including subject public key and subject key identifier, remain unchanged. The new certificate may have an extended validity period and may include new issuer information (e.g., different CRL distribution point, different AIA, and/or signed with a different issuer key).

After certificate renewal, the old certificate may or may not be revoked, but must not be used for requesting further renewals, re-keys, or modifications.

4.6.1 Circumstance for Certificate Renewal

A certificate may be renewed if it has not reached the end of its validity period and has not been revoked, the associated private key has not been compromised, and the Subscriber name and attributes are unchanged. The validity period of the new certificate must not exceed the remaining lifetime of the private key, as specified in Section 5.6. The identity proofing requirement listed in Section 3.3.1 shall also be met.

Subscriber certificates containing policy OIDs cross certified with an IceCAP policy OID shall not be renewed, except during recovery from CA key compromise. In such cases, the renewed certificate shall expire as specified in the original subscriber certificate.

CA certificates and Delegated OCSP responder certificates may be renewed so long as the aggregated lifetime of the private key does not exceed the requirements specified in Section 5.6.

4.6.2 Who may Request Renewal

The CertiPath Operational Authority Manager may request renewal of cross certificates.

A Subject may request the renewal of its certificate.

A PKI Sponsor may request renewal of a device certificate.

A RA may request renewal of a subscriber certificate.

A CA may request renewal of its subscriber certificates, e.g., when the CA re-keys.

4.6.3 Processing Certificate Renewal Requests

A certificate renewal shall be achieved using one of the following processes:

- Initial registration process as described in Section 3.2; or
- Identification & Authentication for Re-key as described in Section 3.3, except the old key can also be used as the new key.

For CA certificates issued by a CertiPath CA, certificate renewal also requires that a valid AGREEMENT exists between CertiPath and the Subject CA, and the term of the AGREEMENT is beyond the expiry period for the new certificate.

When certificates are renewed as a result of CA key compromise, the CA or RA must verify all certificates issued since the date of compromise were issued appropriately. If the certificate cannot be verified, it must not be renewed.

4.6.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

See Section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

See Section 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.7 Certificate Re-Key

Re-keying a certificate means that a new certificate is created that has the same characteristics and level as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key) and a different serial number, and it may be assigned a different validity period. After certificate rekey, the old certificate may or may not be revoked, but must not be used for requesting further re-keys, renewals, or modifications.

4.7.1 Circumstance for Certificate Re-key

A CA may issue a new certificate to the Subject when the Subject has generated a new key pair and is entitled to a certificate.

4.7.2 Who may Request Certification of a New Public Key

A Subject may request the re-key of its certificate.

A PKI Sponsor may request re-key of a device certificate.

4.7.3 Processing Certificate Re-keying Requests

A certificate re-key shall be achieved using one of the following processes:

- Initial registration process as described in Section 3.2; or
- Identification & Authentication for Re-key as described in Section 3.3.

For CA certificates issued by a CertiPath CA, certificate re-key also requires that a valid AGREEMENT exists between CertiPath and the Subject CA, and the term of the AGREEMENT is beyond the expiry period for the new certificate.

4.7.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

See Section 4.4.1.

4.7.6 Publication of the Re-keyed Certificate by the CA

See Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.8 Certificate Modification

Modifying a certificate means creating a new certificate that has the same or a different key and a different serial number, and that differs in one or more other fields, from an existing, currently valid certificate. For example, an Entity CA may choose to update a certificate of a Subscriber whose characteristics have changed (e.g., has just received a medical degree). The old certificate may or may not be revoked, but must not be used for further modifications, re-keys, or renewals.

Further, if an individual's name changes (e.g., due to marriage), then proof of the name change must be provided to the RA or the trusted agent in order for a modified certificate containing the new name to be issued.

4.8.1 Circumstance for Certificate Modification

A CA may issue a new certificate to the Subject when some of the Subject information has changed, e.g., name change due to change in marital status, change in subject attributes, etc., and the Subject continues to be entitled to a certificate.

4.8.2 Who may Request Certificate Modification

A Subject may request modification of its certificate.

A PKI Sponsor may request modification of a device certificate.

4.8.3 Processing Certificate Modification Requests

A certificate modification shall be achieved using one of the following processes:

- Initial registration process as described in Section 3.2; or

- Identification & Authentication for Re-key as described in Section 3.3. In addition, the validation of the changed subject information shall be in accordance with the initial identity-proofing process as described in Section 3.2.

For CA certificates issued by a CertiPath CA, certificate modification also requires that a valid AGREEMENT exists between CertiPath and the Subject CA, and the term of the AGREEMENT is beyond the expiry period for the new certificate.

In the event the modified certificate indicates a reduction in assurance level, the old certificate must be revoked.

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See Section 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

See Section 4.4.2.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.9 Certificate Revocation and Suspension

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

CertiPath shall notify all cross certified entities at least two weeks prior to the revocation of a CA certificate, whenever possible.

For Entity CAs, the CPMA shall be notified at least two weeks prior to the revocation of a CA certificate, whenever possible.

For emergency revocation, CAs shall follow the notification procedures in Section 5.7.

4.9.1 Circumstance for Revocation of a Certificate

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

- Identifying information or affiliation components of any names in the certificate become invalid;
- An organization terminates its relationship with the CA such that it no longer provides affiliation information;
- Privilege attributes asserted in the Subject's certificate are reduced;
- The Subject can be shown to have violated the stipulations of its agreement;
- The private key is suspected of compromise; or
- The Subject or other authorized party (as defined in the applicable CP or CPS) asks for the 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.

In addition, if it is determined subsequent to issuance of new certificates that a private key used to sign requests for one or more additional certificates may have been compromised at the time the requests for additional certificates were made, all certificates authorized by directly or indirectly chaining back to that compromised key shall be revoked.

An Entity PKI shall request that the CBCA revoke its cross-certificate if it does not meet the stipulations of the certificate policies listed in the cross certificate, including the CertiPath policy OIDs and “pass-through” policy OIDs.

4.9.2 Who Can Request Revocation of a Certificate

A certificate subject, human supervisor of a human subject, Human Resources (HR) representative for the human subject, PKI Sponsor for a device, issuing CA, or RA may request revocation of a certificate.

In the case of certificates issued by a CertiPath CA, the CPMA may request revocation of a certificate in accordance with its Charter.

For CA certificates, authorized individuals representing the CA operations may request revocation of certificates.

4.9.3 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 (e.g., digitally or manually signed).

Any CA may unilaterally revoke another CA certificate it has issued. However, the Operational Authority for a CertiPath CA shall revoke an Entity CA cross certificate only in the case of an emergency. Generally, a certificate will be revoked based on the authorized user’s request, authorized representative of subject request, or CPMA request.

Upon receipt of a revocation request, a CA shall authenticate the request and then revoke the certificate. In the case of a CA certificate issued by a CertiPath CA, the Operational Authority shall seek guidance from the CPMA before revocation of the certificate except when the CPMA is not available and there is an emergency situation such as:

- Request from the Subject CA for reason of key compromise;
- Determination by the Operational Authority that a Subject CA key is compromised; or
- Determination by the Operational Authority that a Subject CA is in violation of the CP, CPS, or MOA to a degree that threatens the integrity of the CertiPath PKI.

At the medium-hardware, medium-CBP-hardware, high-hardware, and high-CBP-hardware assurance levels, a Subscriber ceasing its relationship with an organization that sponsored the certificate shall, prior to departure, surrender to the organization (through an accountable mechanism) all cryptographic hardware tokens that were issued by or on behalf of the sponsoring organization. The token shall be zeroized or destroyed promptly upon surrender and shall be protected from malicious use between surrender and zeroization or destruction.

If a Subscriber leaves an organization and the hardware tokens cannot be obtained from the Subscriber, then all Subscriber certificates associated with the unretrieved tokens shall be revoked immediately for the reason of key compromise.

For IceCAP certificates, certificate revocation is mandatory regardless of whether the hardware token is retrieved and zeroized or destroyed.

4.9.4 Revocation Request Grace Period

There is no revocation grace period. Responsible parties must request revocation as soon as they identify the need for revocation.

4.9.5 Time within which CA must Process the Revocation Request

The CBCA and CRCA shall process all revocation requests within six hours of receipt of request.

For Entity CAs, revocation request processing time is specified below:

Assurance Level	Processing Time for Revocation Requests
All Medium Assurance including IceCAP.	Before next CRL is generated unless request is received within 2 hours of CRL generation*
High Hardware and High CBP Hardware	Within six hours of receipt of request

*Revocation requests received within two hours of CRL issuance must be processed before the following CRL is published.

4.9.6 Revocation Checking Requirements for Relying Parties

Use of revoked certificates could have damaging or catastrophic consequences in certain applications. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party and the system accreditor. If it is temporarily infeasible to obtain revocation information, then the Relying Party must either reject use of the certificate, or make an informed decision to accept the risk, responsibility, and consequences for using a certificate whose authenticity cannot be guaranteed to the standards of this policy. Such use may occasionally be necessary to meet urgent operational requirements.

4.9.7 CRL Issuance Frequency

CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below. A CA shall ensure that superseded certificate status information is removed from the PKI Repository upon posting of the latest certificate status information.

Certificate status information shall be published not later than the next scheduled update. This will facilitate the local caching of certificate status information for off-line or remote (laptop) operation. PKI participants shall coordinate with the PKI Repositories to which they post certificate status information to reduce latency between creation and availability.

The following table provides CRL issuance frequency requirements for medium-software, medium-hardware, IceCAP, medium-CBP-software, and medium-CBP-hardware assurance certificates.

	CRL Issuance Frequency
Routine	CAs that are offline and do not issue end-entity certificates except for internal operations must issue CRLs at least monthly; At least once every 24 hours for all others
Loss or Compromise of Private Key	Within 18 Hours of Notification
CA Compromise	Immediately, but no later than 18 hours after notification

The following table provides CRL issuance frequency requirements for the high-hardware and high-CBP-hardware assurance certificates.

	CRL Issuance Frequency
Routine	At least monthly for Off-line CAs; At Least Once every 24 hours for all others
Loss or Compromise of Private Key	Within six Hours of Notification
CA Compromise	Immediately, but no later than six hours after notification

The CAs that issue routine CRLs less frequently than the requirement for Emergency CRL issuance (i.e., CRL issuance for loss or compromise of key or for compromise of CA) shall meet the requirements specified above for issuing Emergency CRLs. Such CAs shall also be required to notify the CertiPath Operational Authority upon Emergency CRL issuance. This requirement shall be included in the AGREEMENT between CertiPath and the Entity.

For off line CAs, the *nextUpdate* shall be less than or equal to *thisUpdate* plus 45 days.

For all other CAs, the *nextUpdate* shall be less than or equal to *thisUpdate* plus 168 hours.

4.9.8 Maximum Latency for CRLs

For CAs that operate online, CRLs shall be published within 4 hours of generation.

For Off-line CAs, pre-generated CRLs intended for publication more than 4 hours after generation shall be protected in a manner commensurate with the protection of the CA until publication. Existing unpublished CRLs must be securely destroyed in the event the CA revokes a certificate.

4.9.9 Online Revocation Checking Availability

In addition to CRLs, CAs and Relying Party client software may support on-line status checking. Client software using on-line status checking need not obtain or process CRLs.

If on-line revocation/status checking is supported by a CA, the latency of certificate status information distributed on-line by the CA or its delegated status responders shall meet or exceed the requirements for CRL issuance stated in 4.9.7.

For IceCAP certificates, CAs shall support on-line status checking via OCSP using the CA-delegated trust model [RFC 6960].

4.9.10 Online Revocation Checking Requirements

Relying Parties are not required to utilize OCSP. If a Relying Party relies on OCSP, it should do so in accordance with the requirements in RFC 6960.

4.9.11 Other Forms of Revocation Advertisements Available

Any alternate forms used to disseminate revocation information shall be implemented in a manner consistent with the security and latency requirements for the implementation of CRLs and on-line revocation and status checking.

4.9.12 Special Requirements Related To Key Compromise

None beyond those stipulated in Section 4.9.7.

4.9.13 Circumstances for Suspension

Suspension may be permitted for end-user certificates issued under or cross certified with the medium-hardware, medium-CBP-hardware and IceCAP-hardware policies, and for certificates issued under or cross certified with the IceCAP-cardAuth policy. Examples of circumstances when suspension may be used are: 1) the discretion of the certificate issuer; 2) the user's token is temporarily unavailable; 3) authority to use the token has been temporarily suspended; 4) token possession is unknown.

4.9.14 Who can Request Suspension

A human Subscriber, human supervisor of a human Subscriber, HR person for the human Subscriber, issuing CA, or RA may request suspension of a certificate.

4.9.15 Procedure for Suspension Request

A request to suspend a certificate shall identify the certificate to be suspended, identify the requestor, explain the reason for suspension, and allow the request and requestor to be authenticated (e.g., digitally or manually signed).

All suspended certificates shall be included on the organization's CRL until they are restored, or they expire. The reason code CRL entry extension shall be populated with "certificateHold".

4.9.16 Limits on Suspension Period

The Entity PKI shall specify the maximum time period a certificate may be suspended. The CPS shall describe in detail how this maximum suspension period is enforced. If the Subscriber has not removed the certificate from hold (suspension) within that period, the certificate shall be revoked for reason of "Key Compromise".

In order to mitigate the threat of unauthorized person removing the certificate from hold, the subscriber identity shall be authenticated in person using initial identity proofing process described in Section 3.2.3 or using the Human Subscriber Re-Authentication process described in Section 3.2.3.3.

If a certificate is suspended for a period greater than 30 days, an authorizing official must verify the need for restoring the credential to the individual. Certificates that have expired or otherwise been revoked for other reasons shall not be restored.

4.10 Certificate Status Services

CAs or Enterprises are not required to support additional certificate status services.

4.10.1 Operational Characteristics

Where applicable, this must be described in the CPS.

4.10.2 Service Availability

Where applicable, this must be described in the CPS.

4.10.3 Optional Features

Where applicable, this must be described in the CPS.

4.11 End Of Subscription

For certificates that have expired prior to or upon end of subscription, revocation is not required. Unexpired CA certificates shall always be revoked at the end of the subscription.

4.12 Key Escrow and Recovery

The CBCA does not support key escrow and recovery.

Entity CAs that issue key management key (encryption) subscriber certificates are required to escrow the private decryption keys.

Escrowed keys should be maintained within the KED for a period of time that satisfies organizational and regulatory requirements, in no case shall the period of retention be less than one year after the expiration of the associated public key certificate.

Subscribers shall be notified that their private decryption keys are escrowed.

4.12.1 Key Escrow and Recovery Policy and Practices

Under no circumstances shall a CA or end user private signature key be escrowed.

Key Recovery practices for private decryption keys must satisfy the privacy and security requirements for the CAs that issue and manage the corresponding key management public key certificates.

4.12.1.1 Key Escrow Process and Responsibilities

Escrowed keys shall be transmitted to and stored in a KED for which the protection mechanisms provide a level of security equal to or greater than that at which the private decryption keys are generated, delivered to and protected by the Subscriber.

KRAs and KROs shall not disclose or allow to be disclosed escrowed keys or escrowed key-related information to any third party unless authorized by this CP; required by law, government rule, or regulation; by the Subscriber's Organization/Enterprise policy; or by order of a court of competent jurisdiction.

4.12.1.2 Key Recovery Process and Responsibilities

Subscribers may request recovery of their own escrowed keys. Key recovery may also be requested by the personnel permitted by the Subscriber's organization policy to

recover subscriber keys and by authorized law enforcement personnel with a court order from a competent court.

Requestor identity authentication shall be commensurate with the assurance level of the certificate associated with the key being recovered.

Entities may implement automated self-recovery for Subscribers seeking the recovery of their own escrowed keys. In all other cases, key recovery requires a KRA or KRO to validate the identity and authenticate the authority of the requestor to request the key recovery.

If Requestor authentication and authorization verification is delegated to a KRO, the KRO must hold a Medium Assurance Hardware certificate issued by the organization that maintains the KRS. The KRO shall provide proof of identity and authorization to the KRA as part of the key recovery request. KRAs shall authenticate the identity of the KRO before accepting and processing a request for key recovery. If the requestor digital signature is available, KRAs shall also authenticate the identity of the requestor, i.e., when the requestor makes an electronic request that is digitally signed, the KRO shall forward the requestor digital signature in a form verifiable by the KRA. In addition, KRAs may request additional information or verification from the KROs if deemed necessary.

When a KRA or KRO initiates a key recovery request for a Requestor, the requestor is generally a third-party, but this CP does not preclude the Subscriber from seeking the assistance of a KRA or KRO to recover the Subscriber's private key.

With the exception of self-recovery, the following requirements apply to key recovery:

- A Subscriber's escrowed keys shall be recovered only upon receipt of a request from an authorized requestor.
- The identity of any requestor seeking a key recovery shall be validated. The process for validating the identity shall be the same as the one used for identity proofing as defined in Section 3.2.3 or 3.2.3.1.
- A digital signature may be accepted as proof of identity provided the associated certificate is issued by the organization that controls the KRS, the certificate has not expired, is not revoked, and is for the same or greater assurance level than the certificate associated with the key in the recovery request. In addition, the requestor's authorization to recover the specific keys in this request shall be verified.
- If a KRO performs the requestor authentication and authorization validation, the KRO sends the key recovery request to the KRA.
- The KRAs shall verify the request and perform the key recovery in a manner that ensures that at no point during the recovery process shall a single individual control both the recovered key and the decryption material.

  Notwithstanding the above, if recovery is performed by a KRA in support of a forensic investigation, that KRA may control both the recovered key and the decryption material.
- The recovered key and information required to decrypt the key are provided to the Requestor by separate channels. If the Requestor retrieves the recovered key in person, one KRA shall deliver the encrypted recovered key, while the other KRA shall deliver the information required to decrypt the key. For electronic retrieval, the recovered key is sent via protected channel and in encrypted form to the Requestor. Information required to decrypt the recovered

key is provided to the Requestor by a separate channel. The Requestor shall acknowledge receipt of the recovered key.

- KROs and KRAs shall protect all information regarding all occurrences of key recovery. They shall not communicate any information concerning a key recovery to the Subscriber except when the Subscriber is the requestor.
- Records of all recovery requests and their disposition shall be retained, including acknowledgement of receipt by the requestor. The audit records shall not contain Subscribers' keys in any form: plaintext, split, encrypted, etc.

During delivery, recovered keys shall be protected against disclosure to any party except the requestor in a manner commensurate with the level of assurance of the associated certificate.

4.12.1.2.1 Third-party Requestors Identity Proofing and Authentication

Entities shall determine how third-party requests for recovery of decryption keys are managed. For example, the external third-party requestor may be required to establish its identity to an authorized organizational representative who will then act as an internal third-party requestor for the recovery of the requested decryption key.

The internal third-party requestor shall establish its identity to the KRA or KRO using one of the following methods:

- In-person using the process described in Section 3.2.3.1; or
- On the basis of an electronically authenticated request using a valid signature or authentication private key and associated certificate issued by the organization that owns the KRS at an assurance level equal to or higher than the certificate associated with the escrowed key to be recovered.

The antecedent process shall not be used. The authority of the requestor to recover the requested key shall be verified prior to initiating the key recovery request, in consultation with Organization/Enterprise management and/or legal counsel, as appropriate.

Practice Note:
Organizations are advised to determine internal notification requirements for External Third-Party key recovery requests and provide a provision for situations where the law requires the KED to release a Subscriber's private decryption key without organizational notification.

4.12.1.2.2 Subscribers Identity Proofing and Authentication

With the exception of automated self-recovery, Subscribers shall establish their identities to the KRA or the KRO prior to initiation of the key recovery request using one of the following processes:

- In-person using the process described in Section 3.2.3.1; or
- On the basis of an electronically authenticated request using a valid signature or authentication private key and associated certificate issued by the organization that owns the KRS at an assurance level equal to or higher than the certificate associated with the escrowed key to be recovered.

For automated self-recovery, the Subscriber must be authenticated to the KED using a valid authentication private key and associated certificate issued by the organization that owns the KRS. The certificate policy assurance level of the authentication certificate

shall be equal to or greater than that of the certificate associated with the private key being recovered.

4.12.1.2.3 KRA and KRO Authentication

The KRA shall authenticate to the KED directly using a public key certificate issued by the organization that owns the KRS. The assurance level of the certificate shall be the same as or greater than that of the certificate whose associated private key is being recovered.

The KRO shall authenticate to the KRA using a public key certificate issued by the organization that owns the KRS. The assurance level of the certificate shall be the same as or greater than that of the certificate whose associated private key is being recovered. The KRA shall verify that the KRO is authorized to request recovery of keys associated with the identified Subscriber.

4.12.1.2.4 DDS Authentication

The Data Decryption Server (DDS) shall authenticate to the KED directly using a public key certificate issued by the organization that owns the KRS. The assurance level of the certificate shall be the same as or greater than that of the highest-level encryption certificates associated with the private decryption keys escrowed in the KED.

The KED shall verify that the DDS is authorized to obtain the keys for the claimed subscriber community.

