TSCP LLC

X.509 Certificate Policy

For The

TSCP Bridge Certification Authority (TBCA)

Version 10.12

April 9, 2026

THE TBCA CERTIFICATE POLICY VERSION 10.12 UPDATE BY THE TPMA CHAIR INCORPORATES CHANGES IN CHANGE PROPOSAL 2026-1, AS APPROVED BY VOTE OF THE TPMA ON APRIL 9, 2026.

Shauna Russell
X_ SIG

Digitally signed by Shauna Russell - SIG
Date: 2025.10.31 17:27:03 -04'00'

Shauna Russell
TPMA Chair

Revision History

Document Version	Document Date	Revision Details
0.1	5/23/2013	**NA**, Initial draft derived from FBCA CP 2.26
1.0	2/17/2014	Approved by TPMA e-vote which completed on February 17, 2014 Version 1 contains clarifications resulting from reconciliation of CPS to CP compliance review results
2.0	8/22/2014	Approved by TPMA e-vote which completed on August 22, 2014 PMA Approved Version 2 with changes from CP Change Proposal #2014-1. Includes 26 v.1.1 draft changes needed to comply with the Federal Bridge CPWG comments
3.0	10/9/2014	Approved by TPMA meeting vote on October 9, 2014 Version 3 includes changes from drafts v.2.1 through v.2.7 - changes to address CPWG comments which led to CP Change Proposal #2014-2, changed section 10.3 profile based on interoperability testing to FPKI, added section 10.4 profile change, Included Shauna R.'s minor formatting and wording changes, made initial CPWG White Space review changes (minor)
3.2	11/4/2014	Minor version to include Wendy Brown white space mapping comments and added CRL publication within 4 hours of generation (eliminating pre-generated CRLs)

Document Version	Document Date	Revision Details
		Did not upload version 3.1, when checked in, so changed this version to 3.2
3.3	11/4/2014	Forgot to save changes in 3.3, so saved and created 3.4
3.4	11/4/2014	Changed 2 comments to reflect final decision on comment response
3.5	11/5/2014	Fixed a few section reference errors
3.6	11/5/2014	Fixed section references that broke
3.7	2/6/2015	Made additional changes found from CP Mapping of Airbus, NGC, and LM CPs
3.8	2/6/2015	Operator error uploading…no changes to this doc in this version
4.0	3/12/2015	Approved by TPMA meeting vote on March 12, 2014 Includes changes from drafts v.3.2 through v.3.8 as defined by CP Change Proposal #2015-1
4.1	7/2/2015	For major versions, changed the document date to match the day it was approved by TPMA vote Added additional vote information in revision details Updated Copyright to 2015
4.2	12/9/15	Clarifications and updates from CP Mappings
5.0	12/10/15	Approved by TPMA meeting vote on 12/10/15

Document Version	Document Date	Revision Details
		Includes changes from drafts 4.1 and 4.2 as defined in Change Proposal 2015-2
6.0	1/26/18	CP change 2017-1: Federal Bridge CP update CP change 2017-2: section 9.6.3 entitled "Subscriber Representations and Warranties" to more closely match the Federal Bridge requirements CP change 2017-3: Re-key changes from CP mapping, formatting, remove redundant text, profile cert usage changes CP Change 2018-1: Subject Alt Name optional in Human Subscriber Signature Profile
7.0	3/14/18	CP Change 2018-2 Add OIDs for mediumDevice and mediumDeviceHardware and associated changes; add a definition of PIV-I and reference to Section 12 of the CP for requirements; allow 6-year PIV-I card life and mandate annual testing of PIV-I; add custodial key store requirements.
8,0	8/24/18	CP Change 2018-3 to add various new requirements from the Federal Bridge related to Key Recovery, Extended Key Usage; Transitive Closure; and issuance of a Long Term CRL. CP Change 2018-4 to add new requirements for Virtual Machine Environments. CP Change 2018-5 to add changes for mapping discrepancies based upon the Federal Bridge Annual Review.