4.12.1.2.5 Operational Requirements

For organizations that permit Subscribers to recover their own escrowed keys, a process for automated self-recovery may be implemented (see Section 4.12.1.2.5.3). Otherwise, where Subscriber key recovery is permitted, Subscribers may request recovery of their own escrowed keys from the KRA or KRO. Subscriber identity verification shall be performed in accordance with Section 4.12.1.2.2.

Internal third-party requestors shall submit key recovery requests to the KRA or KRO. Identity verification of the third-party requestor shall be performed in accordance with Section 4.12.1.2.1. The third-party requestor shall provide proof of authority to recover the subject key. Such proof of authority shall be verified by the KRA or KRO.

A DDS shall use electronic means to request subscribers' escrowed keys. Requests shall be authenticated using a process at least as strong as the key being recovered. See Section 4.12.1.2.4.

In all cases, recovered keys must be protected against disclosure to any party except the requestor during transport and delivery.

4.12.1.2.5.1 KRS Operational Security

Communications between and among the KED, KRAs, KROs, DDS, and Requestors shall be secure from protocol threats such as disclosure, modification, replay, and substitution. The strength of all cryptographic protocols shall be equal to or greater than that of the keys they protect.

When any mechanism that includes a shared secret (e.g., a password) is used to protect the key in transit, the mechanism shall ensure that the recipient and the transmitting party are the only holders of this shared secret.

4.12.1.2.5.2 Key Recovery through KRA

The KRA shall provide access to a copy of an escrowed key only in response to a properly authenticated and authorized key recovery request. Such access shall require the actions of at least two KRAs. All copies of escrowed keys shall be protected continuously using two-person control procedures during recovery and delivery to the authenticated and authorized requestor. Split key or password procedures are considered adequate two person controls.

The delivery mechanism for copies of recovered keys shall provide cryptographic protection against disclosure with an assurance equal to or greater than the assurance level of the certificates associated with the escrowed keys.

Notwithstanding the above, if recovery is performed by a KRA in support of a forensic investigation, that KRA may control both the recovered key and the decryption material.

4.12.1.2.5.3 Automated Self-Recovery

A current Subscriber's escrowed keys may be provided directly to that Subscriber using automated self-recovery without imposition of two-person control requirements.

The delivery mechanism for copies of self-recovered keys shall provide cryptographic protection against disclosure with an assurance level equal to or greater than the certificates associated with the escrowed keys.

The KED shall provide self-recovery of escrowed keys to current Subscribers only after:

- Verifying that the authenticated identity of the requestor is the same as the Subscriber associated with the escrowed keys being requested.
- Attempting to notify the Subscriber of all attempts (successful or unsuccessful) to use the automated self-recovery process to recover the Subscriber's escrowed keys. If the KED does not have information (e.g., an email address) necessary to attempt to notify the Subscriber of a key recovery request, then the KED shall not provide the Subscriber with the requested key material using the automated recovery process.
- Ensuring that the recovered keys are being sent only to the authenticated Subscriber associated with the escrowed keys; and
- Ensuring that the recovered keys are encrypted during transmission using cryptography of equal or greater strength than provided by the escrowed keys.

When self-recovery involves delivering the escrowed key directly to the subscriber's hardware token, the KED shall use a secure means (e.g., Global Platform Secure Channel Protocol, Mini-driver API, etc.) to inject the private key onto the hardware token directly. Once injected, the recovered key shall not be exportable from the hardware token.

4.12.1.2.5.4 Recovery by DDS

An escrowed key may be provided directly to the DDS provided the DDS is operated under continuous two-person control. The KED shall perform the following prior to releasing the key:

- Authenticate the requestor as a legitimate DDS.
- Verify that the DDS is authorized to recover the escrowed key for the Enterprise to which the key belongs.

- Ensure that the escrowed keys are protected during transmission using cryptography or other means of equal or greater strength than those provided by the escrowed keys.

A combination of physical, procedural, and technical security controls shall be used to enforce continuous two-person control on the DDS. Where feasible, the DDS shall be designed to use technical means to enforce two-person controls rather than physical or procedural means.

Practice Note:
The DDS is considered under continuous two-person control when any human action performed on the DDS requires two persons.

4.12.1.2.5.5 Key Recovery During Token Issuance

Escrowed keys may be recovered in order to populate a token's key history during new certificate or new hardware token issuance. In this case, the KED shall use a secure means (e.g., Global Platform Secure Channel Protocol, Mini-driver API, etc.) to inject the key history onto the hardware token directly. Once injected, the recovered keys shall not be exportable from the hardware token.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

This CP neither requires nor prohibits the Entity PKI having the capability to recover session keys. If session keys are recoverable, the policy requirements shall be described here, and the practices captured in the corresponding CPS (or KRPS).

5 FACILITY MANAGEMENT & OPERATIONAL CONTROLS

5.1 Physical Controls

5.1.1 Site Location & Construction

The location and construction of the facility housing CA, KED, DDS, and CMS equipment 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 and intrusion sensors, shall provide robust protection against unauthorized access to the CA equipment and records.

Administration Workstations used to administer CA, KED, DDS, CSA and/or CMS equipment shall adhere to the requirements identified below except where specifically noted.

5.1.2 Physical Access

5.1.2.1 CA Physical Access

CA, KED, DDS, CSA, and CMS equipment, including any Administration Workstations, shall always be protected from unauthorized access. The physical security requirements pertaining to CA, KED, DDS, CSA, and CMS equipment, including any Administration Workstations are:

- Ensure no unauthorized access to the hardware is permitted.
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers.
- Ensure manual or electronic monitoring for unauthorized intrusion at all times.
- Ensure an access log is maintained and inspected periodically.
- Provide at least three layers of increasing security such as perimeter, building, and CA room.
- Require two-person physical access control to both the cryptographic module and computer system.

Removable cryptographic modules shall be deactivated prior to storage. When not in use, removable cryptographic modules and the activation information used to access or enable cryptographic modules shall be placed in secure containers. Activation data shall either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module and shall not be stored with the cryptographic module or any removable hardware associated with Administration Workstations.

A security check of the facility housing the CA, KED, DDS, CSA, or CMS equipment or Administration Workstation shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when “open”, and secured when “closed”);
- For off-line systems, all equipment other than the PKI Repository is shut down);
- Any security containers are properly secured;
- Physical security systems (e.g., door locks, vent covers) are functioning properly; and
- The area is secured against unauthorized access.

A person or group of people shall be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.2.2 RA and KRA, Equipment Physical Access

RA and Key Recovery Workstations shall be protected from unauthorized access while the cryptographic module is installed and activated. The RA and KRA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the RA and KRA equipment environment.

5.1.3 Power and Air Conditioning

CAs shall have backup power sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. PKI Repositories shall be provided with Uninterrupted Power sufficient for a minimum of six hours operation in the absence of commercial power, to support continuity of operations.

5.1.4 Water Exposures

CA, KED, DDS, CSA, CMS, RA,KRA, and Administration Workstation equipment shall be installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors).

Water exposure from fire prevention and protection measures (e.g. sprinkler systems) are excluded from this requirement.

5.1.5 Fire Prevention & Protection

CA, KED, DDS, CSA, CMS, RA, KRA, and Administration Workstation equipment shall be installed such that the possibility of fire is minimized. Operational environment shall be equipped with temperature and smoke detectors, alarms, and a fire suppression system appropriate for computer equipment. Operating material (e.g., software, keys) shall be stored such that they are protected from fire.

5.1.6 Media Storage

CA and KRS media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic), theft, and unauthorized access. Media that contains audit, archive, or backup information shall be duplicated and stored in a location separate from the CA location.

5.1.7 Waste Disposal

Sensitive waste material shall be disposed of in a secure fashion.

5.1.8 Off-Site backup

Full system backups of the CAs, sufficient to recover from system failure, shall be made on a periodic schedule, described in the respective CPS. Backups shall be performed and stored off-site not less than once every 7 days, unless the CA is off-line, in which case, it shall be backed up whenever it is activated or every 7 days, whichever is later. At least one full backup copy shall be stored at an offsite location (at a location separate from the CA equipment). Only the latest full backup need be retained. The backup shall

be stored at a site with physical and procedural controls commensurate with that of the operational CA.

5.2 Procedural Controls

5.2.1 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. The people selected to fill these roles must be extraordinarily responsible or the integrity of the CA and associated KRS is weakened. The functions performed in these roles form the basis of trust for all uses of the CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

The requirements of this policy are drawn in terms of four roles (Note: the information derives from the Certificate Issuing and Management Components (CIMC) Protection Profile):

1. *Administrator* – authorized to install, configure, and maintain the CA and KRS; establish and maintain user accounts; configure profiles and audit parameters; and generate component keys.
2. *Officer* – authorized to request or approve certificate issuance, certificate revocation, and key recovery.
3. *Audit Administrator* – authorized to view and maintain audit logs.
4. *Operator* – authorized to perform system backup and recovery.

The following sections define these and other trusted roles.

5.2.1.1 Administrator

The Administrator shall be responsible for:

- Installation, configuration, and maintenance of the CA and KRS;
- Establishing and maintaining CA system accounts;
- Configuring certificate profiles or templates and audit parameters, and;
- Generating and backing up CA keys.

Administrators shall not issue certificates to Subscribers.

5.2.1.2 Officer

The Officer shall be responsible for issuing certificates, that is:

- Registering new Subscribers and requesting the issuance of certificates;
- Verifying the identity of Subscribers and accuracy of information included in certificates;
- Approving and executing the issuance of certificates, and;
- Requesting, approving and executing the revocation of certificates.

5.2.1.3 Audit Administrator

The Audit Administrator shall be responsible for:

- Reviewing, maintaining, and archiving audit logs;
- Performing or overseeing internal compliance audits to ensure that the CA and KRS are operating in accordance with their CPS/KRPS, as appropriate;

5.2.1.4 Operator

The operator shall be responsible for the routine operation of the CA and KRS equipment and operations such as system backups and recovery or changing recording media.

5.2.1.5 Registration Authority

An RA's responsibilities are:

- Verifying identity, pursuant to section 3.2;
- Entering Subscriber information, and verifying correctness;
- Securely communicating requests to and responses from the CA;
- Receiving and distributing Subscriber certificates.

The RA role is highly dependent on public key infrastructure implementations and local requirements. The responsibilities and controls for RAs shall be explicitly described in the CPS of a CA if the CA uses an RA.

5.2.1.6 Key Recovery Agent

The KRA shall be responsible for:

- Verifying a requestor's identity and authorization;
- Enabling (i.e., initiating or approving) the recovery of copies of escrowed keys;
- Distributing copies of recovered escrowed keys to requestors, with appropriate protection.

Note: Organizations may choose to utilize KROs to perform requestor identity and authorization verification on behalf of the KRA. In such cases, the KRAs shall be responsible for monitoring KRO activity.

The individuals assigned to the CA Officer or RA trusted role also may be assigned to the KRA trusted role.

5.2.1.7 CSA Roles

A CSA shall require at least the following roles.

- The CSA administrator shall be responsible for:
  - Installation, configuration, and maintenance of the CSA;
  - Establishing and maintaining CSA system accounts;
  - Configuring CSA application and audit parameters; and
  - Generating and backing up CSA keys.
- The CSA Audit Administrator shall be responsible for:
  - Reviewing, maintaining, and archiving audit logs; and
  - Performing or overseeing internal compliance audits to ensure that the CSA is operating in accordance with its CPS.
- The CSA Operator shall be responsible for:
  - The routine operation of the CSA equipment; and
  - Operations such as system backups and recovery or changing recording media.

The individuals assigned to CA trusted roles also may be assigned to the corresponding CSA trusted roles identified above (i.e., A CA Administrator may also fulfil the CSA

Administrator role, a CA Audit Administrator may also fulfil the CSA Audit Administrator role).

5.2.1.8 CMS Roles

A CMS shall have at least the following roles.

- The CMS administrator shall be responsible for:
  - Installation, configuration, and maintenance of the CMS;
  - Establishing and maintaining CMS accounts;
  - Configuring CMS application and audit parameters; and
  - Generating and backing up CMS keys.
- The CMS Audit Administrator shall be responsible for:
  - Reviewing, maintaining, and archiving audit logs; and
  - Performing or overseeing internal compliance audits to ensure that the CMS is operating in accordance with its CPS.
- The CMS Operator shall be responsible for:
  - The routine operation of the CMS equipment; and
  - Operations such as system backups and recovery or changing recording media.

The individuals assigned to CA trusted roles also may be assigned to the corresponding CMS trusted roles identified above (i.e., A CA Administrator may also fulfil the CMS Administrator role, a CA Audit Administrator may also fulfil the CMS Audit Administrator role).

5.2.2 Number of Persons Required per Task

Two or more persons shall be required to perform the following tasks:

- CA, KED, DDS, CSA, and IceCAP Content Signing key generation;
- CA, KED, DDS, CSA, and IceCAP Content Signing key activation;
- CA, KED, DDS, CSA, and IceCAP Content Signing key backup.

Where multiparty control is required, at least one of the participants shall be an Administrator. All participants shall serve in a trusted role as defined in Section 5.2.1.

Multiparty control shall not be achieved using personnel that serve in the Audit Administrator Role.

In addition to the above, with the exception of subscriber self-recovery (where implemented), two or more KRAs are required to recover an escrowed key.

It is recommended that multiple persons are assigned to all roles in order to support continuity of operations.

5.2.3 Identification and Authentication for Each Role

An individual in a trusted role shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

An individual in a trusted role shall authenticate to remote components of the PKI using a method commensurate with the strength of the PKI. Two factor (or better) access control, where at least one factor is a hardware token, shall be used for log in to the Administration Workstation. In addition, the hardware token used must be acceptable for the highest certificate policy OID supported by the associated CA. Also See Section 6.7 for authentication to the PKI enclave.

All Trusted Roles who operate a CMS shall be allowed access only when authenticated using a method commensurate with IceCAP-hardware requirements.

5.2.4 Roles Requiring Separation of Duties

Role separation, when required as set forth below, may be enforced either by the CA equipment, or procedurally, or by both means.

Individual CA, CSA, and CMS personnel shall be specifically designated to the four roles defined in Section 5.2.1 above as applicable. Individuals may assume more than one role, except:

- Individuals who assume an Officer role may not assume an Administrator or Audit Administrator role;
- Individuals who assume an Audit Administrator role shall not assume any other role; and
- Under no circumstances shall any of the four roles perform its own compliance auditor function.

In addition, KRAs and KROs are limited to the recovery of escrowed keys. KRAs and KROs shall not perform any of the trusted role duties associated with the installation, initial set up, configuration and ongoing maintenance of the KED, including audit log review.

No individual in a trusted role shall be assigned more than one identity.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

A group of individuals responsible and accountable for the operation of each CA, KRS, CMS, and CSA shall be identified and assigned to trusted roles per Section 5.2.1.

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to a background investigation. Personnel appointed to trusted roles (including CA trusted roles, KRS trusted roles, CMS trusted roles, CSA trusted roles, and RA role) shall:

- Have a favorable outcome from the background investigation.
- Have successfully completed an appropriate training program.
- Have demonstrated the ability to perform their duties.
- Have no other duties that would interfere or conflict with their duties for the trusted role.
- Be appointed in writing by an approving authority.

In addition, the person filling the trusted role shall not knowingly:

- Have been previously relieved of duties resulting from violation of trust (e.g. willful mishandling of information or willful mis-issuance of a certificate).
- Have had a security clearance revoked for reasons other than routine review and renewal decisions.
- Have been denied a security clearance, the cause for which has not been resolved and a security clearance subsequently granted.

- Have been criminally convicted as legally reportable (e.g. felony offense).

Practice Note:
In order to make the determination if a person was denied clearance or had clearance revoked for cause, it is sufficient to rely on the local Facility Security Officer database, Joint Personnel Adjudication System (JPAS), and assertions by the person on security clearance forms.

For PKIs operated at medium-software, medium-hardware, and/or high-hardware, each person filling a trusted role shall satisfy at least one of the following requirements:

- The person shall be a citizen of the country where the CA is located; or
- For PKIs operated on behalf of multinational governmental organizations, the person shall be a citizen of one of the member countries; or
- For PKIs located within the European Union, the person shall be a citizen of one of the member states of the European Union; or
- The person shall have a security clearance equivalent to U.S. Secret or higher issued by a NATO member nation or major non-NATO ally as defined by the International Traffic in Arms Regulation (ITAR) – 22 CFR 120.32.

For RAs and personnel appointed to the trusted roles for the CSAs, in addition to the above, the person may be a citizen of the country where the function is located.

For PKIs operated at any of the Commercial Best Practice (CBP) assurance levels, there is no citizenship requirement or security clearance specified.

5.3.2 Background Check Procedures

All persons filling trusted roles (including CA trusted roles, KRS trusted roles, CMS trusted roles, CSA trusted roles, and RA role), shall have completed a favorable background investigation. The scope of the investigation shall include checking the following areas covering the past five years:

- Employment[9];
- Education (Regardless of the date of award, the highest educational degree shall be verified);
- Place of residence (past 3 years);
- Law Enforcement; and
- References

Adjudication of the background investigation shall be performed by a competent adjudication authority using a process consistent with United States Executive Order 12968 August 1995, or equivalent.

The results of these checks shall not be released except as required in Sections 9.3 and 9.4.

Background check procedures shall be described in the CPS.

A favorable national agency check or security clearance that is based on a five year background investigation meets the requirements of this section. For example, a successfully adjudicated United States National Agency Check with Written Inquires (NACI) or United States National Agency Check with Law Enforcement Check (NACLC) on record is deemed to have met the requirements of this section, as is a security

---

[9] If the person has been in the work-force for less than five years, the employment verification shall consist of the periods during which the person has been in the work-force.

clearance equivalent to U.S. Secret or higher issued by a NATO member nation or major non-NATO ally as defined by ITAR – 22 CFR 120.32.

If a formal clearance or other check is the basis for background check, the background refresh shall be in accordance with the corresponding formal clearance or other check. Otherwise, the background check shall be refreshed every ten years.

Practice Note especially for our International customers:
The qualifications of the adjudication authority and procedures utilized to satisfy these requirements must be demonstrated before cross certification with the CBCA.

Practice Note:
Interim clearance may be acceptable. However, if the final adjudication is not favorable, all certificates issued while the person had a trusted role may require re-evaluation and possibly revocation.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of a CA, KRS, CMS, CSA or a RA shall receive comprehensive training. Training shall be conducted in the following areas:

- CA/KRS/CMS/CSA/RA security principles and mechanisms;
- All PKI software versions in use on the CA and KRS system, including the DDS;
- All PKI duties they are expected to perform;
- Disaster recovery and business continuity procedures.
- Stipulations of the applicable CP and CPS

In addition, KRAs and KROs shall be trained in the organizational policy relating to release of recovered escrowed keys and the information associated with such a recovery.

A record of the training completed for each individual shall be maintained by the organization administering the CA.

5.3.4 Retraining Frequency and Requirements

All personnel performing duties with respect to the operation of a CA, KED, DDS, CMS, CSA, RA, KRA, or a KRO shall be aware of changes in the CA, KED, DDS, CMS, CSA, RA, KRA, or KRO operations, as applicable. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are CA or KED software or hardware upgrade, RA or KRA software upgrades, changes in automated security systems, and relocation of equipment.

5.3.5 Job Rotation Frequency and Sequence

Job rotation is optional. Any job rotation shall ensure the following:

- Role separation requirements are not violated.
- The continuity and integrity of the CA and KRS services are not affected.
- All access rights associated with the previous role(s) are terminated.
- A record of each role change is maintained by the organization administering the CA.
- Individuals assuming an auditor role do not audit their own work from a previous role.

5.3.6 Sanctions for Unauthorized Actions

The CPMA or Entity PMA shall take appropriate administrative and disciplinary actions against personnel who violate the applicable certificate policy.

5.3.7 Independent Contractor Requirements

Contractor personnel employed to perform functions pertaining to CA, KED, DDS, CSA, CMS, RA, KRA or KRO operations shall meet applicable requirements set forth in the associated CP (e.g., all requirements of Section 5.3).

5.3.8 Documentation Supplied To Personnel

The CP, CPS, and any relevant complementary documents, such as statutes, policies, and contracts, shall be made available to all trusted role personnel. Other technical, operations, and administrative documents (e.g., Administrator Manual, User Manual, etc.) shall be provided in order for the trusted personnel to perform their duties.

5.4 Audit Logging Procedures

Audit log files shall be generated for all events relating to the security of the CAs, KED, CMS, CSAs, RAs, KRAs, and Administration Workstations. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used.

All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with Section 5.4.3.

A statistically significant sample of security audit data since the last review shall be examined to include a reasonable search for any evidence of malicious activity. Where possible, audit record reviews should be performed using an automated process. Such reviews involve verifying that the log has not been tampered with, there is no discontinuity or other loss of audit data, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs.

A statistically significant sample of KED audit records pertaining to successful key recoveries shall be reconciled against the KRA audit logs and self-recovery requests. All KED audit records of unsuccessful key recoveries shall be analyzed to determine the cause and to ensure that the Key Escrow and Recovery system is operating correctly and securely.

In addition, the event log of the Administration Workstation shall be reconciled with the event log of the corresponding CA, KED, DDS, CMS, or CSA.

The Audit Administrator shall explain all significant events in an audit log summary. Actions taken as a result of these reviews shall be documented.

5.4.1 Types of Events Recorded

All security auditing capabilities of the CA, KED, DDS, CMS, CSA, Administration Workstations (AW), RA and KRA operating systems and the CA, KED, DDS, CMS, CSA, RA and KRA applications required by this CP shall be enabled during installation and remain enabled during operation. As a result, most of the events identified in the table shall be automatically recorded. 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,

- Location of the event (system affected or physical location),
- Source of the event,
- Success or failure where appropriate,
- The identity of any entity, object and/or operator associated with the event.

Any request or action requiring the use of a private key controlled by the CA or KED is an auditable event. If out-of-band processes are used for authorization of certificate issuance or key recovery, external artifacts from the process (e.g. forms, emails, etc.) must be recorded.

The assignment of an individual to a trusted role and removal of an individual from a trusted role are auditable events and shall include the name of the authorizing official.

In addition, and where applicable, KRAs shall monitor KRO activity for patterns of potentially anomalous behavior and initiate inquiries or investigations as appropriate.

The following events shall be audited:

Note: If one or more of the events listed is not applicable to a particular implementation of a PKI component, those non-applicable events need not be audited.

Auditable Event	CA	KED	CSA	KRA	RA	DDS	CMS	AW
SECURITY AUDIT								
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	X	X	X	X	X	X	X	X
Any attempt to delete or modify the Audit logs	X	X	X	X	X	X	X	X
IDENTITY-PROOFING								
Platform or CA application-level authentication attempts	X	X	X	X	X	X	X	X
The value of *maximum number of authentication attempts* is changed	X	X	X	X	X	X	X	X
The number of unsuccessful authentication attempts exceeds the *maximum authentication attempts* during user login	X	X	X	X	X	X	X	X
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	X	X	X	X	X	X	X	X
An Administrator changes the type of authenticator, e.g., from a password to a biometric	X	X	X	X	X	X	X	X
DATA ENTRY AND OUTPUT								
Any additional event that is relevant to the security of the CA or KRS (e.g., remote or local data entry or data export) must be documented	X	X	X	X	X	X	X	X
KEY GENERATION								

Auditable Event	CA	KED	CSA	KRA	RA	DDS	CMS	AW
Whenever the Component generates a key (not mandatory for single session or one-time use symmetric keys)	X	X	X	N/A	X	X	X	X
PRIVATE KEY LOAD AND STORAGE								
The loading of Component private keys	X	X	X	X	X	X	X	X
Receipt of keys for escrow and posting of these keys to the KED		X	-		-	-	X	
All access to certificate subject Private Keys retained for key recovery purposes	X	X	N/A	X	N/A	X	X	N/A
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE								
All changes to the trusted Component Public Keys, including additions and deletions	X	X	X	X	X	X	X	X
PRIVATE AND SECRET KEY EXPORT								
The export of private and secret keys (keys used for a single session or message are excluded)	X	X	X	X	X	X	X	X
CERTIFICATE REGISTRATION								
All records related to certificate request authorization, approval and signature	X	N/A	N/A	N/A	X	N/A	X	N/A
CERTIFICATE REVOCATION								
All records related to certificate revocation request authorization, approval and execution	X	N/A	N/A	N/A	X	N/A	X	N/A
CERTIFICATE STATUS CHANGE APPROVAL								
All records related to certificate status change request authorization, approval and execution	X	N/A	N/A	N/A	N/A	N/A	X	N/A
PKI COMPONENT CONFIGURATION								
Any security-relevant changes to the configuration of the Component	X	X	X	X	X	X	X	X
ACCOUNT ADMINISTRATION								
Roles and users are added or deleted	X	X	X	X	X	X	X	X
The access control privileges of a user account or a role are modified	X	X	X	X	X	X	X	X
CERTIFICATE PROFILE MANAGEMENT								
All changes to the certificate profile	X	N/A	N/A	N/A	N/A	N/A	X	N/A
CERTIFICATE STATUS AUTHORITY MANAGEMENT								
All changes to the CSA profile (e.g. OCSP profile)	N/A	N/A	X	N/A	N/A	N/A	N/A	N/A

Auditable Event	CA	KED	CSA	KRA	RA	DDS	CMS	AW
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT								
All changes to the certificate revocation list profile	X	N/A	N/A	N/A	N/A	N/A	N/A	N/A
MISCELLANEOUS								
Appointment of an individual to or removal from a Trusted Role	X	X	X	X	X	X	X	X
Designation of personnel for multiparty control	X	X	-	X	N/A	X	X	X
Installation of the Operating System	X	X	X	X	X	X	X	X
Installation of the PKI Application	X	X	X	X	X	X	X	N/A
Installation of hardware cryptographic modules	X	X	X	X	X	X	X	X
Removal of hardware cryptographic modules	X	X	X	X	X	X	X	X
Destruction of cryptographic modules	X	X	X	X	X	X	X	X
System Startup	X	X	X	X	X	X	X	X
Logon attempts to PKI Application	X	X	X	X	X	X	X	X
Receipt of hardware / software	X	X	X	X	X	X	X	X
Attempts to set passwords	X	X	X	X	X	X	X	X
Attempts to modify passwords	X	X	X	X	X	X	X	X
Back up of the internal CA database	X	-	-	-	-	-	X	N/A
Restoration from back up of the internal CA database	X	-	-	-	-	-	X	N/A
Critical file manipulation (e.g., creation, renaming, moving)	X	X	-	X	-	X	-	-
Posting of any material to a PKI Repository	X	-	-	-	-	-	-	N/A
Access to the internal CA/KED database	X	X	X	X	-	X	-	N/A
All certificate compromise notification requests	X	N/A	N/A	N/A	X	X	X	N/A
Loading tokens with certificates	X	X	N/A	X	X	X	X	N/A
Shipment of tokens and receipt of Tokens from/by the component that contain key material or that allow access to key material	X	X	N/A	X	X	X	X	N/A
Any action taken (e.g., authentication, authorization, recovery, and delivery) in response to a key recovery request	-	X	-	X	X	X	X	-
Zeroizing and Destroying Tokens	X	X	N/A	X	X	X	X	N/A
Re-key of the Component	X	X	X	X	X	X	X	X

Auditable Event	CA	KED	CSA	KRA	RA	DDS	CMS	AW
CONFIGURATION CHANGES								
Hardware	X	X	X	X	-	X	X	X
Software	X	X	X	X	X	X	X	X
Operating System	X	X	X	X	X	X	X	X
Patches	X	X	X	X		X	X	X
Security Profiles	X	X	X	X	X	X	X	X
PHYSICAL ACCESS / SITE SECURITY								
Personnel Access to room housing Component	X	X	-	X	-	X	X	X
Access to the Component	X	X	X	X	-	X	X	X
Known or suspected violations of physical security	X	X	X	X	X	X	X	X
ANOMALIES								
Software error conditions	X	X	X	X	X	X	X	X
Software check integrity failures	X	X	X	X	X	X	X	X
Equipment failure	X	X	-	X	-	X	X	-
Electrical power outages	X	X	-	X	-	X	X	-
Uninterruptible Power Supply failure	X	X	-	-	-		X	-
Obvious and significant network service or access failures	X	X	-	X	-	X	X	-
Violations of Certificate Policy	X	X	X	X	X	X	X	X
Violations of Certification Practice Statement	X	X	X	X	X	X	X	X
Resetting Operating System clock	X	X	X	X	X	X	X	X

5.4.2 Frequency of Processing Audit Logs

Audit logs shall be reviewed at least monthly, unless the CA is off-line, in which case the off-line CA audit logs shall be reviewed when the system is activated or every 30 days, whichever is later.

5.4.3 Retention Period for Audit Logs

Audit logs shall be retained onsite until reviewed .

5.4.4 Protection of Audit Logs

System configuration and operational procedures shall be implemented together to ensure that:

- Only authorized people have read access to the logs;
- Only authorized people may archive audit logs; and,
- Audit logs are not modified.

For the CA, KED, DDS, CMS, CSA, and the Administration Workstations, the Audit Administrator shall be the only person managing the audit log (e.g., collect, review, backup, rotate, delete, etc.). For the RA and KRA, a System Administrator other than the RA or KRA shall be responsible for managing the audit log.

Procedures must be implemented to protect audit records from deletion or destruction . Audit logs shall be moved to a safe, secure storage location separate from the audited equipment.

It is acceptable for the system to over-write audit logs after they have been backed up and archived.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up at least once monthly, unless the CA is offline, in which case audit logs and audit summaries shall be backed up when the system is activated or every 30 days, whichever is later. A copy of the audit log shall be sent off-site in accordance with the CPS following review.

5.4.6 Audit Collection System (internal vs. external)

The audit log generation process shall be internal to the CA, KED, DDS, CMS, CSA, KRA and RA. The audit log generation process shall run automatically without human intervention.

Audit log generation processes shall be invoked at system startup and cease only at system shutdown. The audit log generation process shall receive confirmation that log records are successfully stored in the audit log collection system.

The audit log collection system may or may not be external. Audit collection systems shall be configured to ensure security audit data is protected against loss (e.g., overwriting or overflow of automated log files).

If an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, the associated operations shall be suspended until the problem is remedied.

5.4.7 Notification to Event-Causing Subject

There is no requirement to provide notice that an event was audited to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability Assessments

CAs shall perform routine vulnerability assessments of the security controls described in the applicable CP.

5.5 Records Archival

5.5.1 Types of Records Archived

CA, KED, DDS, CMS, KRA, CSA, and RA archive records shall be sufficiently detailed to establish the proper operation of the PKI or the validity of any certificate (including those revoked or expired) issued by the CA.

Note: Once the Administration Workstation logs have been reviewed and reconciled with the corresponding CA, KED, DDS, CMS, or CSA logs, they shall be retained for at least one year, further archive of the Administration Workstation logs is not required. However, the reconciliation summary shall be retained for the full archive period

prescribed for the CA archive. In addition, events external to the Administration Workstation (e.g., physical access) shall be retained for the full archive period prescribed for the CA archive.

Data To Be Archived	CA	KED	CSA	KRA	DDS	RA	CMS
Certification Practice Statement/Key Recovery Practice Statement (where applicable).	X	X	X	X	X	X	X
Certificate Policy	X	X	X	X	X	X	X
Contractual obligations	X	X	X	X	X	X	X
System and equipment configuration	X	X	X	X	X	-	X
Modifications and updates to system or configuration	X	X	X	X	X	-	X
All records related to certificate request, authorization, approval and signature	X		-	-		-	X
All records related to recovery of an escrowed key		X		X	X	X	X
All records related to certificate status changes (e.g., revocation, suspension, or restoration).	X	-	-	-		-	X
All records specific to the assignment of an individual to or removal from a trusted role.	X	X	X	X	-	X	X
All records specific to the qualification, appointment, or removal of individuals as Trusted Agents	X	-	-	-	-	X	-
Subscriber identity authentication data as per Section 3.2.3	X	X	N/A	X	-	X	X
Documentation of receipt and acceptance of certificates, including Subscriber Agreements	X		N/A	-	-	X	X
Documentation of receipt of Tokens	X	X	N/A	X	-	X	X
All certificates issued or published	X	-	N/A	-	-	N/A	X
Record of Component CA Re-key	X	X	X	X	-	X	X
All Audit Logs	X	X	X	X	X	X	X
Other data or applications to verify archive contents	X	X	X	X	X	X	X
Documentation required by compliance auditors	X	X	X	X	X	X	X
Compliance Audit Reports	X	X	X	X	X	X	X

5.5.2 Retention Period for Archive

The archive retention period for records associated with a specific CA begins at CA key generation and shall be maintained for a minimum of three (3) years following CA expiration or termination.

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site.

Alternatively, an Entity may retain data using whatever procedures have been approved by the U.S. National Archives and Records Administration or by the respective records retention policies in accordance with whatever laws apply to those entities for that

category of documents. Applications required to process the archive data shall also be maintained for the minimum retention period specified above.

5.5.3 Protection of Archive

Only authorized individuals shall be permitted to write to, modify, or delete the archive. For the CA, KED, DDS, CMS, and CSA, the authorized individuals are Audit Administrators. For the RA and KRA, authorized individuals are someone other than the RA or KRA (e.g., Information Assurance Officer). The contents of the archive shall not be released except as determined by the CPMA for the CertiPath CA, Entity PMA for the Entity CA, or as required by law. Records of individual transactions may be released upon request of any Subscribers involved in the transaction or their legally recognized agents.

Archive media shall be stored in a safe, secure storage facility separate from the PKI components (CA, KED, DDS, CMS, CSA, KRA or RA) with physical and procedural security controls equivalent or better than those of the PKI. Deletion of archive records is not permitted under any circumstances prior to the end of the required retention period.

5.5.4 Archive Backup Procedures

Backup of archive records is optional. If implemented, the CPS or a referenced document shall describe how archive records are backed up, and how the archive backups are managed.

5.5.5 Requirements for Timestamping of Records

CA and KRS archive records shall have accurate timestamps with sufficient precision such that the sequence of events can be determined.

The CPS shall describe how system clocks used for timestamping are maintained in synchrony with an authoritative time standard.

5.5.6 Archive Collection System (internal or external)

The archive collection system may be internal or external but must be identified in the applicable CPS.

5.5.7 Procedures to Obtain & Verify Archive Information

Procedures detailing how to create, verify, package, transmit, and store archive information shall be described in the applicable CPS.

5.6 Key Changeover

As a CA approaches the end of its validity period, planning should be put in place to ensure a smooth transition to a new CA, unless it is the intention of the organization to cease certificate production.

Each CA's private key shall have a validity period no greater than the period described in the table below. Prior to the end of a CA private key's signing validity period a new CA shall be established. From that time on, only the new key shall be used to sign CA and/or subscriber certificates. The older, but still valid, certificate will be available to verify old signatures until all of the certificates signed using the associated private key have also expired. The old private key shall continue to be used to sign CRLs and OCSP Responder certificates until the expiration of the CA certificate or

expiration/revocation of all certificates issued by the CA, whichever comes first, and must be protected accordingly.

The following table provides the maximum lifetimes for the private keys and certificates by certificate type.

Certificate Type	Private Key	Certificate
Self-signed Root CA	20 years	20 years
Intermediate CA	10 years	10 years
Signing CA	10 years	10 years*
Subscriber Identity or Signature	3 years	3 years
Subscriber Encryption	Unrestricted	3 years
Code Signer	3 years	8 years
IceCAP Content Signer	3 years	9 years
OCSP Responder	3 years	120 days
SCVP Server	3 years	3 years
Server	3 years	3 years

*For Intermediate and Signing CAs with at least 3072-bit key length, certificate lifetime may be extended to 13 years.

IceCAP-hardware and IceCAP-cardAuth certificate expiration shall not be later than the expiration date of the hardware token on which the certificates reside.

No CA, including a Bridge CA, shall have a private key that is valid for longer than 20 years. Cross certificates shall not be valid for more than 10 years.

CAs must not issue subscriber certificates that extend beyond the expiration date of their own certificates and public keys.

Notwithstanding the above table, in all cases the CA private key may be used to sign OCSP certificates and CRLs until the CA certificate expires.

For additional constraints on certificate life and key sizes, see Section 6.1.5.

5.7 Compromise and Disaster Recovery

Administration Workstations shall be subject to the same incident and compromise handling requirements as the components they administer, including but not limited to compromise investigation, damage assessment, and mitigation planning and implementation.

5.7.1 Incident and Compromise Handling Procedures

Each organization operating an Entity PKI shall have a formal disaster recovery plan.

If an Entity PKI detects a potential hacking attempt or other form of compromise, it shall perform an investigation in order to determine the nature and the degree of damage. If the CA, KED, DDS or CSA key is suspected of compromise, the procedures outlined in Section 5.7.3 shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the CA, KED, DDS, or CSA needs to be rebuilt, only some certificates need to be revoked, and/or the CA, KED, DDS, or CSA key needs to be declared compromised. If it is determined that an incident has occurred with the potential to affect the operations and/or security environments, CertiPath shall be notified within 24 hours of determination and provided a preliminary remediation analysis.

Once the incident has been resolved, the CA, KRS, or CMS owner shall notify CertiPath. The notification shall provide detailed measures taken to remediate the incident and include the following:

- Which CA components were affected by the incident
- The CA's interpretation of the incident
- Who is impacted by the incident
- When the incident was discovered
- A statement that the incident has been fully remediated.

The CertiPath PMA members and other cross certified entities shall be notified within 24 hours of determination if any of the following occurs:

- Suspected or detected compromise of the CBCA system;
- Physical or electronic attempts to penetrate the CBCA system;
- Denial of service attacks on a CBCA component; or
- Any incident preventing the CBCA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

CertiPath shall follow the process identified above to notify all cross-certified entities of the final incident resolution.

The CertiPath PMA members shall be notified if any of the following cases occur:

- A CA certificate revocation is planned; or
- Any incident preventing a CA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

The above measures will allow member entities to protect their interests as Relying Parties.

A CA Operational Authority shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the respective CPS.

The CMS shall have documented incident handling procedures that are approved by the head of the organization responsible for operating the CMS. If the CMS or CMS keys are compromised, all certificates issued to the CMS shall be revoked, if applicable. The damage caused by the CMS compromise shall be assessed and all Subscriber certificates that may have been compromised shall be revoked, and Subscribers shall be notified of such revocation. The CMS shall be re-established.

5.7.2 Computing Resources, Software, and/or Data Corruption

If a CA or CSA equipment is damaged or rendered inoperative, but the signature keys are not destroyed; the operation shall be reestablished as quickly as possible, giving priority to the ability to generate certificate status information. Before returning to operation, ensure that the system's integrity has been restored.

If a CA cannot issue a CRL prior to the time specified in the next update field of its currently valid CRL, then all CAs that have been issued certificates by the CA shall be securely[10] notified immediately. This will allow other CAs to protect their Subscribers' interests as Relying Parties.

[10] With confidentiality, source authentication, and integrity security services applied.

If the ability to revoke certificates is inoperative or damaged, the CA shall reestablish revocation capabilities as quickly as possible in accordance with procedures set forth in the respective CPS. If the CA's revocation capability cannot be established in a reasonable timeframe, the CA shall determine whether to request revocation of its certificate(s). If the CA is a Root CA, the CA shall determine whether to notify all Subscribers that use the CA as a trust anchor to delete the trust anchor.

5.7.3 Private Key Compromise Procedures

5.7.3.1 CA, CSA, and RA Private Key Compromise Procedures

If a CA's signature keys are compromised, lost, or suspected of compromise:

1. The CA shall request revocation of any certificates issued to the compromised CA immediately;
2. A new CA key pair shall be generated by the CA in accordance with procedures set forth in the applicable CPS;
3. New CA certificates shall be requested in accordance with the initial registration process described elsewhere in this CP;
4. If the CA can obtain accurate information on the certificates it has issued and that are still valid (i.e., not expired or revoked), the CA may re-issue (i.e., renew) those certificates with the *notAfter* date in the certificate remaining the same as in original certificates; and
5. If the CA is a Root CA, it shall provide the Subscribers the new trust anchor using secure means.

The CA governing body shall also investigate what caused the compromise or loss, and what measures must be taken to preclude recurrence.

If a CSA key is compromised, all certificates issued to the CSA shall be revoked, if applicable. The CSA will generate a new key pair and request new certificate(s), if applicable. If the CSA is a trust anchor, the relying parties will be provided the new trust anchor in a secure manner (so that the trust anchor integrity is maintained) to replace the compromised trust anchor.

If RA signature keys are compromised, lost, or suspected of compromise:

1. The RA certificate shall be revoked immediately;
2. A new RA key pair shall be generated in accordance with procedures set forth in the applicable CPS;
3. A new RA certificate shall be requested in accordance with the initial registration process described elsewhere in this CP;
4. All certificate registration requests approved by the RA since the date of the suspected compromise shall be reviewed to determine which are legitimate; and
5. For those certificate requests or approval whose legitimacy cannot be ascertained, the resultant certificates shall be revoked and their subjects (i.e., Subscribers) shall be notified of revocation.

5.7.3.2 KRS Private Key Compromise Procedures

In the event that a KED or DDS is compromised or is suspected to be compromised, the Entity PMA shall be notified. The Entity PMA shall be granted sufficient access to information to determine the extent of the compromise. The Entity PMA shall direct the appropriate action. This may include revocation of certificates associated with the compromised private keys stored in the KED.

If the KRA or KRO certificate is compromised, lost, or suspected of compromise:

1. The KRA or KRO certificate shall be revoked immediately;
2. A new key pair shall be generated in accordance with procedures set forth in the applicable CPS;
3. A new certificate shall be requested in accordance with the initial registration process in Section 3.2.
4. All key recovery actions undertaken by the KRA or KRO since the date of the suspected compromise shall be reviewed to determine whether the escrowed keys may have been exposed during the recovery process;
5. The certificates associated with the potentially exposed escrowed keys shall be revoked, according to procedures specified in Section 4.9.3, and the Subscriber shall be notified of the revocation.