Document Version	Document Date	Revision Details
9.0	1/22/2019	CP Change 2018-6 to add new provisions related to Supervised Remote Identity Proofing. CP Change 2018-7 to align more closely with the Federal Bridge CP for Sections 10.8 and 10.9.
10.00	4/26/2019	CP Change 2019-1 to align with the Federal Bridge CP CP Change 2019-2 to allow remote access to the CA under conditions allowed by the Federal Bridge
10.1	8/20/2020	CP Change 2020-1 to correct errors in the chart in Section 10,22 and to align with the Federal Bridge
10.2	4/8/2021	CP Change 2021-1 to update references and align with the Federal Bridge
10.3	7/14/2022	CP Change 2022-1 to add basic assurance certificates and to make several changes to align with the Federal Bridge
10.4	7/22/2023	CP Change to add changes required by the FB CP 3.0 and 3.1 (dated 4-17-2023) and to remove SHA-1 certificates
10.5	8/26/2023	Correction of typos, spacing, and table format
10.6	12/14/2023	CP Change to add changes required by Federal Bridge Change Proposal 2023-3 to clarify audit and archive record requirements for trusted role assignments and to update key/certificate operational periods
10.7	4/29/2024	Change to clarify key lifetimes and to make a change to 3.1.1 Types of Names to ensure

Document Version	Document Date	Revision Details
		Devices subject names are unique and do not take the form of human names
10.8	10/18/2024	CP Change to add changes required by Federal Bridge Change Proposal 2024-05 to clarify the definition of Remote Workstations and to ensure that Remote Workstations are protected and controlled using the same requirements that are applicable to CAs.
10.9	1/9/2025	CP Change to add changes required by the Federal Bridge. Clarifications related to Trust Agent role and Key Recovery Officials and to add requirements for Third Party Key Recovery Requestors.
10.10	10/1/2025	CP Change to add Federal Bridge requirements, make updates to reflect the for profit business, and make clarifying changes and Clerical Corrections
10.11	10/16/2025	Changes to update Section 10 Certificate Profiles to reflect new SHA384 CA.
10.12	4/10/2026	Changes to comply with Federal Bridge requirements and other clarifications.

Table of Contents

1. INTRODUCTION

This Certificate Policy (CP) defines multiple assurance levels for use by the TSCP Bridge Certification Authority (TBCA) to facilitate interoperability between the TBCA and other Entity PKI domains. The level of assurance refers to the strength of the binding between the public key and the individual whose subject name is cited in the certificate, the mechanisms used to control the use of the private key, and the security provided by the PKI itself.

The TBCA enables interoperability among Entity PKI domains in a peer-to-peer fashion. The TBCA issues certificates only to those CAs designated by the Entity operating that PKI (called "Principal CAs"). The TBCA may also issue certificates to individuals who operate the TBCA. The TBCA certificates issued to Principal CAs act as a conduit of trust.

Any use of or reference to this TBCA CP outside the purview of the TBCA is completely at the risk of using party. An Entity shall not assert the TBCA CP OIDs in any certificates the Entity CA issues, except in the *policyMappings* extension establishing an equivalency between a TBCA OID and an OID in the Entity CA's CP.

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

The terms and provisions of this TBCA CP shall be interpreted under and governed by applicable Delaware law.

1.1 OVERVIEW

1.1.1 Certificate Policy (CP)

TBCA certificates 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. The OID corresponds to a specific level of assurance established by this Certificate Policy (CP) which shall be available to Relying Parties. Each certificate issued by the TBCA will assert the appropriate level of assurance in the *certificatePolicies* extension.

1.1.2 Relationship between the CP & CPS

A CP states what assurance can be placed in a certificate issued by the CA. The Certification Practice Statement (CPS) states how the CA establishes that assurance. A CPS shall be more detailed than the CP with which it aligns.

1.1.3 Relationship between the TBCA CP and the Entity CP

The TPMA maps Entity CP(s) to one or more of the levels of assurance in the TBCA CP. The relationship between these CPs and the TBCA CP is asserted in CA certificates issued by the TBCA in the policyMappings extension.

1.1.4 Scope

The TBCA exists to facilitate trusted electronic business transactions across industry, State, and international boundaries. The generic term “entity” applies equally to organizations, Federal or otherwise, owning or operating PKI domains. As used in this CP, Entity PKI or Entity CA may refer to an organization’s PKI, a PKI provided by a commercial service, or a bridge CA serving a community of interest.