   Note: It is recognized that this will constitute implicit notification to the Subscriber of key recovery.

5.7.4 Business Continuity Capabilities after a Disaster

In the case of a disaster whereby a CA installation is physically damaged and all copies of the CA Signing Key are destroyed as a result, the CA shall request revocation of its certificates. Further, the CA shall re-establish operations as quickly as possible by following the procedures for CA key loss or compromise detailed in Section 5.7.3 above.

5.8 CA, CMS, CSA, KED, DDS, and RA Termination

In the event CertiPath terminates the CBCA or CRCA, cross-certified entities shall be given as much advance notice as circumstances permit and attempts to provide alternative sources of interoperation shall be sought.

In the event of an Entity CA termination, the Entity responsible shall provide notice to all cross certified CAs. Prior to the termination, the CA shall request revocation of all certificates issued to it. In addition:

- The CA, CMS, CSA, KED, DDS, KRA, and RA shall archive all audit logs and other records prior to termination.
- The CA, CMS, CSA, KED, DDS, KRA, and RA shall destroy all their private keys upon termination.
- The CA, CMS, CSA,KED, DDS, KRA, and RA archive records shall be transferred to an appropriate authority such as the PMA responsible for the entity.
- 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.

Whenever possible, notification of termination shall be provided at least two weeks prior to the CA termination.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The following table provides the requirements for key pair generation for the various entities.

Entity	FIPS 140 Level	Hardware or Software	Key Storage Restricted To The Module on Which The Key Was Generated
CA	3	Hardware	Yes
KED	3	Hardware	Yes
DDS	3	Hardware	Yes
CMS	2	Hardware	Yes
RA/KRA/KRO	2	Hardware	Yes
OCSP Responder	2	Hardware	Yes
SCVP Server	2	Hardware	Yes
Code Signing	2	Hardware	Yes
Content Signing	2	Hardware	Yes
Card Authentication	2 (Section 12 also applies)	Hardware	Yes
End Entity Signature or Authentication (medium-software and medium-CBP-software)	1	Software	No Requirement
End Entity Encryption (medium-software and medium-CBP-software)	1	Software	No Requirement
End Entity Signature or Authentication (IceCAP-hardware, medium-hardware, medium-CBP-hardware, high-hardware, and high-CBP-hardware)	2 (For IceCAP-hardware, Section 12 also applies)	Hardware	Yes
End Entity Encryption (medium-hardware, medium-CBP-hardware, high-hardware, and high-CBP-hardware)	2	Hardware	No Requirement
Server (medium-software and medium-CBP-software)	1	Software	No Requirement
Server (medium-hardware, medium-CBP-hardware, high-hardware, and high-CBP-hardware)	2	Hardware	Yes

Key generation must be performed using a method validated against FIPS 140 or an equivalent international standard. Key generation events should use the configuration that was the basis of the validation (e.g., FIPS-validated modules should be operated in FIPS mode). If the required keys cannot be generated while in a validated configuration, the specific configuration and reason for use of a different method should be documented by the CA.

Random numbers for IceCAP-hardware, IceCAP-cardAuth, medium-hardware, medium-device-hardware, medium-CBP-hardware, high-hardware, and high-CBP-hardware assurance level subscriber keys shall be generated in FIPS 140 Level 2 validated hardware cryptographic modules.

When private keys are not generated on the token to be used, originally generated private keys shall be destroyed after they have been transferred to the token. This does not prohibit the key generating modules to act as the key escrow module also.

Multiparty control shall be used for CA key pair generation, as specified in Section 5.2.2.

The CA key pair generation process shall create a verifiable audit trail that the security requirements for the process were followed. The documentation of the process shall be detailed enough to show that appropriate role separation was used. The process shall be validated by an independent third party.

Activation of the CMS Master Key shall require strong authentication of Trusted Roles. Key diversification operations by the CMS shall also occur on the CMS hardware cryptographic module. The diversified keys shall only be stored in hardware cryptographic modules that support IceCAP-hardware. CMS Master Key and diversified keys shall be protected from unauthorized disclosure and distribution. Card management shall be configured such that only the authorized CMS can manage issued cards.

6.1.2 Private Key Delivery to Subscriber

A CA shall generate its own key pair and therefore does not need private key delivery.

If Subscribers generate their own key pairs, then there is no need to deliver private keys, and this section does not apply.

When CAs or RAs generate keys on behalf of the Subscriber, then the private key shall be delivered securely to the Subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases, the following requirements shall be met:

- Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key after delivery of the private signing key to the Subscriber.
- The private key shall be protected from activation, compromise, or modification during the delivery process.
- The Subscriber 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 Subscribers.
    - For hardware modules, accountability for the location and state of the module shall be maintained until the Subscriber accepts possession of it.
    - 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 being delivered. Activation data shall be delivered using a separate secure channel.

The CA or the RA shall maintain a record of the subscriber acknowledgement of receipt of the token.

6.1.3 Public Key Delivery to Certificate Issuer

Where key pairs are generated by the Subscriber or RA, the public key and the Subscriber's identity shall be delivered securely to the CA for certificate issuance. The delivery mechanism shall bind the Subscriber's verified identity to the public key. If cryptography is used to achieve this binding, it shall be at least as strong as the subscriber key pair.

6.1.4 CA Public Key Delivery to Relying Parties

The public key of a trust anchor shall be provided to the Subscribers acting as relying parties in a secure manner so that the trust anchor is not vulnerable to modification or substitution. Acceptable methods for delivery of a trust anchor include but are not limited to:

- Secure distribution of a trust anchor through secure out-of-band mechanisms; or
- Downloading a trust anchor from a web site secured with a currently valid certificate and subsequent comparison of the hash of the certificate against a hash value made available via authenticated out-of-band sources (note that fingerprints or hashes posted in-band along with the certificate are not acceptable as an authentication mechanism).

Systems using high-hardware and high-CBP-hardware assurance certificates shall store Trust Anchor Certificates such that unauthorized alteration or replacement is readily detectable.

6.1.5 Key Sizes

If CertiPath or the CPMA determines that the security of a particular algorithm may be compromised**,** it may require the CAs to revoke the affected certificates.

All public keys placed in newly generated certificates (including self-signed certificates) and uses of public key cryptography by PKI components for signature and/or key agreement/encryption operations shall use the following algorithm suites for the time periods indicated:

	Public Key Algorithm	**Sunset Date**
Signature	2048-bit RSA, 256 bit ECDSA in prime field, or 283 bit ECDSA in binary field	12/31/2030
	3072- or 4096-bit RSA, 256-bit ECDSA in prime field, or 283 bit ECDSA in binary field	No stipulation
Encryption	2048-bit RSA, 256 bit ECDH in prime field, or 283 bit ECDH in binary field	12/31/2030

	Public Key Algorithm	Sunset Date
	3072- or 4096-bit RSA, 256-bit ECDH in prime field, or 283 bit ECDH in binary field	No stipulation

All data encryption (including network protocols) used by or in connection with PKI components for administration, communications, and protection of keys or other sensitive data shall use the following symmetric algorithms for the time periods indicated:

Symmetric Algorithm	Sunset Date
3 Key TDES	Deprecated. May be used until 12/31/2023 only for data blocks that are 8 MB or less per unique key bundle. [11]
AES	No stipulation

All certificates (excluding self-signed certificates), CRLs, and OCSP Responses, shall use the following hashing algorithms for the time periods indicated:

	Issued before 12/31/2030	Issued after 12/31/2030
Hash Algorithm for Certificates, CRLs and OCSP Responses	SHA-256 SHA-384	SHA-256 SHA-384 SHA-512

CRLs, OCSP Responder certificates, and OCSP Responses shall use the same or stronger signature algorithms, key sizes, and hash algorithms as used by the CA to sign the certificate in question.

All PKI components that use hash algorithms for security relevant functions, such as key generation or agreement, communication protocols (e.g. TLS), or password protection, shall use the same or larger bit versions of the hash algorithm(s) used by the CA to sign certificates.

All IceCAP certificates shall contain public keys and algorithms that also conform to [NIST SP 800-78].

6.1.6 Public Key Parameters Generation and Quality Checking

For RSA, the PKI shall conduct public key parameters generation and quality checking in accordance with NIST SP 800-89.

For ECC, public keys shall fall within curves defined in Section 7.1.3. Additionally, the PKI shall confirm the validity of all keys as specified in NIST SP 800-56A.

[11] See NIST SP 800-131 regarding the deprecation of 3 Key TDES

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

The use of a specific key is determined by the key usage and extended key usage extensions in the X.509 certificate.

- Certificates to be used for authentication shall set the *digitalSignature* bit only.
- Certificates to be used by human Subscribers for digital signatures shall set the *digitalSignature* and *nonRepudiation* bits.
- Certificates that have the *nonRepudiation* bit set, shall not have *keyEncipherment* bit or *keyAgreement* bit set.
- Certificates to be used for encryption shall set the *keyEncipherment* bit.
- Certificates to be used for key agreement shall set the *keyAgreement* bit.
- CA certificates shall set *cRLSign* and *keyCertSign bits*.

Keys associated with CA certificates shall be used for signing certificates and CRLs only.

Public keys that are bound into human subscriber certificates shall be certified for use in signing or encrypting, but not both.

Device subscriber certificates that provide authenticated connections using key management certificates may set both the *digitalSignature* and *keyEncipherment* bits. With the exception of OCSP Responder certificates, device certificates must not assert the *nonRepudiation* bit.

For End Entity certificates, the Extended Key Usage extension shall always be present and shall not contain *anyExtendedKeyUsage* {2.5.29.37.0}.

The extended key usage shall meet the requirements stated in Section 10.21. Extended Key Usage values shall be consistent with key usage bits asserted.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is FIPS 140, *Security Requirements for Cryptographic Modules*. The CPMA may determine that other comparable validation, certification, or verification standards are also sufficient. These standards will be published by the CPMA. Cryptographic modules shall be validated to the FIPS 140 level identified in Section 6.1.1 or equivalent. The CPMA reserves the right to review technical documentation associated with any cryptographic modules under consideration for use by the CAs.

The table in Section 6.1.1 summarizes the minimum requirements for cryptographic modules; higher levels may be used. In addition, private keys shall not exist outside the cryptographic module in plaintext form.

For IceCAP-hardware tokens, see Section 12.

6.2.2 Private Key Multi-Person Control

Use of a CA private signing key, CSA private signing key, and IceCAP-contentSigning private key shall require action by at least two persons.

6.2.3 Private Key Escrow

Under no circumstances shall signature keys be escrowed by a third-party.

Human subscriber private keys used for decryption shall be escrowed. For Device subscriber private keys used for decryption, escrow is mandatory unless the data protected by these keys will never require recovery. This escrow shall take place prior to the generation of the corresponding certificates.

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Private Signature Key

The CA private signature keys shall be backed up under the same multi-person control as used to generate and protect the original signature key. A single backup copy of the signature key shall be stored at or near the CA location. A second backup copy shall be kept at the CA backup location. Procedures for CA private signature key backup shall be included in the appropriate CPS and shall meet the multiparty control requirement of Section 5.2.2.

6.2.4.2 Backup of KED Private Decryption Key

The KED key shall be backed up as necessary to provide secure continuity of key recovery operations. The backup keys shall only be created, stored, and restored under two-person control. The process of restoring the backup KED key shall maintain two party control throughout and shall meet the multiparty control requirement in Section 5.2.2.

6.2.4.3 Backup of Subscriber Private Signature Key

Subscriber private signature keys whose corresponding public key is contained in a certificate asserting medium-software and/or medium-CBP-software may be backed up or copied but the backup must be held in the Subscriber's control. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module.

Device private signature keys whose corresponding public key is contained in a certificate asserting medium-device-software may be backed up or copied but must be held in the control of the device's human sponsor or other authorized administrator.

Subscriber private signature keys whose corresponding public key is contained in a certificate asserting IceCAP-hardware, IceCAP-cardAuth, medium-hardware, medium-device-hardware, medium-CBP-hardware, high-hardware, and/or high-CBP-hardware shall not be backed up or copied.

6.2.4.4 CSA Private Key Backup

If backed up, the CSA private signature keys shall be backed up under the same multi-person control used to generate the CSA private signature keys and shall be accounted for and protected in the same manner as the original. A single backup copy of the CSA private signature key may be stored at or near the CSA location. A second backup copy may be kept at the CSA backup location. Procedures for CSA private signature key backup shall be included in the appropriate CPS.

6.2.4.5 IceCAP Content Signing Key Backup

If backed up, the IceCAP-contentSigning private keys shall be backed up under the same multi-person control used to generate the original content signing key. When implemented, procedures for IceCAP-contentSigning private key backup and storage shall be included in the appropriate CPS and shall meet the multiparty control requirement of Section 5.2.2.

6.2.5 Private Key Archival

Private signature keys shall not be archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

CA, KED, DDS, CMS, and CSA private keys shall be generated by and remain in an approved cryptographic module. The keys may be backed up in accordance with Section 6.2.4.

If any private key is transported from one cryptographic module to another, the private key shall be protected using a FIPS approved algorithm and at a bit strength commensurate with the key being transported.

Private or symmetric keys used to encrypt other private keys for transport must be protected from disclosure.

6.2.7 Private Key Storage on Cryptographic Module

The cryptographic module may store Private Keys in any form as long as the keys are not accessible without the use of an authentication mechanism that is in compliance with the FIPS 140 rating of the cryptographic module.

6.2.8 Method of Activating Private Key

The user must be authenticated to the cryptographic module before the activation of any private key(s), except as indicated below. Acceptable means of authentication include but are not limited to passphrases, PINs or biometrics. When passphrases or PINs are used, they shall be a minimum of six (6) characters. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

For IceCAP-cardAuth, user activation of the private key is not required.

For device certificates, the device may be configured to activate its private key without requiring its human sponsor or 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.

6.2.9 Methods of Deactivating Private Key

After use, a subscriber cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS. Activated cryptographic modules shall not be left unattended or otherwise open to unauthorized access. Removable cryptographic modules shall be protected when not in use.

CA, CSA, CMS, KED and DDS hardware cryptographic modules shall be removed and stored in a secure container when not in use. If a cryptographic module contains a complete (versus split) key for activating CA, CSA, CMS, KED, or DDS keys, all storage procedures and mechanisms for that module shall require two-person control.

6.2.10 Method of Destroying Private Key

Private signature keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. For software cryptographic

modules, this can be accomplished by overwriting the data. For hardware cryptographic modules, this will usually require executing a “zeroize” command.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects Of Key Management

6.3.1 Public Key Archival

The public key is archived as part of the certificate archival.

6.3.2 Certificate Operational Periods/Key Usage Periods

See Section 5.6.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

For IceCAP-cardAuth, id-medium-device-software and id-medium-device-hardware, private keys may be activated without entry of activation data.

For all other policies governed by this CP, the activation data used to unlock private keys, in conjunction with any other access control procedure, shall have an appropriate level of strength for the keys or data to be protected and shall meet the applicable security policy requirements of the cryptographic module used to store the keys. Subscriber activation data may be user selected. For CAs, activation data shall either entail the use of biometric data or satisfy the policy enforced at/by the cryptographic module. 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.

When a CA uses passwords as activation data for the CA signing key, at a minimum the activation data shall be changed upon CA re-key.

6.4.2 Activation Data Protection

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data should be either biometric in nature, memorized, or contained within an organizationally approved device or software tool (e.g., password manager) that leverages encryption commensurate with the bit-strength of the key it activates. If written down, activation data shall be secured at the level of the data that the associated cryptographic module is used to protect and shall not be stored with the cryptographic module. In all cases, the protection mechanism shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the respective CP or CPS.

6.4.3 Other Aspects of Activation Data

CAs, CMS, CSAs, and RAs shall change the activation data whenever the token is re-keyed or returned from maintenance.

For IceCAP-hardware, the activation data may be reset upon a successful biometric 1:1 match of the applicant by an RA or a trusted agent against the biometrics collected during the identity proofing process (see Section 3.2.3).

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The CA, KED, DDS, CMS, CSA, Administration Workstations, KRA, and RA shall include the following functionality:

- Require authenticated logins.
- Provide Discretionary Access Control, including managing privileges of users to limit users to their assigned roles.
- Provide a security audit capability (See Section 5.4)
- Prohibit object re-use.
- Require use of cryptography for session communication and database security
- Require a trusted path for identification and authentication.
- Provide domain isolation for processes.
- Provide self-protection for the operating system.
- Require self-test security related CA services (e.g., check the integrity of the audit logs)
- Support recovery from key or system failure.

In addition, the KRS shall be provided with residual information protection by the underlying operating system.

When CA and KRS equipment is hosted on evaluated platforms in support of computer security assurance requirements, the system (hardware, software, operating system) shall, where possible, operate in an evaluated configuration. At a minimum, such platforms shall use the same version of the computer operating system as that which received the evaluation rating.

The computer system shall be configured with the minimum of the required accounts and network services.

6.5.2 Computer Security Rating

For the CBCA, not applicable.

Entity CAs shall identify computer security rating requirements, if any.

6.6 Life-Cycle Technical Controls

6.6.1 System Development Controls

The System Development Controls for the CA, KED, DDS, KRA, CMS, and CSA are as follows:

- Use software that has been designed and developed under a formal, documented development methodology.
- Where open-source software has been utilized, security requirements shall be achieved through software verification and validation and structured development life-cycle management.
- Procured hardware and software shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).
- Specially developed hardware and software shall be developed in a controlled environment, and the development process shall be defined and documented.

This requirement does not apply to commercial off-the-shelf hardware or software.

- All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability from the purchase location to the operations location.
- The hardware and software shall be dedicated to performing PKI activities. There shall be no other applications; hardware devices, network connections, or component software installed which is not part of the PKI operation.
- Proper care shall be taken to prevent malicious software from being loaded onto the equipment. Applications required to perform PKI operations shall be obtained from sources authorized by local policy. Hardware and software shall be scanned for malicious code on first use and periodically thereafter.
- Hardware and software updates shall be purchased or developed in the same manner as original equipment and shall be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of the CA, KED, DDS, CMS, CSA, Administration Workstations, KRA, and RA systems as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism to periodically verify the integrity of the software and to detect unauthorized modification to the CA, KED, DDS, CMS, and CSA software or configuration. The CA, KED, DDS, and CSA software, when first loaded, shall be verified as that supplied by the vendor, with no modifications, and as the version intended for use.

All Administration Workstations shall be dedicated to remote administration and shall be protected while at rest. In particular, they shall not be used as personal workstations. The Administration Workstations shall be maintained at the same level as the equipment they access (i.e. all policies on patching, virus scanning, etc. that are levied on the target systems shall apply to this workstation as well).

In addition, only applications required to perform the organization's mission shall be loaded on the KRA, KRO or RA workstation, and all such software shall be obtained from sources authorized by local policy.

6.6.3 Life Cycle Security Controls

For the CBCA, not applicable.

CAs shall identify any life cycle security control requirements.

6.7 Network Security Controls

CAs, KEDs, DDSs, CSAs, CMSs, Administration Workstations, KRAs, and RAs shall employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures shall include the use of guards, firewalls and filtering routers. Unused network ports and services shall be turned off. Any network software present shall be necessary to the functioning of the Entity CA.

If the Administration Workstation is located outside the security perimeter of the CA, KED, DDS, CMS, and CSA, it shall access the PKI Enclave using site-to-site VPN. The VPN shall use FIPS approved cryptography commensurate with the cryptographic strength of certificates issued by the PKI being administered. The VPN shall be configured for mutual authentication, encryption and integrity. If mutual authentication is shared secret based, the shared secret shall be changed at least annually, shall be

randomly generated, and shall have entropy commensurate with the cryptographic strength of certificates issued by the PKI being administered. Alternatively, when the Administration Workstation is located inside the security perimeter of the CA, KED, DDS, CMS, and CSA, and protected by the boundary controls of the PKI Enclave, appropriate techniques shall be used for mutual authentication of the PKI components and mutual authentication of traffic flowing among them.

Any boundary control devices used to protect the network on which the PKI equipment is hosted shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

Remote access shall be mediated by a bastion host or "jump server" (i.e. a machine that presents a limited interface for interaction). All network activity to the PKI components (e.g. CA, KED, DDS, CMS, and/or CSA) shall be initiated from the bastion host. The bastion host is considered part of the CA, KED, DDS, CMS, and/or CSA and shall meet the security requirements for these components. A remote workstation or user shall perform mutual authentication with the bastion host using strong authentication (e.g., PKI credential) commensurate with the cryptographic strength of certificates issued by the PKI being administered. Cryptographic material derived from the authentication shall be used to protect the communication with the bastion host. (Note: client-authenticated TLS, SSH and IPSEC are examples of protocols that meet this requirement.) In addition, the user shall authenticate to the PKI component being administered via the bastion host. In other words, authentication to the bastion host does not alleviate the need to authenticate to the PKI component(s) being administered.

Remote administration shall be designed such that there are positive controls to meet the two-person control requirements specified in this CP. In addition, the remote administration shall be designed such that there are positive controls to meet the requirement for the Audit Administrator to control the event logs. Remote administration shall continue to fully enforce the integrity, source authentication and destination authentication, as applicable for administrative functions such as configuration, patch management, and monitoring.

6.8 Time Stamping

All CA and CSA components shall regularly synchronize with a time service such as the National Institute of Standards and Technology (NIST) Atomic Clock or the NIST Network Time Protocol (NTP) Service. Time derived from the time service shall be used for establishing the time of:

- Initial validity time of a Subscriber's Certificate
- Revocation of a Subscriber's Certificate
- Posting of CRL updates
- OCSP or other CSA responses

Asserted times shall be accurate to within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events as listed in Section 5.4.1.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

Section 10 contains the certificate profiles.

7.1.1 Version Numbers

CAs shall issue X.509 v3 certificates (populate version field with integer "2").

7.1.2 Certificate Extensions

CA certificates shall not include critical private extensions.

Critical private extensions in subscriber certificates shall be interoperable in their intended community of use.

Issuer CA and Subscriber certificates may include any extensions as specified by RFC 5280 in a certificate, but must include those extensions required by this CP. Any optional or additional extensions shall be non-critical and shall not conflict with the certificate and CRL profiles defined in this CP.

7.1.3 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}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}
sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13}
ecdsa-with-Sha256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) specified(3) sha256(2)}
ecdsa-with-Sha384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) specified(3) sha384(3)}
ecdsa-with-Sha512	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) specified(3) sha512(4)}

Certificates under this CP shall use the following OIDs for identifying the subject public key information:

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) public-key-type(2) 1}

7.1.4 Name Forms

The subject and issuer fields of the certificate shall be populated with a unique Distinguished Name in accordance with one or more of the X.500 series standards, with the attribute type as further constrained by RFC5280. Subject and issuer fields shall include attributes as detailed in the table below.

Issuer and Subject Name Form (CAs)

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
1	Recommended	CN	0…1	Descriptive name for CA, e.g., “CN=XYZ Inc CA”
	Optional	OU	0…N	As needed
	Recommended	OU	0…1	“Certification Authorities” or similar text
	Required	O	1	Issuer name, e.g., “O=XYZ Inc”
	Required	C	1	Country name, e.g., “C=US”
2	Recommended	CN	0…1	Descriptive name for CA, e.g., “CN=XYZ Inc CA”
	Optional	OU	0…N	As needed
	Recommended	OU	0…1	“Certification Authorities” or similar text
	Optional	O	0…1	Issuer name, e.g., “O=XYZ Inc”
	Optional	C	0…1	Country name, e.g., “C=US”
	Required	DC	1	Domain name, e.g., “DC=xyzinc”
	Required	DC	1…N	Domain root label(s), e.g., “DC=com” or “DC=com, DC=au”, etc.

Subject Name Form (Non-CAs)

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
1	Required	See Content description	1…N	Additional naming attributes for uniquely identifying the subject including common name, serialNumber, etc.
	Optional	OU	0…N	As needed
	Required	O	1	Issuer name, e.g., “O=XYZ Inc” exactly as it appears in the CA certificate(s)
	Required	C	1	Country name, e.g., “C=US” exactly as it appears in the CA certificate(s)
2	Required	See Content description	1…N	Additional naming attributes for uniquely identifying the subject including common name, serialNumber, etc.
	Optional	OU	0…N	As needed
	Optional	O	0…1	Issuer name, e.g., “O=XYZ Inc”

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
	Required	DC	1	Domain name, e.g., “DC=xyzinc” exactly as it appears in the CA certificate(s)
	Required	DC	1…N	Domain root label(s), e.g., “DC=com” or “DC=com, DC=au”, etc. exactly as it appears in the CA certificate(s)

When multiple values exist for an attribute in a DN, the DN shall be encoded so that each attribute value is encoded in a separate relative distinguished name.

7.1.5 Name Constraints

For all Enterprise CAs, CertiPath shall assert name constraints that limit the name space of the subject CAs to name spaces that are appropriate for the subject CA domain.

Principal CAs may assert critical or non-critical name constraints beyond those specified in the Certificate Formats in Section 10 subject to the requirements above.

When issuing cross certificates to another Bridge CA (say CA X), the CBCA shall use the excluded sub-tree field to exclude all other Bridge CAs except X.

7.1.6 Certificate Policy Object Identifier

With the exception of self-signed Root CA certificates, all CA and subscriber certificates shall contain at least one certificate policy OID.

Cross-certified CAs shall not assert the CBCA policy OIDs in the certificates they issue with the exception of the *subjectDomain* field in the policy mappings extension of the cross certificate issued to the CBCA.

When a CA asserts a policy OID, it may also assert all lower assurance policy OIDs.

Certificates that map to IceCAP-cardAuth or IceCAP-contentSigning shall contain only that specific mapped policy OID.

OCSP Responder certificates shall assert all policy OIDs for which the issuing CA is authoritative.

7.1.7 Usage of Policy Constraints Extension

When present, the policy constraints extension shall be marked critical.

The CBCA shall assert the policy constraints extension to inhibit policy mapping by the PCAs and to require explicit policy.

The Issuer Principal CAs are required to adhere to the policy constraints identified in the Certificate Formats described in this CP since inhibiting policy mapping may limit interoperability.

The CBCA will assert inhibit policy mapping with skipCerts value = 1 or 2 when issuing certificates to other Bridge CAs. Bridge certification paths will include no more than two Bridge CAs. In other words, all Bridge – Bridge interoperability shall be on a bilateral basis.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under the CertiPath CP may contain the following policy qualifiers: user notice, policy name, and CP and CPS pointers.

Certificates issued by cross certified CAs may contain policy qualifiers identified in RFC 5280.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

The certificate policies extension shall not be marked critical.

7.1.10 Inhibit Any Policy Extension

If present, this extension shall not be marked critical. SkipCerts shall be set to '0'.

7.2 CRL Profile

7.2.1 Version Numbers

CAs shall issue X.509 version two (v2) CRLs (populate version field with integer "1").

7.2.2 CRL and CRL Entry Extensions

Critical private extensions shall be interoperable in their intended community of use.

Section 10 contains the CRL formats.

7.3 OCSP Profile

OCSP requests and responses shall be in accordance with RFC 6960. Section 10 contains the OCSP request and response formats.

All OCSP Responders must accept and return SHA-1 hashes in the certID and responderID fields. OCSP responses shall not contain a hash algorithm in the certID that differs from the certID in the request.

7.3.1 Version Number

The version number for requests and responses shall be v1.

7.3.2 OCSP Extensions

Critical extensions shall not be used in OCSP requests or responses.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

CAs shall have a compliance audit mechanism in place to ensure that the requirements of their CP/CPS and the provisions of the AGREEMENT are being implemented and enforced.

8.1 Frequency or Circumstances of Assessments

All CAs, KRSs, CMSs, RAs and CSAs shall be subject to a periodic compliance audit at least once per year.

8.2 Identity and Qualifications of Assessor

The compliance auditor shall demonstrate competence in the field of compliance audits, and shall be thoroughly familiar with requirements of the applicable CP. The compliance auditor must perform such compliance audits as a primary responsibility. The applicable CPS shall identify the compliance auditor and justify the compliance auditor's qualifications.

8.3 Assessor's Relationship to Assessed Entity

The compliance auditor shall either represent a firm, which is independent from the entity being audited, or it shall be sufficiently organizationally separated from that entity to provide an unbiased, independent evaluation. An example of the latter situation may be an organizational audit department provided it can demonstrate organizational separation and independence. To further ensure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining the entity's PKI Facility, associated IT and network systems, or certificate practices statement. The CPMA shall determine whether a compliance auditor meets this requirement.

In the event an entity chooses to engage compliance auditor services internal to its parent organization, it shall undergo an audit from an external third-party audit firm every third year, at a minimum.

8.4 Topics Covered by Assessment

The purpose of a compliance audit shall be to verify that a component operates in accordance with the applicable CP, CPS, KRPS, if applicable, the AGREEMENT between the Entity PKI and CertiPath, and any additional MOAs between the Entity PKI and other Entities. The compliance audit must include an assessment of the applicable CPS (and KRPS, if applicable) against the applicable CP, to determine that the CPS (and KRPS) adequately addresses and implements the requirements of the CP.

8.5 Actions Taken as a Result of Deficiency

The CPMA may determine that a CA is not complying with its obligations, as set forth in the applicable CP, CPS (and KRPS) or AGREEMENT. When such a determination is made in relation to the CBCA or CRCA, the CPMA may suspend operation of the affected CA until a remediation has been performed.; When such a determination is made in relation to a CertiPath Member CA, the CPMA may direct the CertiPath Operational Authority to cease interoperating with the affected Entity Principal CA (e.g., by revoking the certificate that the CBCA issued to the Entity Principal CA), or may direct that other corrective actions be taken which allow interoperation to continue. When the compliance auditor finds a discrepancy between how the CA is designed or is being

operated or maintained, and the requirements of the applicable CP, CPS, or Agreement, , the following actions shall be performed:

- The compliance auditor shall note the discrepancy;
- The compliance auditor shall notify the Entity of the discrepancy. The Entity shall notify the CPMA promptly and communicate the discrepancy mitigation plan;
- The party responsible for correcting the discrepancy shall determine what further notifications or actions are necessary pursuant to the requirements of the applicable CP and the AGREEMENT, and then proceed to make such notifications and take such actions without delay.

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

8.6 Communication of Results

An Audit Compliance Report package, including identification of corrective measures taken or being taken by the Entity PKI, shall be provided to the CPMA as set forth in Section 8.1. This package shall be prepared in accordance with the "Compliance Audit Reference Documents" and must include an assertion from the Entity PKI PMA that all PKI components have been audited - including any components that may be separately managed and operated. The package shall identify the versions of the CP and CPS (and KRPS) used in the assessment. Additionally, where necessary, the results shall be communicated as set forth in 8.5 above.

Practice Note:
The different components of the Infrastructure may be audited separately. In these cases, the Compliance Audit Package will contain multiple audit reports, one for each separately audited component.

---

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance and Renewal Fees

Unless (a) otherwise restricted by separate agreement with CertiPath or (b) prohibited by applicable law or any cross-certified authorities, CertiPath Member CAs (as defined in Section 1.1.4) may set any reasonable certificate issuance and renewal fees.

9.1.2 Certificate Access Fees

CertiPath Member CAs may not charge for access to any certificates.

9.1.3 Revocation or Status Information Access Fees

CertiPath Member CAs may not charge for access to any revocation or status information.

9.1.4 Fees for Other Services

Unless (a) otherwise restricted by separate agreement with CertiPath or (b) prohibited by applicable law or any cross-certified authorities, CertiPath Member CAs may set any reasonable fees for any other services that those CertiPath Member CAs may offer.

9.1.5 Refund Policy

CertiPath Member CAs may, but are not required, to have a documented refund process.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

CertiPath maintains reasonable levels of insurance coverage. CertiPath Member CAs shall also maintain reasonable levels of insurance coverage to address all foreseeable liability obligations to PKI Participants, as those entities are described in Section 1.3 of this CP.

9.2.2 Other Assets

CertiPath maintains sufficient financial resources to maintain operations and fulfill duties. CertiPath Member CAs shall also maintain reasonable and sufficient financial resources to maintain operations, fulfill duties, and address commercially reasonable liability obligations to participants in the CertiPath PKI.

9.2.3 Insurance or Warranty Coverage for End-Entities

CertiPath Member CAs may, but are not required to, offer protection to end entities that extends beyond the protections provided in this CP. Any such protection shall be offered at commercially reasonable rates.

9.3 Confidentiality of Business Information

The treatment of confidential business information provided to CertiPath in the context of submitting an application for cross certification will be in accordance with the terms of the agreements entered into between the applicable entity and CertiPath.

Each CertiPath Member CA shall maintain the confidentiality of confidential business information that is clearly marked or labeled as confidential or by its nature should reasonably be understood to be confidential and shall treat such information with the same degree of care and security as the CertiPath Member CA treats its own most confidential information.

When key recovery is requested as part of an investigation or court order, information concerning the request shall be protected from unauthorized disclosure.

9.4 Privacy of Personal Information

CertiPath collects, stores, processes and discloses personally identifiable information in accordance with the CertiPath Privacy Policy, located at https://certipath.com/privacy/.

Each CertiPath Member CA may store, process, and disclose personally identifiable information in accordance with the privacy policy of that CertiPath Member CA, except that the storage of PII shall be limited to the minimum necessary to validate the identity of the Subscriber or Key Recovery Requestor. This may include attributes that correlate identity evidence to authoritative sources. The RA shall provide explicit notice to the Subscriber regarding the purpose for storing a record of the PII necessary for identity proofing and the consequences for not providing the information. PII stored for identity proofing purposes shall not be used for any other purpose.

9.5 Intellectual Property Rights

Neither the CertiPath Operational Authority nor any CertiPath Member CA shall knowingly violate any intellectual property rights held by others.

9.5.1 Property Rights in Certificates and Revocation Information

Subject to any agreements between CertiPath and its customers, CertiPath Member CAs shall retain all Intellectual Property Rights in and to the Certificates and revocation information that they issue. For any certificates issued under the CRCA, CertiPath grants permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to a Memorandum of Agreement (or equivalent contractual mechanism) with the relevant CA. CertiPath shall grant permission to use revocation information to perform Relying Party functions, subject to applicable contractual agreements.

9.5.2 Property Rights in the CPS

All Intellectual Property Rights in this CP are owned by CertiPath and/or its licensors. All Intellectual Property Rights in CBCA and CRCA CPSs are owned by CertiPath.

9.5.3 Property Rights in Names

As between CertiPath and a Certificate Applicant, the Certificate Applicant retains all rights, if any, in any trademark, service mark, or trade name of the Certificate Applicant contained in any Customer Application.

9.5.4 Property Rights in Keys

Subject to any agreements between CertiPath and its customers, ownership of and property rights in key pairs corresponding to Certificates of CertiPath Member CAs and Subscribers shall be specified in the applicable CPS of the Entity CA regardless of the physical medium within which they are stored and protected. Such persons retain all Intellectual Property Rights in and to these key pairs. Notwithstanding the foregoing, CertiPath's root public keys and the root Certificates containing them are the property of CertiPath.

9.6 Representations and Warranties

Representations and warranties contained in commercial agreements between CertiPath and other involved parties are contained in the following documents:

- Master Services Agreements between CertiPath and its customers
- Current Customer Service Orders

The above-listed documents may contain additional and/or supplemental representations and warranties between the parties.

9.6.1 CA Representations and Warranties

9.6.1.1 CertiPath CA

CertiPath represents and warrants that, to its knowledge:

- There are no material misrepresentations of fact in the Cross Certificates known to or originating from the CertiPath OA approving the Cross Certification Applications or issuing the Cross Certificates,
- There are no errors in the information in the Cross Certificates that were introduced by the CertiPath OA approving the Cross Certification Application or issuing the Cross Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate,
- CertiPath certificates meet all material requirements of this CP, and
- Revocation services and use of a repository conform to the applicable CPS in all material aspects.

The applicable contractual agreements described in Section 9.6 may include additional representations and warranties.

9.6.1.2 Subordinate or Cross-Certified CAs

CertiPath Member CAs represent and warrant that:

- The CA signing private key is protected and that no unauthorized person has ever had access to that private key;
- All representations made by the CertiPath Member CA in any applicable agreements are true and accurate, to the best knowledge of the applicable CA;
- If applicable (i.e., if the CertiPath Member CA has issued certificates to a Subscriber), each Subscriber has been required to represent and warrant that all information supplied by the Subscriber in connection with, and/or contained in the Certificate is true;
- If applicable, CAs shall maintain an agreement with Affiliated Organizations concerning the obligations required by this CP; and
- The Cross Certificate and any other certificates issued by the Cross-Certified CA is being used exclusively for authorized and legal purposes, consistent with this

and any other applicable CP or CPS, to the best knowledge of the Cross-Certified CA.

9.6.2 RA, KRA and KRO Representations and Warranties

Registration Authorities and KROs shall represent and warrant that identity verification is performed in accordance with Section 3 of the applicable certificate policy.

KRAs shall:

- represent and warrant that subscribers' escrowed keys shall be released only for properly authenticated and authorized requests.
- validate the authorization of the KRO to act on behalf of the Subscriber whose key recovery has been requested.
- communicate knowledge of a recovery process only to the KROs and Requestor involved in the key recovery, and to those other individuals with a need to know as determined by organizational policy.
- protect subscribers' escrowed keys from unauthorized disclosure, including the encrypted files and associated decryption keys.
- protect recovered keys from compromise.
- protect all information, including the KRA's own key(s) used to recover subscribers' escrowed keys.

In the event the Key Recovery Requestor is someone other than the Subscriber (i.e., Third-party Requestor), the KRA or KRO shall validate the Key Recovery Requestor's authority to request the Subscriber's private key. In addition, KROs shall

- accurately represent themselves when requesting key recovery services.
- validate the identity of the requestor seeking a key recovery.
- communicate knowledge of a recovery process only to the KRAs and the Key Recovery Requestor, and to those other individuals with a need to know as determined by organizational policy.
- protect all information, including the KRO's own key(s) used to request recovery of subscribers' escrowed keys.
- retain records pertaining to recovery requests and disposition, including acknowledgment of receipt by the Key Recovery Requestor.

9.6.3 Subscriber

A Subscriber shall be required to sign a document (e.g., a subscriber agreement) containing the requirements the Subscriber shall meet respecting protection of the private key and use of the certificate before or immediately following certificate issuance.

In signing the document described above, each Subscriber shall agree to the following:

- Subscriber shall accurately represent itself in all communications with the Issuing PKI authorities.
- Subscriber shall promptly notify the appropriate CA upon suspicion of loss or compromise of its private keys. Such notification shall be made directly or indirectly through mechanisms consistent with the Issuing CA's CPS.

In signing the document described above, each Subscriber shall represent and warrant that:

- The data contained in any certificates issued to the Subscriber is accurate;
- The Subscriber lawfully holds the private key corresponding to the public key identified in the Subscriber's certificate;
- The Subscriber will protect its private keys at all times, in accordance with this policy, as stipulated in the certificate acceptance agreements, and local procedures; and
- The Subscriber will abide by all the terms, conditions, and restrictions levied on the use of the private keys and certificates.

9.6.4 Relying Party

Parties who rely upon the certificates issued under a policy defined in this document shall:

- Use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension);
- Check each certificate for validity, using procedures described in the X.509 standard [ISO 9594-8], prior to reliance;
- Establish trust in the CA that issued the certificate by verifying the certificate path in accordance with the guidelines set by the X.509 Version 3 Amendment;
- Preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data. Note: data format changes associated with application upgrades will often invalidate digital signatures and shall be avoided.

9.6.5 Representations and Warranties of Affiliated Organizations

Affiliated Organizations shall authorize the affiliation of Subscribers with the organization and shall inform the CA of any severance of affiliation with any current Subscriber.

9.6.6 Representations and Warranties of Other Participants

9.6.6.1 Third-party Key Recovery Requestors

Third-Party Key Recovery Requestors shall formally acknowledge and agree to the obligations described here:

- Request and use the subscriber's escrowed keys only to recover data they are authorized to access.
- Protect subscribers' recovered keys from compromise using a combination of computer security, cryptographic, network security, physical security, personnel security, and procedural security controls commensurate with the level of assurance of the keys being recovered.
- Destroy subscribers' private keys when no longer needed (i.e., data has been recovered) in accordance with the process established in Section 6.2.10 of the associated CPS.
- Accurately represent themselves during any key recovery operation.
- Protect information concerning each key recovery operation.

- Sign an acknowledgment of agreement to follow the law and the subscriber's organization policies relating to protection and release of the recovered key. Such agreement shall include the following attestations:
    - Requestor has been accurately identified,
    - Requestor has truthfully described the reason(s) for the key recovery request,
    - Requestor has a legitimate and official need to obtain the requested key,
    - Requestor has received the recovered key,
    - Requestor shall use the recovered key only for the stated purposes,
    - Requestor shall protect the recovered key from unauthorized access and shall destroy the key or return it to the organization when no longer needed,
    - Requestor is bound by applicable laws and regulations concerning the protection of the recovered key and any data recovered using the key.

9.6.6.2 Data Decryption Servers

Prior to the beginning of the operation of a DDS, the Entity shall formally acknowledge and agree to the obligations described here, in accordance with the stipulations of the applicable CP:

- The DDS shall accurately identify and authenticate itself to a degree commensurate with the assurance level of the key being requested.
- The DDS shall use a combination of computer security, cryptographic, network security, physical security, personnel security, and procedural security controls to protect their own keys and recovered subscribers' keys.
- The DDS shall destroy subscribers' keys when no longer required (i.e., when the data has been recovered).
- The DDS shall request and use a subscriber's escrowed key(s) only upon receipt of a request to decrypt subscriber data from an authenticated authorized Enterprise system (e.g., an email Server)

9.7 Disclaimers of Warranties

To the extent permitted by applicable law, Policy Mapping Agreements, Cross Certificates Agreements, Memoranda of Agreement, Master Services Agreements, and any other related agreements may contain disclaimers of all warranties (other than any express warranties contained in such agreements or set forth in this CP).