1.1.5 Interaction with PKIs External to TSCP, LLC

The TBCA will extend interoperability only when it is beneficial to the members of TSCP, LLC (TSCP) or governments who participate with TSCP.

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 Object Identifier (OID), to be asserted in certificates issued by the TBCA. Entity Principal CAs may assert these OIDs in policyMappings extensions of certificates issued to the TBCA. The TBCA policy OIDs are a sub-assignment of TSCP Private Enterprise Number (PEN) registered in the IANA PEN Registry. The PEN sub-assignment is allocated to TBCA policy OID as follows:

Table 1 - TBCA Certificate Policies

id-tscp OBJECT IDENTIFIER	1.3.6.1.4.1.38099
id-security OBJECT IDENTIFIER	id-tscp 1
id-pki	id-security 1
id-tscp-certificate-policies	id-pki 1
id-Basic	tscp-certificate-policies 0
id-Medium	tscp-certificate-policies 1
id-MediumHardware	tscp-certificate-policies 2
id-Medium-CBP	tscp-certificate-policies 3
id-MediumHardware-CBP	tscp-certificate-policies 4
id-PIVI	tscp-certificate-policies 5
id-PIVI-CardAuth	tscp-certificate-policies 6
id-PIVI-ContentSigning	tscp-certificate-policies 7
id-mediumDevice	tscp-certificate-policies 12

id-mediumDeviceHardware	tscp-certificate-policies 13

The requirements associated with the mediumDevice policy are identical to those defined for the Medium Assurance policy with the exception of identity proofing, re-key, and activation data. The requirements associated with the mediumDeviceHardware policy are identical to those defined for the Medium Hardware Assurance policy with the exception of identity proofing, re-key, and activation data. In this document, the term "device" is defined as a non-person entity, i.e., a hardware device or software application. The use of the mediumDevice and mediumDeviceHardware policies are restricted to devices and systems.

End-Entity certificates issued to devices shall assert policies mapped to TSCP Medium Device, Medium Device Hardware, or PIV-I Content Signing policies. All other policies defined in this document should be reserved for human subscribers when used in End-Entity certificates.

The requirements associated with an assurance level with a CBP suffix (e.g. id-Medium-CBP) are identical to those defined for the corresponding assurance level without the suffix (e.g. id-Medium) with the exception of personnel security requirements (see Section 5.3.1).

The requirements associated with the id-MediumHardware assurance level are identical to those defined for the id-Medium assurance level with the exception of subscriber cryptographic module requirements (see Section 6.2.1).

The requirements associated with the id-PIVI and id-PIVI-Content Signing assurance levels are identical to the id-MediumHardware assurance level except where specifically noted.

In addition, the id-PIVI-ContentSigning assurance level is reserved for certificates used by the Card Management System (CMS) to sign the PIV-I card security objects.

The TBCA may assert certificate policy OIDs not listed above in an Entity cross certificate, if requested by the Entity CA. These policy OIDs are called "pass-through" OIDs.

1.3 PKI ENTITIES

The following are roles relevant to the administration and operation of the TBCA.

1.3.1 PKI Authorities

1.3.1.1 TSCP LLC

TSCP LLC is Limited Liability Company registered in the State of Delaware and is led by its Chief Executive Officer. TSCP LLC. is ultimately accountable for its PKI bridging services.

1.3.1.2 Program Management Office (TPMO)

The TSCP PMO operates under the authority of TSCP's Chief Executive Officer. The TPMO is responsible for:

- Overseeing the activities of the TSCP Policy Management Authority (TPMA) and TSCP Operations Authority (TOA),

- Legally obligating TSCP, LLC. to relevant contracts, policies, and PKI Bridge Service Agreements (MTFSAs) or similar agreements with cross-certified Entities,
- Approving TBCA CPS, and
- Promoting the use of TSCP, LLC's federated PKI bridging services.

In particular, this CP was established under the authority of and with the approval of the TPMO.

1.3.1.3 TSCP Policy Management Authority (TPMA)

The TPMA is chartered by and under the authority of the TSCP PMO. The TPMA owns this policy and represents the interest of TSCP. The TPMA is responsible for:

- Authoring and maintaining this CP, including revisions,
- Authoring and maintaining the methodology for cross-certification,
- Accepting applications from Entities desiring to interoperate using the TBCA,
- Approving cross-certification of Entities, and
- After an Entity is authorized to cross-certify with the TBCA, ensuring continued conformance of that Entity with applicable requirements as a condition for allowing continued interoperability using the TBCA.