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CERTIPATH MEMBER CAS MAY DISCLAIM ANY EXPRESS OR IMPLIED WARRANTIES, OTHER THAN THOSE EXPRESS WARRANTIES CONTAINED IN THIS CP.

EXCEPT FOR THE EXPLICIT REPRESENTATIONS, WARRANTIES, AND CONDITIONS PROVIDED IN THIS CP OR THOSE BETWEEN CERTIPATH AND ITS CUSTOMERS UNDER SEPARATE AGREEMENTS, (A) CERTIFICATES ISSUED BY CERTIPATH AND THE CERTIPATH PKI ARE PROVIDED "AS IS", AND CERTIPATH, ITS EMPLOYEES, OFFICERS, AGENTS, REPRESENTATIVES, AND DIRECTORS DISCLAIM ALL OTHER WARRANTIES, CONDITIONS AND OBLIGATIONS OF EVERY TYPE (INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF

MERCHANTABILITY, NON-INFRINGEMENT, TITLE, SECURITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE, OR ACCURACY OF INFORMATION PROVIDED), AND FURTHER DISCLAIM ANY AND ALL LIABILITY FOR NEGLIGENCE, FAILURE TO WARN, OR LACK OF REASONABLE CARE AND (B) THE ENTIRE RISK OF THE USE OF ANY CERTIPATH CERTIFICATES, ANY SERVICES PROVIDED BY CERTIPATH, OR THE VALIDATION OF ANY DIGITAL SIGNATURES LIES WITH THE APPLICABLE PARTICIPANT.

9.8 Limitations of Liabilities

The liability (and/or limitation thereof) of CertiPath to CertiPath Member CAs to which CertiPath issues Certificates shall be set forth in the applicable agreements.

OTHER THAN THE ABOVE-DESCRIBED LIMITATIONS OF LIABILITY, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL CERTIPATH BE LIABLE FOR ANY INDIRECT DAMAGES OF ANY KIND, INCLUDING CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE, OR OTHER DAMAGES WHATSOEVER ARISING OUT OF OR RELATED TO THIS CP, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE TOTAL, AGGREGATE LIABILITY OF CERTIPATH ARISING OUT OF OR RELATED TO THIS CP SHALL BE LIMITED TO DIRECT DAMAGES ACTUALLY INCURRED, UP TO THE GREATER OF (A) THE AMOUNTS ACTUALLY PAID TO CERTIPATH UNDER THIS CP BY THE PARTY CLAIMING SUCH DAMAGES DURING THE TWELVE MONTHS IMMEDIATELY PRECEDING THE EARLIEST EVENT(S) GIVING RISE DIRECTLY TO THE LIABILITY OR (B) TEN THOUSAND DOLLARS ($10,000 USD).

THE TOTAL, AGGREGATE LIABILITY OF EACH CERTIPATH MEMBER CA ARISING OUT OF OR RELATED TO IMPROPER ACTIONS BY THE CERTIPATH MEMBER CA SHALL BE LIMITED TO ONE THOUSAND DOLLARS ($1,000 USD) PER TRANSACTION AND ONE MILLION DOLLARS ($1 MILLION USD) PER INCIDENT[12].

9.9 Indemnities

9.9.1 Indemnification Customer CAs

To the extent permitted by applicable law, each CertiPath Member CA shall indemnify CertiPath and its contractors, agents, assigns, employees, officers, and directors from and against any third-party claims, liabilities, damages, costs and expenses (including reasonable attorney's fees), relating to or arising out of any certificates issued by CertiPath, including, without limitation, for:

- Falsehood or misrepresentation of fact by the CertiPath Member CA in the applicable contractual agreements.
- Failure by the CertiPath Member CA to disclose a material fact in any applicable contractual agreement, if the misrepresentation or omission was made negligently or with intent to deceive any party,
- The CertiPath Member CA's failure to protect the CertiPath Member CA private key, to use a Trustworthy System, or to otherwise take the precautions

[12] For the purposes of Section 9.8, the following definitions apply:
Incident – Misuse relating to a single credential regardless of the relying parties involved
Transaction - Any use of a single credential. Multiple transactions associated with misuse of a single credential constitute an incident.

necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the CertiPath Member CA private key, or
- The CertiPath Member CA's use of a name (including without limitation within a common name, domain name, or email address) that infringes upon the Intellectual Property Rights of a third-party.

Any applicable contractual agreement between CertiPath and an Entity CA that is a customer of CertiPath within the CertiPath PKI may include additional indemnity obligations, but these would not apply to cross-certified CAs that are not customers of CertiPath.

9.9.2 Indemnification by Relying Parties

To the extent permitted by applicable law, each Relying Party shall indemnify CertiPath and its contractors, agents, assigns, employees, officers, and directors from and against any third-party claims, liabilities, damages, costs and expenses (including reasonable attorney's fees), relating to or arising out of the use of or reliance by the Relying Party on any certificates issued by CertiPath, including, without limitation:

- The Relying Party's improper, illegal, or unauthorized use of a Certificate (including use of any expired, revoked, or unvalidated Certificate);
- The Relying Party's unreasonable reliance on a Certificate, given the circumstances;
- The Relying Party's use of a Certificate that asserts a "pass-through" policy OID as defined in Section 1.2 of this CP; or
- The Relying Party's failure to check the status of a Certificate on which it relies to determine if the Certificate is expired or revoked.

Any applicable contractual agreement between CertiPath and a Relying Party within the CertiPath PKI may include additional indemnity obligations, but these would not apply to relying parties that are not customers of CertiPath.

9.10 Term and Termination

9.10.1 Term

The CP becomes effective upon ratification by the CertiPath PMA, adoption by the CertiPath Board and publication in the CertiPath Repository as a PDF document. Amendments to this CP become effective upon ratification by the CertiPath PMA and adoption by the CertiPath Board and publication at:
https://certipath.com/services/federated-trust/policy-management-authority/

There is no specified term for this CP.

9.10.2 Termination

While this CP may be amended from time to time, it shall remain in force until replaced by a newer version or explicitly terminated by a resolution of the CertiPath Board of Directors. For purposes of clarity, termination of any Agreement shall not operate as a termination of this CP unless this CP is explicitly terminated by a separate resolution of the CertiPath Board of Directors.

9.10.3 Effect of Termination and Survival

Upon termination of this CP, CAs cross certified with or subordinate to CertiPath are nevertheless bound by its terms for all Certificates issued for the remainder of the

validity periods of such Certificates. The following sections of this CP shall survive the termination of this CP: 2.1, 2.2, 5.4, 5.5, 6.2-6.4, 6.8, 9.2-9.4, 9.7-9.10, 9.13-9.16.

9.11 Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, CertiPath shall use commercially reasonable methods to communicate with cross-certified or subordinate CAs, taking into account the criticality and subject matter of the communication.

Unless otherwise specified by agreement between the parties, all CertiPath Member CAs shall use commercially reasonable methods to communicate with CertiPath, taking into account the criticality and subject matter of the communication.

Any planned change to the infrastructure of a CertiPath Member CA that has the potential to affect the CBCA operational environment shall be communicated to the CPMA at least two weeks prior to implementation, and any new CA certificates produced as a result of the change provided to the CPMA within 24 hours following implementation.

9.12 Amendments

9.12.1 Procedure for Amendment

The CertiPath PMA shall review the CP at least once every year. Additional reviews may be enacted at any time at the discretion of the CPMA or at the request of the CertiPath Board.

If the CPMA wishes to recommend amendments or corrections to the CP, such modifications shall be circulated to appropriate parties identified by the CPMA and CertiPath Board (including, without limitation, all CertiPath Member CAs). Comments from such parties will be collected by the CPMA in a fashion determined by the CPMA.

The CertiPath Board of Directors has final authority over the incorporation of modifications in the CertiPath CP; however, authority has been delegated to the CPMA to act on the CertiPath Board of Directors behalf for maintaining and updating the CP and for processing new applicants for CertiPath membership. For clarity, it should be noted that the CPMA has primary authority and responsibility for the CertiPath PKI and, under normal circumstances, its decisions are final. The only situation where the CertiPath Board would intervene is in a case where the CPMA has decided to or not to cross-certify or subordinate with an applicant, and such decision impacts the fiduciary duty of the CertiPath Board. In these cases, the CertiPath Board will act as the final decision authority after reviewing all evidence. If the evidence suggests the CPMA acted outside of its scope or without impartiality, it could result in the CPMA recommendation being modified or disregarded.

Notwithstanding the foregoing, if the CPMA believes that material amendments to the CP are necessary immediately to stop or prevent a breach of the security of CertiPath, CertiPath shall be entitled to make such amendments effective immediately upon publication in the Repository. CertiPath shall use commercially reasonable efforts to immediately notify CertiPath Member CAs of such changes.

9.12.2 Notification Mechanism and Period

The most up-to-date copy of the CP are published online at:
https://certipath.com/services/federated-trust/policy-management-authority/

In addition, changes, including a description of the change, are communicated by the CPMA to every CertiPath Customer via a designated point of contact.

This CP and any subsequent changes shall be made publicly available within thirty (30) days of approval.

9.12.3 Circumstances under Which OID Must be Changed

Certificate Policy OIDs shall be changed if the CPMA determines that a change in the CP reduces the level of assurance provided.

9.13 Dispute Resolution Provisions

9.13.1 Disputes among CertiPath and Customers

Provisions for resolving disputes between CertiPath and its Customers shall be set forth in the applicable agreements between the parties.

9.13.2 Alternate Dispute Resolution Provisions

Except as otherwise agreed (e.g., under an agreement described in Section 9.13.1 above), any dispute under this CP shall be resolved by binding arbitration in accordance with the commercial rules (or international rules, if the other party to the dispute is a non-US entity) of the American Arbitration Association then in effect. The arbitration panel shall consist of one (1) neutral arbitrator if the amount in controversy is less than $10,000, otherwise the panel shall consist of three (3) neutral arbitrators, each an attorney with five (5) or more years of experience in computer and technology law and/or the primary area of law as to which the dispute relates. The arbitrator(s) shall have never been employed (either as an employee or as an independent consultant) by either of the Parties, or any parent, subsidiary or affiliate thereof. The Parties shall have the right to take discovery of the other Party by any or all methods provided in the Federal Rules of Civil Procedure. The arbitrator(s) may upon request exclude from being used in the arbitration proceeding any evidence not made available to the other Party pursuant to a proper discovery request. The arbitrator(s) shall apply federal law of the United States and/or the law of the State of New York, and the arbitration proceeding shall be held in New York City, New York, USA or in such other location as is mutually agreed upon. The cost of the arbitration shall be borne equally by the Parties, unless the arbitrator(s) awards costs and attorney's fees to the prevailing Party. Notwithstanding the choice of law provision in this Agreement, the Federal Arbitration Act, except as modified herein, shall govern the interpretation and enforcement of this provision. All arbitration proceedings shall be conducted in English. Any claim, dispute and controversy shall be arbitrated on an individual basis and not aggregated with the claims of any third party. Class action arbitration is prohibited. The arbitrator(s) shall have no discretion to award punitive damages. Notwithstanding the foregoing dispute resolution procedures, either Party may apply to any court having jurisdiction to (i) enforce the agreement to arbitrate, (ii) seek provisional injunctive relief so as to maintain the status quo until the arbitration award is rendered or the dispute is otherwise resolved, or to otherwise prevent irreparable harm, (iii) avoid the expiration of any applicable limitation period, (iv) preserve a superior position with respect to creditors, or (v) challenge or vacate any final decision or award of the arbitration panel that does not comport with the express provisions of this CP.

9.14 Governing Law

Subject to any limits appearing in applicable law, the federal laws of the United States and/or the laws State of New York shall govern the enforceability, construction, interpretation, and validity of this CP, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in the State of New York. This choice of law is made to ensure uniform procedures and interpretation for all CertiPath Customers, no matter where they are located.

This governing law provision applies only to this CP. Agreements incorporating this CP by reference may have their own governing law provisions, provided that this Section 9.14 governs the enforceability, construction, interpretation, and validity of the terms of this CP separate and apart from the terms of such other agreements, subject to any limitations appearing in applicable law.

9.15 Compliance with Applicable Law

This CP is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No Stipulation

9.16.2 Assignment

Except where specified by other contracts, no party may assign or delegate this CP or any of its rights or duties under this CP, without the prior written consent of the other party (such consent not to be unreasonably withheld), except that CertiPath may assign and delegate this CP to any party of its choosing.

9.16.3 Severability

If any provision of this CP is held to be invalid by a court of competent jurisdiction, then the remaining provisions will nevertheless remain in full force and effect.

9.16.4 Waiver of Rights

No waiver of any breach or default or any failure to exercise any right hereunder shall be construed as a waiver of any subsequent breach or default or relinquishment of any future right to exercise such right. The headings in this CP are for convenience only and cannot be used in interpreting this CP.

9.16.5 Force Majeure

CertiPath shall not be liable for any failure or delay in its performance under this CP due to causes that are beyond its reasonable control, including, but not limited to, an act of God, act of civil or military authority, fire, epidemic, flood, earthquake, riot, war, failure of equipment, failure of telecommunications lines, lack of Internet access, sabotage, and governmental action. CERTIPATH HAS NO LIABILITY FOR ANY DELAYS, NON-DELIVERIES, NON-PAYMENTS, MIS-DELIVERIES OR SERVICE INTERRUPTIONS CAUSED BY ANY THIRD-PARTY ACTS OR THE INTERNET INFRASTRUCTURE OR ANY NETWORK EXTERNAL TO CERTIPATH.

9.17 Other Provisions

No stipulation.

10 CERTIFICATE, CRL, AND OCSP FORMATS

This section contains the formats for the various PKI objects such as certificates, CRLs, and OCSP requests and responses.

Certificates and CRLs issued under a policy OID of this CP may contain extensions not listed in the profiles in this section only upon CPMA approval.

First entries in the caIssuers field of the AIA extension and CRL DP shall point to a resource that is publicly available using HTTP. If LDAP pointers are used, they shall appear only after the HTTP pointers.

For attribute values other than dc and email address:[13]: All CA Distinguished Names (in various fields such as Issuer, Subject, Subject Alternative Name, Name constraints, etc.) shall be encoded as a printable string. All subscriber DN portions to which name constraints apply shall be encoded as a printable string. Other portions of the subscriber DN shall be encoded as a printable string if possible. If a portion cannot be encoded as a printable string, then and only then shall it be encoded using a different format and that format shall be UTF8.

For dc and email address attribute values: All dc attribute values shall be encoded as IA5 string.

CAs may issue partitioned CRLs as long as the CRLs are not indirect CRLs, are not partitioned by reason code, and the CRL DP and *issuingDistributionPoint* do not assert a name *relativeToIssuer*. If a CRL does not include *issuingDistributionPoint*, it must be a full and complete CRL covering all certificates signed by any and all keys associated with the CA.

If Delta CRLs are implemented, the CRL extension *id-ce-freshestCRL* must not be marked critical.

Global Unique Identifier (GUID) used in certificates shall conform to the RFC 4122 requirements. Since GUID is associated with a card, the same GUID shall be asserted as the UUID in all applicable certificates and in all applicable other signed objects on the card.

Practice Note:
If the Entity PKI leverages the CRL to provide revocation status for its delegated OCSP services, that CA should issue a full and complete CRL (i.e., a CRL without *issuingDistributionPoint* extension). This will ensure all revocation information is in one place and readily available to the OCSP Responder.

---

[13] Note that CertiPath does not recommend using email address in a DN.

10.1 CBCA → Principal CA Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha384 WithRSAEncryption {1 2 840 113549 1 1 12}
Issuer Distinguished Name	cn=CertiPath Bridge CA <CA identifying text>, ou=Certification Authorities, o=CertiPath, c=us
Validity Period	Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	Per Section 10.22
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as in PKCS-10 request from the CBCA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the PCA)
Key Usage	c=yes; *keyCertSign, cRLSign, digitalSignature* (optional), *nonRepudiation* (optional)
Application Policies[14]	c=no; EKU OIDs as appropriate except code-signing and *anyExtendedKeyUsage*
Certificate Policies	c=no; Applicable certificate policies from Section 1.2
Policy Mapping	c=no; Applicable policy mappings
Basic Constraints	c=yes; cA=True; path length constraint optional[15]
Name Constraints[16]	c=yes; permitted subtrees for DN, RFC-822, and DNS name forms
Policy Constraints	c=yes; inhibitPolicyMapping skipCerts = 0; requireExplicitPolicy skipCerts = 0
Authority Information Access	c=no; id-ad-caIssuers access method entry containing HTTP URL for .p7c file containing certificates issued to CBCA
Subject Information Access	c=no, id-ad-caRepository (1.3.6.1.5.5.7.48.5) containing an HTTP URI pointing to a file that has an extension of .p7c. The file is a certs-only Cryptographic Message Syntax file (RFC 5751) that includes valid CA certificates issued by the subject CA. If the certificate asserts a path length constraint of zero in Basic Constraints, this extension may be omitted.
CRL Distribution Points[17]	c=no;
Inhibit anyPolicy	c=no; skipCerts = 0

[14] This extension is optional; it is always present when the partner does not follow EKU guidance stipulated in Sections 6.1.7 and 10.21.

[15] Path length constraint must be present and must be "0" if certificate is issued to a Signing CA. Otherwise the path length constraint should be asserted only if the cross certified domain PKI hierarchy (depth) is not expected to change over time.

[16] Name constraint extension may be omitted with PMA approval, e.g., when the PCA includes service providers. CPMA may decide to assert a subset of or additional name forms in special circumstances.

[17] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain the HTTP (i.e., of the form http://…) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain *nameRelativetoCRLIssuer*)

10.2 Principal CA → CBCA Certificate

Note: When the Principal CA is other than a Root CA, the CertiPath Bridge must be issued a cross-certificate from a Principal CA that is unconstrained with respect to path length by the upstream PKI hierarchy starting with the Root. Otherwise, valid paths may not be built or validated successfully.

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}; sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13} ecdsa-with-SHA256 {1 2 840 10045 4 3 2} ecdsa-with-SHA384 {1 2 840 10045 4 3 3} ecdsa-with-SHA512 {1 2 840 10045 4 3 4}
Issuer Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	cn=CertiPath Bridge CA <CA identifying text>, ou=Certification Authorities, o=CertiPath, c=us
Subject Public Key Information	Per Section 10.22
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as in PCA PKCS-10 request to the CBCA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the CBCA)
Key Usage	c=yes; *keyCertSign, cRLSign, digitalSignature* (optional), *nonRepudiation* (optional)
Application Policies	c=no; optional, EKU OIDs as appropriate except code-signing and *anyExtendedKeyUsage*
Certificate Policies	c=no; Applicable certificate policies
Policy Mapping	c=no; Applicable policy mappings
Basic Constraints	c=yes; cA=True; path length constraint absent
Name Constraints	c=yes; optional, excluded subtrees: Name forms as determined by the Entity PMA
Policy Constraints[18]	Optional; c=yes; requireExplicitPolicy skipCerts = 0
Authority Information Access	c=no; id-ad-caIssuers access method entry containing HTTP URL for p7c file containing certificates issued to PCA
CRL Distribution Points[19]	c = no;
Inhibit anyPolicy	c=no; skipCerts = 0

[18] Inclusion of Policy Constraints in a Principal CA cross certificate to the CBCA is optional. If implemented, all certificates with a trust path that traverses the CertiPath Bridge must be valid for one or more mapped policies.

[19] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain the HTTP (i.e., of the form http://…) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain *nameRelativetoCRLIssuer*).

10.3 CBCA → XBCA Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha384 WithRSAEncryption {1 2 840 113549 1 1 12}
Issuer Distinguished Name	cn=CertiPath Bridge CA <CA identifying text>, ou=Certification Authorities, o=CertiPath, c=us
Validity Period	Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	2048 bit modulus, rsaEncryption {1 2 840 113549 1 1 1}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as in PCA PKCS-10 request from the CBCA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request to the CBCA)
Key Usage	c=yes; *keyCertSign, cRLSign, digitalSignature* (optional), *nonRepudiation* (optional)
Application Policies[20]	c=no; EKU OIDs as appropriate except code-signing and *anyExtendedKeyUsage*
Certificate Policies	c=no; Applicable certificate policies from Section 1.2
Policy Mapping	c=no; Applicable policy mappings
Basic Constraints	c=yes; cA=True; path length constraint absent
Name Constraints	c=yes; excluded subtrees: DNs for all Bridge CAs except XBCA
Policy Constraints	c=yes; inhibitPolicyMapping skipCerts = 2; requireExplicitPolicy skipCerts = 0
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for p7c file containing certificates issued to CBCA
Subject Information Access	c=no, id-ad-caRepository (1.3.6.1.5.5.7.48.5) containing an HTTP URI pointing to a file that has an extension of .p7c. The file is a certs-only Cryptographic Message Syntax file (RFC 5751) that includes valid CA certificates issued by the subject CA. If the certificate asserts a path length constraint of zero in Basic Constraints, this extension may be omitted.
CRL Distribution Points[21]	c = no;
Inhibit anyPolicy	c=no; skipCerts = 0

[20]This extension is optional; it is always present when the cross certified Bridge does not follow or does not enforce EKU guidance stipulated in Sections 6.1.7 and 10.21.

[21] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain the HTTP (i.e., of the form http://…) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain *nameRelativetoCRLIssuer*).

10.4 XBCA → CBCA Certificate

For Bridge Certification Authorities cross-certifying with the CertiPath Bridge, the following is the recommended certificate profile:

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}; sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13} ecdsa-with-SHA256 {1 2 840 10045 4 3 2} ecdsa-with-SHA384 {1 2 840 10045 4 3 3} ecdsa-with-SHA512 {1 2 840 10045 4 3 4}
Issuer Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	cn=CertiPath Bridge CA <CA identifying text>, ou=Certification Authorities, o=CertiPath, c=us
Subject Public Key Information	2048 bit modulus, rsaEncryption {1 2 840 113549 1 1 1}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as in XBCA PKCS-10 request to the CBCA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the CBCA)
Key Usage	c=yes; *keyCertSign, cRLSign, digitalSignature* (optional), *nonRepudiation* (optional)
Certificate Policies	c=no; Applicable certificate policies
Policy Mapping	c=no; Applicable policy mappings
Basic Constraints	c=yes; cA=True; path length constraint absent
Name Constraints	c=yes; excluded subtrees: DNs for all Bridge CAs except CBCA
Policy Constraints	optional; c=yes; inhibitPolicyMapping skipCerts = 1; requireExplicitPolicy skipCerts = 0.
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for p7c file containing certificates issued to XBCA
CRL Distribution Points[22]	c = no;
Inhibit anyPolicy	c=no; skipCerts = 0

[22] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain the HTTP (i.e., of the form http://…) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain *nameRelativetoCRLIssuer*).

10.5 CRCA or Enterprise PKI Self-Signed Root Certificate (also called Trust Anchor)

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}; sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13} ecdsa-with-SHA256 {1 2 840 10045 4 3 2} ecdsa-with-SHA384 {1 2 840 10045 4 3 3} ecdsa-with-SHA512 {1 2 840 10045 4 3 4}
Issuer Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	Per Section 10.22
Extension	**Value**
Subject Key Identifier	c=no; Octet String
Key Usage	c=yes; *keyCertSign, cRLSign, DigitalSignature, nonRepudiation*
Basic Constraints	c=yes; cA=True; path length constraint absent

10.6 Intermediate or Signing CA Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}; sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13} ecdsa-with-SHA256 {1 2 840 10045 4 3 2} ecdsa-with-SHA384 {1 2 840 10045 4 3 3} ecdsa-with-SHA512 {1 2 840 10045 4 3 4}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 Subject CA DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	Per Section 10.22
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the subject CA)
Key Usage	c=yes; *keyCertSign, cRLSign, digitalSignature* (optional), *nonrepudiation* (optional)
Certificate Policies	c=no; Applicable certificate policies
Basic Constraints[23]	c=yes; cA=True; path length constraint absent or value per Issuer PKI
Name Constraints[24]	optional; c=yes; permitted subtree per the name space for the CA
Policy Constraints[25]	optional; c=no; inhibitPolicyMapping skipCerts = 0.
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA
Subject Information Access	c=no, id-ad-caRepository (1.3.6.1.5.5.7.48.5) containing an HTTP URI pointing to a file that has an extension of .p7c. The file is a certs-only Cryptographic Message Syntax file (RFC 5751) that includes valid CA certificates issued by the subject CA. If the certificate asserts a path length constraint of zero in Basic Constraints, this extension may be omitted.
CRL Distribution Points[26]	c = no;

[23] In general, Basic Constraints path length constraint is set to zero for an issuing CA.
[24] Included to support Enterprise CAs under the CertiPath common policy root.
[25] Included to support Enterprise CAs under the CertiPath common policy root.
[26] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain the HTTP (i.e., of the form http://…) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

10.7 Subscriber Identity Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}; sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13} ecdsa-with-SHA256 {1 2 840 10045 4 3 2} ecdsa-with-SHA384 {1 2 840 10045 4 3 3} ecdsa-with-SHA512 {1 2 840 10045 4 3 4}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue; Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	Per Section 10.22
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA per RFC 5280 method 1 or other method)
Key Usage	c=yes; *digitalSignature*
Extended Key Usage	c-no; per Section 10.21
Certificate Policies	c=no; Applicable certificate policies
Subject Alternative Name	c=no; URI[27], [28]: urn:uuid:<32 character hex representing 128 bit GUID> other name forms optional
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder[29]
CRL Distribution Points[30]	c = no;

[27] Note this name form is tagged [6] and encoded as an IA5String.
[28] URI must be present in certificates asserting IceCAP-hardware or equivalent certificate policy OID. It is optional in other certificates.
[29] OCSP must be present when IceCAP-hardware or an equivalent certificate policy OID is also present on the hardware token. It is optional in other certificates.
[30] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain the HTTP (i.e., of the form http://…) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

10.8 Subscriber Signature Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}; sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13} ecdsa-with-SHA256 {1 2 840 10045 4 3 2} ecdsa-with-SHA384 {1 2 840 10045 4 3 3} ecdsa-with-SHA512 {1 2 840 10045 4 3 4}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue; Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	Per Section 10.22
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; *digitalSignature, nonRepudiation*
Extended Key Usage	c=no; per Section 10.21
Certificate Policies	c=no; Applicable certificate policies
Subject Alternative Name	c=no; RFC822 email address (required) URI[31]: urn:uuid:<32 hex representing 128 bit GUID> (optional) others optional
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder[32]
CRL Distribution Points[33]	c = no;

[31] Note this name form is tagged [6] and encoded as an IA5String.
[32] OCSP must be present when IceCAP-hardware or an equivalent certificate policy OID is also present on the hardware token; otherwise optional.
[33] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain the HTTP (i.e., of the form http://…) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

10.9 Subscriber Encryption Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}; sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13} ecdsa-with-SHA256 {1 2 840 10045 4 3 2} ecdsa-with-SHA384 {1 2 840 10045 4 3 3} ecdsa-with-SHA512 {1 2 840 10045 4 3 4}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue; Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	Per Section 10.22
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; RSA: *keyEncipherment* (required), *dataEncipherment* (optional); or ECC: *keyAgreement* (required)
Extended Key Usage	c=no; per Section 10.21
Certificate Policies[34]	c=no; Applicable certificate policies
Subject Alternative Name	c=no; RFC822 email address (required) URI[35]: urn:uuid:<32 hex representing 128 bit GUID> (optional) others optional
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder[36]
CRL Distribution Points[37]	c = no;

[34] Only assert the software OID in order to support key recovery to software tokens
[35] Note this name form is tagged [6] and encoded as an IA5String.
[36] OCSP must be present when IceCAP-hardware or an equivalent certificate policy OID is also present on the hardware token; otherwise optional.
[37] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain the HTTP (i.e., of the form http://…) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

10.10 Card Authentication Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}; sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13} ecdsa-with-SHA256 {1 2 840 10045 4 3 2} ecdsa-with-SHA384 {1 2 840 10045 4 3 3} ecdsa-with-SHA512 {1 2 840 10045 4 3 4}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue; Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	sn=<GUID> with applicable DN prefix.
Subject Public Key Information	Per Section 10.22
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA per RFC 5280 method 1 or other method)
Key Usage	c=yes; *digitalSignature*
Extended Key Usage	c-yes; id-PIV-cardAuth {2.16.840.1.101.3.6.8}
Certificate Policies	c=no; id-IceCAP-cardAuth or equivalent
Subject Alternative Name	c=no; URI[38] urn:uuid:<32 character hex representing 128 bit GUID>
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points[39]	c = no;

[38] Note this name form is tagged [6] and encoded as an IA5String.

[39] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain the HTTP (i.e., of the form http://…) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

10.11 IceCAP Content Signer Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}; sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13} ecdsa-with-SHA256 {1 2 840 10045 4 3 2} ecdsa-with-SHA384 {1 2 840 10045 4 3 3} ecdsa-with-SHA512 {1 2 840 10045 4 3 4}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	9 years from date of issue; Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	Per Section 10.22
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; *digitalSignature*
Extended key usage	c=yes; id-fpki-pivi-content-signing; {2.16.840.1.101.3.8.7}
Certificate Policies	c=no; id-IceCAP-contentSigning or equivalent
Subject Alternative Name	optional; c=no
CRL Distribution Points[40]	c = no;
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder

[40] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain the HTTP (i.e., of the form http://…) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

10.12 Code Signing Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}; sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13} ecdsa-with-SHA256 {1 2 840 10045 4 3 2} ecdsa-with-SHA384 {1 2 840 10045 4 3 3} ecdsa-with-SHA512 {1 2 840 10045 4 3 4}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	3 years from date of issue; Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	Per Section 10.22
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; *nonRepudiation, digitalSignature*
Extended key usage	c=yes; { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) id-kp(3) id-kp-codesigning (3) }
Certificate Policies	c=no; Applicable certificate policies
Subject Alternative Name	DN of the person controlling the code signing private key
CRL Distribution Points[41]	c = no;
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA

[41] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain the HTTP (i.e., of the form http://…) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

10.13 Device or Server Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}; sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13} ecdsa-with-SHA256 {1 2 840 10045 4 3 2} ecdsa-with-SHA384 {1 2 840 10045 4 3 3} ecdsa-with-SHA512 {1 2 840 10045 4 3 4}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	3 years from date of issue; Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP cn={ Host URL | Host IP Address | Host Name }
Subject Public Key Information	Per Section 10.22
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; RSA: *keyEncipherment, digitalSignature* ECC: *digitalSignature* (required)[42], *keyAgreement* (optional)
Extended Key Usage	c=no; per Section 10.21
Certificate Policies	c=no; Applicable certificate policies
Subject Alternative Name	c=no; always present, Host URL | IP Address | Host Name
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA (optional) id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points[43]	c = no; always present

[42] TLS Servers and devices should use certificates for authentication and Ephemeral DH obviating the need for key agreement.

[43] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain the HTTP (i.e., of the form http://…) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

10.14 Role Signature Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}; sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13} ecdsa-with-SHA256 {1 2 840 10045 4 3 2} ecdsa-with-SHA384 {1 2 840 10045 4 3 3} ecdsa-with-SHA512 {1 2 840 10045 4 3 4}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	3 years from date of issue; Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 subject DN for role as specified in Section 7.1.4 of this CP
Subject Public Key Information	Per Section 10.22
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; *nonRepudiation, digitalSignature*
Extended Key Usage	c=no; per Section 10.21
Certificate Policies	c=no; Applicable certificate policies
Subject Alternative Name	c = no; DN of the person controlling the role signing private key; RFC822 email address of role (Optional)
CRL Distribution Points[44]	c = no;
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA (optional) id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder

[44] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain the HTTP (i.e., of the form http://…) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

10.15 Role Encryption Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}; sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13} ecdsa-with-SHA256 {1 2 840 10045 4 3 2} ecdsa-with-SHA384 {1 2 840 10045 4 3 3} ecdsa-with-SHA512 {1 2 840 10045 4 3 4}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	3 years from date of issue; Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 subject DN for role as specified in Section 7.1.4 of this CP
Subject Public Key Information	Per Section 10.22
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; RSA: *keyEncipherment* ECC: *keyAgreement*
Extended Key Usage	c=no; per Section 10.21
Certificate Policies	c=no; Applicable certificate policies
Subject Alternative Name	c=no; RFC822 email address of role (required); others optional
CRL Distribution Points[45]	c = no;
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA (optional) id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder

[45] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain the HTTP (i.e., of the form http://…) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

10.16 OCSP Responder Certificate

The following table contains the OCSP Responder certificate profile assuming that the OCSP Responder certificate is issued by the same CA using the same key as the Subscriber Certificate.

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}; sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13} ecdsa-with-SHA256 {1 2 840 10045 4 3 2} ecdsa-with-SHA384 {1 2 840 10045 4 3 3} ecdsa-with-SHA512 {1 2 840 10045 4 3 4}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	120 days or less; Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 OCSP Responder (subject) DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	Per Section 10.22
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; *digitalSignature* (required), *nonrepudiation* (optional)
Extended key usage	c=yes; id-kp-OCSPSigning {1 3 6 1 5 5 7 3 9}
Certificate Policies[46]	c=no; Applicable certificate policies
Subject Alternative Name	c=no; URI: HTTP URL for the OCSP Responder (preferred); and/or DNS: Fully qualified domain name of the OCSP Responder
No Check id-pkix-ocsp-nocheck; {1 3 6 1 5 5 7 48 1 5}	c=no; Null
Authority Information Access	c=no; optional; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to issuing CA

[46] This field shall contain all of the certificate policy OIDs for which the CA issues certificates.

10.17 PKCS 10 Request Format

The following table contains the format for PKCS 10 requests.

Field	Value
Version	V1 (0)
Subject Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	Per Section 10.22
Subject's Signature	Signed using the private key associated with above Subject Public Key
Extension (encoded in extension request attribute)	**Value**
Subject Key Identifier	c=no; Octet String
Key Usage	c=yes; optional; keyCertSign, cRLSign, DigitalSignature, nonRepudiation
Basic Constraints	c=yes; optional; cA=True; path length constraint (absent or 0 as appropriate)
Name Constraints	c=yes; optional; permitted subtrees for DN, RFC-822, and DNS name forms

10.18 CRL Format

10.18.1 Full and Complete CRL

If the Entity PKI provides OCSP Responder Services, the Entity PKI shall make a full and complete CRL available to the OCSP Responders as specified below. This CRL may also be provided to the relying parties.

Field	Value
Version	V2 (1)
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}; sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13} ecdsa-with-SHA256 {1 2 840 10045 4 3 2} ecdsa-with-SHA384 {1 2 840 10045 4 3 3} ecdsa-with-SHA512 {1 2 840 10045 4 3 4}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
thisUpdate	Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
nextUpdate	Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter; >= thisUpdate + CRL issuance frequency
Revoked certificates list	0 or more 2-tuple of certificate serial number and revocation date (Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter)
CRL Extension	**Value**
CRL Number	c=no; monotonically increasing whole number (never repeated)
Authority Key Identifier	c=no; Octet String (same as in Authority Key Identifier field in certificates issued by the CA)
CRL Entry Extension	**Value**
Reason Code	c=no; optional, must be included when revoked for key compromise or CA compromise

10.18.2 Distribution Point Based Partitioned CRL

The Entity PKI may make a distribution based partitioned CRL available to the relying parties in lieu of or in addition to the full and complete CRL. The distribution point based partition CRL shall adhere to the following profile. Note that the CRL may not be an indirect CRL, may not be partitioned based on reason codes, and may not assert a distribution point that is a nameRelativetoCRLIssuer.

Field	**Value**
Version	V2 (1)
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}; sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13} ecdsa-with-SHA256 {1 2 840 10045 4 3 2} ecdsa-with-SHA384 {1 2 840 10045 4 3 3} ecdsa-with-SHA512 {1 2 840 10045 4 3 4}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
thisUpdate	Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
nextUpdate	Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter; >= thisUpdate + CRL issuance frequency
Revoked certificates list	0 or more 2-tuple of certificate serial number and revocation date (Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter)
CRL Extension	**Value**
CRL Number	c=no; monotonically increasing whole number (never repeated)
Authority Key Identifier	c=no; Octet String (same as in Authority Key Identifier field in certificates issued by the CA)
Issuing Distribution Point	c=yes; distribution point field must contain a full name (i.e., distribution point field may not contain nameRelativetoCRLIssuer; the following fields must all be absent: onlySomeReasons, indirectCRL, and onlyContainsAttributeCerts
CRL Entry Extension	**Value**
Reason Code	c=no; optional, must be included when revoked for key compromise or CA compromise

10.19 OCSP Request Format

Requests sent to Issuer PKI OCSP Responders are not required to be signed but may be at the discretion of the Issuer PKI. See RFC 6960 for detailed syntax. The following table lists the fields that are expected by the OCSP Responder.

Field	**Value**
Version	V1 (0)
Requester Name	DN of the requestor (required)
Request List	Must contain one and only one certID
Request Extension	**Value**
None	None
Request Entry Extension	**Value**
None	None

10.20 OCSP Response Format

See RFC 6960 for detailed syntax. The following table lists which fields are populated by the OCSP Responder.

Field	Value
Response Status	As specified in RFC 2560
Response Type	id-pkix-ocsp-basic {1 3 6 1 5 5 7 48 1 1}
Version	V1 (0)
Responder ID	KeyHash as specified in RFC 6960 (SHA-1 hash of the BIT STRING subjectPublicKey excluding the tag, length, and number of unused bits in the responder's certificate).
Produced At	GeneralizedTime
List of Responses	Each response will contain certificate id; certificate status[47], thisUpdate, nextUpdate[48],
Responder Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}; sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13} ecdsa-with-SHA256 {1 2 840 10045 4 3 2} ecdsa-with-SHA384 {1 2 840 10045 4 3 3} ecdsa-with-SHA512 {1 2 840 10045 4 3 4}
Certificates	Applicable OCSP Responder certificate
Response Extension	**Value**
Nonce	(optional) c=no; Value in the nonce field of request (only included if present in the request)[49]
Response Entry Extension	**Value**
None	None

[47] If the certificate is revoked, the OCSP Responder shall provide the revocation time and revocation reason from the CRL entry and CRL entry extension.

[48] The OCSP Responder shall use thisUpdate and nextUpdate from the CA CRL.

[49] An OCSP Responder may operate entirely offline, only pre-generating OCSP Responses that do not include a nonce. If the OCSP Responder is online and available to sign responses, support for inclusion of a nonce is optional.

10.21 Extended Key Usage

Certificate Type	Required EKU	Optional EKU	Prohibited EKU
CA[50]	None	None	All
Code Signing	id-kp-codesigning {1 3 6 1 5 5 7 3 3}	Lifetime Signing {1.3.6.1.4.1.311.10.3.13}[51]	All Others
Domain Controller	id-kp-serverAuth {1 3 6 1 5 5 7 3 1}; id-kp-clientAuth {1.3.6.1.5.5.7.3.2}; id-pkinit-KPKdc {1 3 6 1 5 2 3 5}; smartCardLogon {1.3.6.1.4.1.311.20.2.2}	None	All Others
Trusted Role Authentication and Signature Certificate	id-kp-clientAuth {1.3.6.1.5.5.7.3.2}; smartCardLogon {1.3.6.1.4.1.311.20.2.2}; id-pkinit-KPClientAuth {1 3 6 1 5 2 3 4}[52]; id-kp-emailProtection {1.3.6.1.5.5.7.3.4}	Any EKU that is consistent with Key Usage	Any EKU that is not consistent with Key Usage *anyExtendedKeyUsage* {2.5.29.37.0}
Trusted Role Encryption Certificate	See Subscriber Group, Role, Encryption Certificate	See Subscriber Group, Role, Encryption Certificate	See Subscriber Group, Role, Encryption Certificate
OCSP Responder	id-kp-OCSPSigning {1 3 6 1 5 5 7 3 9}	None	All Others
PIV-I, Card Authentication Certificate	id-PIV-cardAuth {2.16.840.1.101.3.6.8}	None	All Others
PIV-I Content Signing Certificate	id-fpki-pivi-content-signing {2.16.840.1.101.3.8.7}	None	All Others

[50] CA certificate includes self-signed Root, cross certificates, subordinate CA certificates, and self-issued key rollover certificates.
[51] It is recommended that this EKU be included so that MSFT platforms will not verify signed code using an expired certificate.
[52] The last two only if the private key is in hardware.

Certificate Type	Required EKU	Optional EKU	Prohibited EKU
Subscriber, Group, Role, PIV-I, Authentication Certificate	id-kp-clientAuth {1.3.6.1.5.5.7.3.2}; smartCardLogon {1.3.6.1.4.1.311.20.2.2}; id-pkinit-KPClientAuth {1 3 6 1 5 2 3 4}[53]	Any EKU that is consistent with Key Usage	Any EKU that is not consistent with Key Usage *anyExtendedKeyUsage* {2.5.29.37.0}
Subscriber Group, Role, Encryption Certificate[54]	id-kp-emailProtection {1.3.6.1.5.5.7.3.4};	Any EKU that is consistent with Key Usage, e.g., Encrypting File System {1.3.6.1.4.1.311.10.3.4}	Any EKU that is not consistent with Key Usage *anyExtendedKeyUsage* {2.5.29.37.0}
Subscriber, Group, Role, Signature Certificate	id-kp-emailProtection {1.3.6.1.5.5.7.3.4}; MSFT Document Signing {1.3.6.1.4.1.311.10.3.12};	Adobe Certified Document Signing {1.2.840.113583.1.1.5} Any EKU that is consistent with Key Usage	Any EKU that is not consistent with Key Usage *anyExtendedKeyUsage* {2.5.29.37.0}
Subscriber, Group, Role Authentication and Signature Certificate (Two Certificate Solution)	id-kp-clientAuth {1.3.6.1.5.5.7.3.2}; smartCardLogon {1.3.6.1.4.1.311.20.2.2}; id-pkinit-KPClientAuth {1 3 6 1 5 2 3 4}[55]; id-kp-emailProtection {1.3.6.1.5.5.7.3.4}; MSFT Document Signing {1.3.6.1.4.1.311.10.3.12};	Adobe Certified Document Signing {1.2.840.113583.1.1.5} Any EKU that is consistent with Key Usage	Any EKU that is not consistent with Key Usage *anyExtendedKeyUsage* {2.5.29.37.0}
Time Stamp Authority	id-kp-timestamping {1 3 6 1 5 5 7 3 8}	None	All Others
VPN Client	id-kp-clientAuth {1.3.6.1.5.5.7.3.2}; iKEIntermediate {1.3.6.1.5.5.8.2.2}; id-kp-ipsecIKE {1 3 6 1 5 5 7 3 17}	None	All Others

[53] The last two only if the private key is in hardware.