1.3.1.4 TSCP Policy Working Group (TPWG)

The TPWG provides policy coordination and analysis services in support of the TPMO, TPMA, and TOA. The TPWG is responsible for the following:

- Analyzing and reviewing the TBCA CPS and TBCA audit results,
- Analyzing change requests for this CP,
- Recommending CP Change requests to the TPMA, TPMO, and TOA,
- Performing analysis and coordination services according to the cross-certification methodology. The results of such services are reports and recommendations to the TPMA and TPMO who make approval decisions, and
- Performing analysis and coordination services for incident handling, disaster recovery, change control, and business continuity scenarios.

1.3.1.5 TSCP Operations Authority (TOA)

The TOA is the organization that operates and maintains the TBCA on behalf of TSCP LLC, according to this CP. The TSCP Operations Authority is led by TSCP's VP of Operations who is principally responsible for the proper operation of the TBCA.

1.3.1.6 Entity Certification Authority (Entity CA)

A CA that acts on behalf of an Entity and is under the operational control of an Entity. The term 'Entity CA' refers to the Entity PCA ~~as well as~~ and the Entity Subordinate CAs (SCAs) under the PCA that are cross-certified with the TSCP CA and come under the jurisdiction of a TSCP

MTFSA or similar agreement. The Entity may be an organization, corporation, or community of interest.

Entity CAs shall be responsible for all aspects of the issuance and management of certificates including:

- Control over the registration process,
- The identification and authentication process,
- The certificate manufacturing process,
- Publication of certificates,
- Revocation of certificates,
- Re-key of TBCA signing material, and
- Generation and destruction of CA signing keys.

CA and related applications (e.g., OCSP, CMS, and KRS) may be hosted on one or more System Software Layers. Operational and technical security controls including audit logging requirements specified in this CP apply to all System Software Layers, where applicable**.**

1.3.1.7 Entity Principal Certification Authority (PCA)

A Principal CA is an Entity CA within a PKI that has been designated to cross-certify directly with the TBCA (e.g., through the exchange of cross-certificates). The Principal CA issues either end-entity certificates, or CA certificates to other Entity or external party CAs, or both. Where the Entity operates a hierarchical PKI, the Principal CA is typically the Entity Root CA. Where the Entity operates a mesh PKI, the Principal CA may be any CA designated by the Entity for cross-certification with the TBCA.

The PCA shall be responsible for all aspects of issuance and management of certificates as specified in 1.3.1.6 above.

It should be noted that an Entity may request that the TBCA cross-certify with more than one CA within the Entity; that is, an Entity may have more than one Principal CA. Additionally, this CP may refer to CAs that are "subordinate" to the Principal CA. The use of the term "subordinate CA" shall encompass any CA under the control of the Entity that has a certificate issued to it by the Entity Principal CA or any CA subordinate to the Principal CA, whether or not the Entity employs a hierarchical or other PKI architecture.

The Entity shall ensure that no CA under its PKI shall have more than one trust path to the FBCA (regardless of path validation results).

1.3.1.8 Entity PKI Policy Management Authority (PMA)

Entity PKIs (including other Bridges) that are cross certified with the TBCA shall identify an individual or group that is responsible for maintaining the entity PKI CP and for ensuring that all Entity PKI components (e.g., CAs, CSSs, CMSs, RAs) are operated in compliance with the

entity PKI CP. This body is referred to as Entity PKI Policy Management Authority (PMA) within this CP.

The Entity PKI PMA shall be responsible for notifying the TPMA of any change to the infrastructure that has the potential to affect the TSCP Bridge operational environment at least two weeks and a day prior to implementation; all new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the change shall be provided to the TPMA within 24 hours following implementation. The notice period will begin to run upon written acknowledgement of the TPMA.

1.3.1.9 TSCP Bridge Certification Authority (TBCA)

The TBCA is the CA operated by the TOA that is authorized by the TPMA and TPMO to create, sign, and issue public key certificates to Principal CAs. As operated by the TOA, the TBCA 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 TBCA signing material, and
- Generation and destruction of CA signing keys.

1.3.1.10 Certificate Status Servers (CSS)

PKIs may optionally include an authority that provides status information about certificates on behalf of a CA through online transactions. In particular, PKIs may include OCSP responders to provide online status information. Such an authority is termed as a Certificate Status Server (CSS). Where the CSS is identified in certificates as an authoritative source for revocation information, the operations of that authority are considered within the scope of this CP. Examples of CSS that fall within the scope of this CP include:

- OCSP servers that are identified in the authority information access (AIA) extension, and
- SCVP servers that validate paths or perform certificate status checking.

Examples of CSS that do not fall within the scope of this CP include:

- OCSP servers that are locally trusted, as described in RFC 6960, and
- SCVP servers that develop certificate paths but do not perform validation or certificate status checking.

OCSP responders that solely repeat responses from other OCSP responders shall meet the security requirements of a Repository rather than those of a CSS.

Entity CAs that issue certificates at the id-PIVI, id-PIVI-CardAuth, and id-PIVI-ContentSigning assurance levels must provide an OCSP responder.

OCSP servers covered by this policy shall be issued and use CA-delegated certificates.

1.3.2 Registration Authority (RA)

An RA is an Entity authorized by the CA to oversee the registration process, and collect-and verify Subscriber identity and information for inclusion in the Subscriber's public key certificate.

Entity CAs designate their own RAs. The requirements for RAs in Entity PKIs are set forth elsewhere in this document.

1.3.3 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 only associated with the id-PIVI, id-PIVI-CardAuth, and id-PIVI-ContentSigning assurance levels. Entity CAs issuing such 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 assert the id-PIVI or id-PIVI-CardAuth assurance level.

1.3.4 Key Recovery Authorities

For Entities that have implemented Key Recovery, the applicable requirements for physical, personnel, and procedural security controls, technical security controls, and Compliance Audit apply as follows:

• CA requirements apply to the Key Escrow Database (KED) and to the Data Decryption Server (DDS),

• RA requirements apply to the Key Recovery Agent (KRA) and KRA automated systems. and

• RA requirements apply to the Key Recovery Official (KRO) and KRO automated systems, when the KRO has privileged access to the KED.

1.3.4.1 Key Escrow Database

The KED 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 KRAs or self-recovery by a current subscriber. Section 5.2.1.8 contains the description of Trusted Roles required to operate the KED.

1.3.4.2 Data Decryption Server

A DDS is an automated system that has the capability to obtain subscriber private keys from the KED or another DDS 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 has access to escrowed key management keys and must meet all security requirements of the KED as outlined in this policy.

Implementation of a DDS is optional based upon Entity operational requirements.

1.3.4.3 Key Recovery Agent

A KRA is an individual who is authorized, as specified in the applicable KRPS or CPS, to recover an escrowed key. A KRA sends the recovered key to the KRO or directly to the Requestor. A KRA has high level, sensitive access to the KED and the KRA is considered a Trusted Role (see Section 5.2.1). As a KRA can recover large numbers of keys, the number and location of KRAs should be closely controlled.

A KRA performs the following functions:

- Confirms the validity and completeness of requests,
- Recovers copies of escrowed keys, and
- Sends the recovered key to either the KRO or to the Requestor, as provided in Section 4.12.1.2.1.

A KRA may additionally conduct requestor identity verification and authorization validation when a KRO is not used.

1.3.4.4 Key Recovery Official

A KRO may be appointed by an organization to support identity verification and authorization validation tasks.

1.3.4.5 Key Recovery Requestor

A Requestor is an individual or DDS that requests the recovery of a decryption private key. A Requestor may be the Subscriber or a third-party (e.g., supervisor, corporate officer, or law enforcement officer) authorized to request recovery of a Subscriber's escrowed key on behalf of the Subscriber or on behalf of the Entity. Any individual who can demonstrate verifiable authority and a need to obtain a recovered key may be considered a Requestor.

1.3.4.6 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 Issuing Entity (i.e., the Entity on behalf of which the CA issues certificates to Subscribers).

1.3.4.7 External Third-Party Requestor

An External Third-Party Requestor is someone (e.g., investigator) outside the Issuing Entity with a court order or other legal instrument to obtain the decryption private key of the Subscriber.