[54] This certificate is defined as the one that has only the key encipherment or key agreement bit set and optionally data encipherment bit set.

[55] The last two only if the private key is in hardware.

Certificate Type	Required EKU	Optional EKU	Prohibited EKU
VPN Server	id-kp-serverAuth {1 3 6 1 5 5 7 3 1}; id-kp-clientAuth {1.3.6.1.5.5.7417.3.2}; iKEIntermediate {1.3.6.1.5.5.8.2.2}; id-kp-ipsecIKE {1 3 6 1 5 5 7 3 17}	None	All Others
Web Client	id-kp-clientAuth {1.3.6.1.5.5.7.3.2}	None	All Others
Web Server	id-kp-serverAuth {1 3 6 1 5 5 7 3 1} id-kp-clientAuth {1.3.6.1.5.5.7.3.2}	None	All Others
Workstation	id-kp-clientAuth {1.3.6.1.5.5.7.3.2}; iKEIntermediate {1.3.6.1.5.5.8.2.2}; id-kp-ipsecIKE {1 3 6 1 5 5 7 3 17}	None	All Others

10.22 Subject Public Key Information Format

If the Subject Public Key is RSA, it shall be of the following format:

Algorithm OID: rsaEncryption {1 2 840 113549 1 1 1}
Parameters: NULL
Modulus m and public exponent e where,
m is 2048, 3072, or 4096 bits; and
$2^{16} < e < 2^{256}$

If the Subject Public Key is Elliptic Curve key, it shall be of the following format. This example assumes P256 curve is used. See Section 7.1.3 for additional allowable curves.

Algorithm OID: ecPublicKey {1 2 840 10045 2 1},
Parameters: namedCurve P-256 {1 2 840 10045 3 1 7},
Subject Public Key: Uncompressed EC Point

11 PKI REPOSITORY INTEROPERABILITY PROFILE

This section provides an overview of the PKI Repository interoperability profiles. The following topics are discussed:

- Protocol
- Authentication
- Naming
- Object Class
- Attributes

Each of these items is described below.

11.1 Protocol

Each Enterprise shall implement a PKI Repository that provides HTTP protocol access to certificates and CRLs.

11.2 Authentication

Each PKI Repository shall permit “none” authentication to read certificate and CRL information.

Each Enterprise shall be free to implement authentication mechanisms of its choice for browse and list operations.

Any write, update, add entry, delete entry, add attribute, delete attribute, change schema etc., shall require password over TLS or a stronger authentication mechanism.

11.3 Naming

This CP has defined the naming convention.

When a LDAP repository is used:

1. Certificates shall be stored in the LDAP Repository in the entry that appears in the certificate subject name;
2. The issuedByThisCA element of crossCrossCertificatePair shall contain the certificate(s) issued by a CA whose name the entry represents; and
3. CRLs shall be stored in the LDAP Repository in the entry that appears in the CRL issuer name.

11.4 Object Class

When a LDAP repository is used:

1. Entries that describe CAs shall be defined by the organizationUnit structural object class. These entries shall also be a member of pkiCA cpCPS auxiliary object classes; and
2. Entries that describe individuals (human entities) shall be defined by the inetOrgPerson class, which inherits from other classes: person, and organizationalPerson. These entries shall also be a member of pkiUser auxiliary object class.

11.5 Attributes

When a LDAP repository is used:

1. CA entries shall be populated with the caCertificate, crossCertificatePair, certificateRevocationList, cPCPS attributes, as applicable; and
2. User entries shall be populated with userCertificate attribute containing the encryption certificate. Signature certificate need not be published to the LDAP Repository.

12 INTEROPERABLE SMART CARD DEFINITION

IceCAP enables the issuance of smart cards that are technically interoperable with Federal Personal Identity Verification (PIV) Card readers and applications as well as PIV-Interoperable (PIV-I) card readers and applications. IceCAP fully maps to the PIV-I specification as defined by the U.S. Federal Government. This section defines the specific requirements of an IceCAP Smart Card. It relies heavily on relevant specifications from the National Institute of Standards and Technology (NIST).

1. The smart card platform shall be listed on the GSA's FIPS 201 Evaluation Program Approved Product List (APL) and shall use the PIV application identifier (AID). In the event card stock is subsequently found to be unsuitable for PIV-I use, it may be removed from the APL and placed on the Removed Products List. In such cases, the following applies:
    a. Card stock that has been placed on the Removed Products List may continue to be issued for no more than one year after GSA approved replacement card stock is available.
    b. Once replacement card stock has been available for one year, PIV-I cards issued using card stock that has been placed on the Removed Products List may continue to be used until the current subscriber certificates expire, unless otherwise notified.
2. The smart card shall contain a private key and associated identity certificate asserting IceCAP-hardware or an IceCAP-hardware mapped certificate policy OID that conforms to the Identity Authentication certificate profile, Section 10.7.
3. The smart card shall contain a private key and associated card authentication certificate asserting IceCAP-cardAuth or an IceCAP-cardAuth mapped certificate policy OID that conforms to the IceCAP cardAuth certificate profile, Section 10.10.
4. The smart card may contain a private key and associated digital Signature certificate asserting medium-hardware or a medium-hardware mapped certificate policy OID.
5. The smart card may contain a private key and associated encryption certificate asserting medium- or a medium mapped certificate policy OID.
6. The smart card and all data objects on it shall be issued in accordance with SP 800-73
7. The smart card shall contain an electronic representation (as specified in SP 800-73 and SP 800-76) of the Cardholder Facial Image printed on the card.
8. Biometrics on the smart card shall also comply with Section 4.2.3 of FIPS 201-3 and SP 800-76.
9. The Cardholder Unique Identifier (CHUID) shall also comply with FIPS 201. The CHUID shall contain a 16 byte Global Unique Identifier (GUID).
10. The CMS-Signed objects such as fingerprint and photograph shall contain the GUID as the entryUUID attribute in place of FASC-N as pivFASC-N attribute.
11. IceCAP Smart Cards shall be visually distinct from the US Federal PIV Card. At a minimum, images or logos on an IceCAP Card shall not be placed entirely within Zone 11, *Agency Seal*, as defined by [FIPS 201].
12. The smart card physical topography shall include, at a minimum, the following items on the front of the card:
    a) Cardholder facial image;

b) Cardholder full name;
c) Organizational Affiliation, if it exists; otherwise the issuer of the card; and
d) Card expiration date.

13. The smart card shall have an expiration date not to exceed 6 years from date of issuance.
14. Expiration of the IceCAP Content Signing certificate shall be later than the expiration of the end user certificates on the card.[56] The Content Signing certificate shall conform to the content signing certificate profile specified in Section 10.11.
15. The IceCAP Content Signing certificate and corresponding private key shall be managed within a trusted CMS in accordance with the requirements specified in this document.
16. At issuance, the RA shall activate and release the smart card to the Subscriber only after a successful 1:1 biometric match of the applicant against the biometrics collected during identity-proofing (See Section 3.2.3).
17. The smart card may support card activation by the CMS to support card personalization and post-issuance card update. To activate the card for personalization or update, the CMS shall perform a challenge response protocol using cryptographic keys stored on the card in accordance with [SP800-73]. When cards are personalized, card management keys shall be specific to each smart card. That is, each smart card shall contain a unique card management key. Card management keys shall meet the algorithm and key size requirements stated in [SP 800-78].
18. On an annual basis, one populated representative IceCAP Smart Card must be submitted for testing for each smart card platform and configuration in use by the issuing organization.
19. Acceptable Identity Source Documents (see Section 3.2.3.1) are as follows:

    At least one identity source document SHALL meet the requirements of Strong evidence as specified in [SP 800-63A] and be one of the following forms of identification:

    - U.S. Passport or a U.S. Passport Card
    - driver's license or ID card that is compliant with [REAL-ID] requirements described in this section
    - Permanent Resident Card or Alien Registration Receipt Card (Form I-551)
    - Foreign Passport
    - Employment Authorization Document that contains a photograph (Form I-766)
    - U.S. Military ID card
    - U.S. Military dependent's ID card
    - PIV Card

    The second piece of evidence may be from the list above, but it shall not be of the same type as the primary identity source document. The second identity source document may also be one of the following:

[56] It is recommended that expiration of the content-signing certificate is later than expiration of the card.

- ID card issued by a federal, state, or local government agency or entity, provided that it contains a photograph
- voter's registration card
- U.S. Coast Guard Merchant Mariner Card
- Certificate of U.S. Citizenship (Form N-560 or N-561)
- Certificate of Naturalization (Form N-550 or N-570)
- U.S. Citizen ID Card (Form I-197)
- Identification Card for Use of Resident Citizen in the United States (Form I-179)
- Certification of Birth Abroad or Certification of Report of Birth issued by the Department of State (Form FS-545 or Form DS-1350)
- Reentry Permit (Form I-327)
- Employment authorization document issued by the Department of Homeland Security (DHS)
- driver's license issued by a Canadian government entity
- Native American tribal document
- U.S. Social Security Card issued by the Social Security Administration
- original or certified copy of a birth certificate issued by a state, county, municipal authority, possession, or outlying possession of the United States bearing an official seal
- another piece of evidence that meets the requirements of Fair evidence specified in [SP 800-63A]

13 BIBLIOGRAPHY

The following documents are sources and/or references for this CP:

ANSI X9.62-2005	Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA),
ANSI X9.63-2011 (R2017)	Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport using Elliptic Curve Cryptography,
CHARTER	CertiPath PMA Charter
FIPS 140	Security Requirements for Cryptographic Modules, http://csrc.nist.gov/publications/PubsFIPS.html
FIPS 186	Digital Signature Standard, https://csrc.nist.gov/publications/fips
FIPS 201	Personal Identity Verification (PIV) of Federal Employees and Contractors, https://csrc.nist.gov/publications/fips
RFC 4210	Certificate Management Protocol, Adams Farrell et al, September 2005. http://www.ietf.org/rfc/rfc4210.txt.
RFC 3647	Certificate Policy and Certificate Practices Framework, Chokhani, Ford, Sabett, Merrill, and Wu. November 2003. http://www.ietf.org/rfc/rfc3647.txt
RFC 4122	A Universally Unique Identifier (UUID) URN Namespace, Leach, Mealling, and Salz, July 2005 http://www.ietf.org/rfc/rfc4122.txt
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Cooper et. al., May 2008 http://www.ietf.org/rfc/rfc5280.txt
RFC 6712	Internet X.509 Public Key Infrastructure—HTTP Transfer for the Certificate Management Protocol (CMP) September 2012 https://www.ietf.org/rfc/rfc6712.txt
RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, Santesson, Myers et. al., June 2013 http://www.ietf.org/rfc/rfc6960.txt
RFC 7292	PKCS #12: Personal Information Exchange Syntax v1.1 July 2014 https://www.ietf.org/rfc/rfc7292.txt
SP800-73	Interfaces for Personal Identity Verification https://csrc.nist.gov/publications/sp800
SP800-76	Biometric Data Specification for Personal Identity Verification,. https://csrc.nist.gov/publications/sp800
SP800-78	Cryptographic Algorithms and Key Sizes for Personal Identity Verification, https://csrc.nist.gov/publications/sp800

14 ACRONYMS & ABBREVIATIONS

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
C	Country
CA	Certification Authority
CBCA	CertiPath Bridge Certification Authority
CBP	Commercial Best Practices
CHUID	Cardholder Unique Identifier
CMS	Card Management System
CN	Common Name
CP	Certificate Policy
CPMA	CertiPath Policy Management Authority
CPS	Certification Practice Statement
CPWG	CertiPath Policy Working Group
CRCA	CertiPath Root Certification Authority
CRL	Certificate Revocation List
CSA	Certificate Status Authority
DC	Domain Component
DDS	Data Decryption Server
DN	Distinguished Name
DNS	Domain Name Service
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EKU	Extended Key Usage
FASC-N	Federal Agency Smart Credential Number
FIPS	(US) Federal Information Processing Standard
GUID	Globally Unique Identifier
HTTP	Hypertext Transfer Protocol
IceCAP	Identity and Credential Assurance Policy
ID	Identifier
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
KED	Key Escrow Database
KRA	Key Recovery Agent
KRO	Key Recovery Officer
KRP	Key Recovery Policy
KRPS	Key Recovery Practices Statement
KRS	Key Recovery System

LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Standards and Technology
O	Organization
OA	Operational Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organizational Unit
PCA	Principal Certification Authority
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification - Interoperable
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PMA	Policy Management Authority
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SCVP	Simple Certificate Validation Protocol
SHA-	Secure Hash Algorithm,
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UUID	Universally Unique Identifier

15 GLOSSARY

Access	Ability to make use of any information system (IS) resource.
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems.
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Affiliated Organization	Organizations that authorize affiliation with Subscribers of IceCAP certificates
Agreement (document)	Agreement (as used in the context of this CP, between an Entity and CertiPath allowing interoperation between the CertiPath CA and Entity Principal CA). The Agreement will generally take the form of a “Master Services Agreement” or Memorandum of Agreement and is binding on both parties.
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.
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.
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event.
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.
Backup	Copy of files and programs made to facilitate recovery if necessary.
Binding	Process of associating two related elements of information.
Biometric	A physical or behavioral characteristic of a human being.
Bridge Certification Authority Membrane	The Bridge Certification Authority Membrane consists of a collection of Public Key Infrastructure components including a variety of Certification Authority PKI products, Databases, CA specific PKI Repositories, Border PKI Repository, Firewalls, Routers, Randomizers, etc.

Card Management System	The hardware/software responsible for managing smart card token content
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 certificates that expressly reference the OID of this CP in the “Certificate Policies” field of an X.509 v.3 certificate.
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.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies it’s Subscriber, (3) contains the Subscriber’s public key, (4) identifies it’s operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]
Certification Authority Software	Key Management and cryptographic software used to manage certificates issued to Subscribers.
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).
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 which it has issued that are revoked prior to their stated expiration date.

Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness and may also provide additional attribute information for the subject certificate.
CertiPath Operational Authority (CertiPath OA)	The CertiPath Operational Authority is the organization selected by the CertiPath PMA (CPMA) to be responsible for operating the CBCA and CRCA.
CertiPath PMA (CPMA)	The CertiPath PMA (CPMA) is a body responsible for setting, implementing, and administering policy decisions regarding PKI interoperability that uses the CertiPath.
CertiPath Root Certification Authority (CRCA)	The CertiPath Root Certification Authority consists of a collection of Public Key Infrastructure components (Certificate Authorities, PKI Repositories, Certificate Policies and Certificate Practice Statements) that are used to issue certificates to Entity Principal Certification Authorities.
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.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.
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.
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.
Court of Competent Jurisdiction	Any court or forum that has the power and authority to properly exercise jurisdiction to interpret and/or enforce laws.
Credential	Evidence attesting to one’s right to credit or authority; in this CP, it is any software- or hardware-based artifact and data elements associated with an individual that authoritatively binds an identity (and, optionally, additional attributes) to that individual. For IceCAP, the credential is the hardware token defined in Section 12 of this CP.
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. [FIPS1402]

Customer	Any commercial organization that is a paying member of CertiPath. A customer CA (independent of whether cross certified with CBCA or a sub-ordinate CA to CRCA) is a Certificate Authority operated by the Customer.
Cryptoperiod	Time span during which each key setting remains in effect.
Data Decryption Server	An automated system that obtains subscriber private keys from the Key Escrow Database or other DDS in order to support decryption of data entering and leaving the Organization (e.g., encrypted email).
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.
Dual Use Certificate	A certificate that is intended for use with both digital signature and data encryption services.
Duration	A field within a certificate which is composed of two subfields; "date of issue" and "date of next issue".
E-commerce	The use of network technology (especially the internet) to buy or sell goods and services.
Employee	Any person employed by an Entity as defined above.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
End Entity	Relying Parties and Subscribers.
Enterprise CA	A CA operated by or on behalf of an organization for the primary purpose of issuing credentials to its own employees and other affiliated organizations.
Entity	An organization with operational control of a CA that will interoperate with a CertiPath CA.
Entity CA	A CA that acts on behalf of an Entity and is under the operational control of an Entity.
Extended Key Usage	A certificate extension to further restrict the applications for which the public key in the certificate can be used.
Firewall	Gateway that limits access between networks in accordance with local security policy.
Inside threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.

Integrity	Protection against unauthorized modification or destruction of information. 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	The retention of the private component of the key pair associated with a Subscriber's encryption certificate to support key recovery.
Key Escrow Database	The function, system, or subsystem that maintains the key escrow repository and responds to key registration and key recovery requests from at least two Key Recovery Agents. It may also support subscriber automated self-recovery and automated recovery by a Data Decryption Server.
Key Exchange	The process of exchanging public keys in order to establish secure communications.
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Key Pair	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.
Key Recovery	Production of a copy of an escrowed key and delivery of that key to an authorized requestor.
Key Recovery Agent	An individual authorized to interface with the key escrow database (in conjunction with one or more other Key Recovery Agents) to cause the key escrow database to carry out key recovery requests.
Key Recovery Officer	An individual authorized to authenticate and submit key recovery requests to the Key Recovery Agent on behalf of requestors.
Key Recovery Practice Statement	When utilized, a statement of the practices, procedures and mechanisms that a key recovery system employs in registering and recovering escrowed keys.
Key Recovery Requestor	An individual who is authorized to request recovery of a Subscriber's escrowed key. Subscribers may request recovery of their own keys.
Key Recovery Workstation	A dedicated workstation from which the Key Recovery Agent interfaces with the key escrow database.

Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community.
Mission Support Information	Information that is important to the support of deployed and contingency forces.
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. 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. Legal non-repudiation refers to how well possession or control of the private signature key can be established.
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.
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 online).
Outside Threat	An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.
Personally Identifiable Information	Information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual.
Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.
PKI Repository	See Repository
PKI Sponsor	Fills the role of a Subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this CP.
Policy Management Authority (PMA)	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.

Principal CA	The Principal CA is a CA designated by an Entity to interoperate with the CertiPath CAs. An Entity may designate multiple Principal CAs to interoperate with the CertiPath CAs.
Privacy	Restricting access to Subscriber or Relying Party information in accordance with Federal law and Entity policy.
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 made publicly available normally 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.
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 on 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. In this CP, Repository refers to PKI Repository.
Responsible Individual	A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.
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.

Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
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.
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.
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 or network device
Sunset Date	As used in this document, the expiration or termination date after which a specific provision is no longer permitted.
Superior CA	In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).
Supervised Remote Identity Proofing	A real-time identity proofing event where the RA/Trusted Agent is not in the same physical location as the applicant/Subscriber. The RA/Trusted Agent controls the device utilized by the applicant/Subscriber during the remote identity proofing process. The remote identity proofing process employs physical, technical and procedural measures that provide sufficient confidence that the remote session can be considered equivalent to a physical, in-person identity proofing process. Supervised Remote Identity Proofing must meet the criteria specified in Section 5.3.3 of NIST SP 800-63A, dated June 2017; and must have the capacity to capture an approved biometric when utilized for PIV-I credential issuance.
System Equipment Configuration	A comprehensive accounting of all system hardware and software types and settings.
Technical non-repudiation	The contribution public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.
Third-party Key Recovery Requestor	A person, other than the Subscriber, who requests recovery of an escrowed key (e.g., supervisor, law enforcement).

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.
Trust List	Collection of trusted certificates used by Relying Parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of an Entity in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.
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".
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
Trustworthy System	Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.
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.
Update (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.
Update (in reference to significant change)	Alterations to Licensed Software, including code and/or error corrections and minor code enhancements or modifications, that may be developed and released from time to time by the Software Vendor and made available to the customer (licensee). Software Updates do not include: (i) Software Upgrades of the Licensed Software that may be developed and released from time to time by the software vendor
Upgrade (in reference to significant change)	Enhancements to the Licensed Software providing a new program feature or function that may be developed and generally released from time to time by the software vendor and made available to customer (licensee). Software Upgrades do not include: (i) Software Updates of the Licensed Software that may be developed and released from time to time by the software updates

Wildcard Certificate	A single SSL/TLS certificate with a wildcard character (*) in the domain name field. This allows the certificate to secure multiple sub domain names (hosts) pertaining to the same base domain.
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. [FIPS1402]