1.3.5 Subscribers

A Subscriber is the user to whom or the device to which a certificate is issued. TBCA Subscribers include only TOA personnel and applicable devices. Where certificates are issued to devices, the entity must have a human sponsor who is responsible for carrying out Subscriber duties. Note that CAs are sometimes technically considered "subscribers" in a PKI. However, the term "Subscriber" as used in this document does not refer to CAs. There is a subset of Human Subscribers who may be issued role-based certificates. These certificates identify a specific role on behalf of which the Subscriber is authorized to act rather than the Subscriber's name. See

Section 3.2.3.4 for more information on how and under what conditions role-based certificates may be issued to Human Subscribers.

1.3.6 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 will be indicated in the certificate. Affiliated Organizations are responsible for verifying the affiliation at the time of certificate application and requesting revocation of the certificate if the affiliation is no longer valid.

1.3.7 Relying Parties

A Relying Party uses a Subscriber's certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the Subscriber. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. 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.

This CP makes no assumptions or limitations regarding the identity of Relying Parties. While Relying Parties are generally Subscribers, Relying Parties are not required to have an established relationship with the TBCA or an Entity CA.

1.3.8 Other Participants

1.3.8.1 Trusted Agent

A Trusted Agent is the entity authorized by the PKI to act on its behalf to collect and verify a Subscriber's 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 is not a Trusted Role as described in Section 5, but acts in a sensitive position with access to Subscriber information. The PKI shall document Trusted Agent authorization requirements, which at a minimum shall include trustworthiness, vetting, and training, or appointments (e.g., notary public).

A Trusted Agent shall not have access to the CA to enter or approve Subscriber information.

1.3.8.2 Additional Participants

The TBCA and Entity CAs may require the services of other security, community, auditors, and application authorities. If required, the TBCA or Entity CPS shall identify the parties, define the services, and designate the mechanisms used to support these services.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

The sensitivity of the information processed or protected using certificates issued by TBCA or an Entity CA will vary significantly. Relying Parties 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 done by each Relying Party for its application and is not controlled by this CP.

To provide sufficient granularity, this CP specifies security requirements at multiple levels of assurance. The following table provides a brief description of the appropriate uses for certificates at each level of assurance defined in this CP. These descriptions are intended as guidance and are not binding.

Assurance Level	Appropriate Certificate Uses
id-Basic	This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level that users are not likely to be malicious.
id-Medium id-Medium-CBP id-MediumDevice	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.
id-PIVI-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.

Assurance Level	Appropriate Certificate Uses
id-MediumHardware id-MediumHardware-CBP id-MediumDeviceHardware id-PIVI id-PIVI-ContentSigning	This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

1.4.2 Prohibited Certificate Uses

No stipulation.

1.5 POLICY ADMINISTRATION

1.5.1 Organization administering the document

The TPMA 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 TPMA, who can be reached at pma@tscpllc.com.

1.5.3 Person Determining Certification Practices Statement Suitability for the Policy

The Certification Practices Statement must conform to the corresponding Certificate Policy. The TPMO is responsible for asserting whether the TBCA CPS conforms to this CP. Entities must designate the person or organization that asserts that their CPS(s) conforms to their CP(s).

In each case, the determination of suitability shall also be based on an external independent auditor's results and recommendations. See Section 8 for further details.

1.5.4 CPS Approval Procedures

The TOA shall prepare and submit the TBCA CPS to the TPMO for approval. If rejected, the identified discrepancies shall be resolved and the TBCA CPS shall be resubmitted to the TPMO.

Entity CAs shall specify their CPS approval procedures in their CP.

1.5.5 Waivers

Waivers shall not be issued. Instead, CP and/or CPS changes shall be made, or remediation activities shall be scheduled and implemented.

1.6 DEFINITIONS AND ACRONYMS

See Sections 14 and 15 of the CP.

2. PUBLICATION & REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

The TOA shall operate repositories to support TBCA operations.

Entity PKIs are responsible for operation of repositories to support their PKI operations.

Entities who cross-certify with the TBCA shall ensure interoperability with the TBCA repository.

2.1.1 Repository Obligations

CAs may use a variety of mechanisms for posting information into a Repository as required by this CP. These mechanisms at a minimum shall include:

- Web Server System accessible through the Hypertext Transport Protocol (HTTP);
- Availability of the information as required by the certificate information posting and retrieval stipulations of this CP; and
- Access control and communication mechanisms when needed to protect repository information as described in later sections.

Optionally, an X.500 Directory Server System may also function as a Repository to complement a Web Server System. In such cases, the Repository shall be accessible through the Lightweight Directory Access Protocol (LDAP) and meet the availability and access control requirements as stated above.

In cases where a CA has multiple Repositories, the following rule shall apply to Repository references within certificates:

- All HTTP URI shall appear before LDAP URI.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 Publication of Certificates and Certificate Status

With the exception of self-signed certificates, CA and End Entity certificates shall only contain valid Uniform Resource Identifiers (URIs) that are accessible by relying parties in the Authority Information Access (AIA) extension. This URI must be asserted in all valid certificates issued by the Subject CA.

The TOA shall publish all CA certificates issued by or to the TBCA and all CRLs issued by the TBCA in the TBCA repository.

The repository shall:

● contain a binary (DER encoded) certs-only Cryptographic Message Syntax file that has an extension of .p7c and a http response content type header of ‘application/pkcs7-mime’, or

● contain a single binary (DER encoded) certificate that has an extension of .cer and a http response content type header of ‘application/pkix-cert’.

The certs-only Cryptographic Message Syntax format is preferred as it allows flexibility for inclusion of multiple certificates.

At a minimum, the Entity repositories shall contain all CA certificates issued by or to the Entity PKI and CRLs issued by the Entity PKI.

For the TBCA, mechanisms and procedures shall be designed to ensure CA certificates and CRLs are available for retrieval 24 hours a day, 7 days a week, with a minimum of 99% availability overall per year. Further, the repository shall be designed and implemented to limit scheduled down-time to 0.5% annually.

Entity CAs being considered for cross certification shall be designed to comply with a similar requirement.

2.2.2 Publication of CA Information

The TOA shall publish information concerning the TBCA necessary to support its use and operation. The TBCA CP shall be publicly available on the TSCP website (see http://www.tscpllc.com).

Entities who cross-certify with the TBCA shall meet these requirements and may elect to publish a redacted version of their CPS.

2.2.3 Interoperability

Where certificates and CRLs are published in a X.500 Directory Server System, standards-based schemas for directory objects and attributes are required and shall be consistent with the Repository Profile. See Section 11 for more details.

2.3 FREQUENCY OF PUBLICATION

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

Certificates and certificate status information, including pre-generated OCSP responses, if implemented, shall be published as specified in sections 4.4.2 , 4.9.7, 4.9.8, 0, and 4.9.10.

2.4 ACCESS CONTROLS ON REPOSITORIES

The TOA and Entity CAs shall protect any repository information not intended for public dissemination or modification.

Certificates and certificate status information in the TBCA repository shall be publicly available through the Internet.

Direct and/or remote access to information in Entity CA repositories shall be determined by the Entity pursuant to the rules and statutes that apply to that entity. Certificates and certificate status information in the Entity repository should be publicly available through the Internet wherever

reasonable. At a minimum, the Entity repositories shall make CA certificates and CRLs issued by the Entity PKI and CA certificates issued to the Entity PKI available to Relying Parties on the Internet.

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

3. IDENTIFICATION & AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

The TBCA shall only generate and sign certificates that contain a non-null subject Distinguished Name (DN). Certificates issued by the TBCA may also include alternative name forms.

For Entity CAs, the following rules apply:

- All certificates shall include a non-NULL subject DN and a non-NULL issuer DN;
- The Entity CP shall define the permitted Base DN(s);
- Role-based and group certificates may be issued under any human subscriber policy except for PIV-I;
- The subjectName DN in a group certificate shall not imply that the subject is a single individual (e.g., by including a human name form);
- The DN may be formed as either internet domain component or geo-political forms;
- Certificates may include Subject Alternative Names if marked non-critical; and
- A Device subject name shall be a unique name for the Device and shall not take the form of a Human Subscriber name.

Certificates shall indicate whether or not the Subscriber is associated with an Affiliated Organization by taking one of the following forms:

For certificates with an Affiliated Organization	Affiliated Organization name is present in the distinguished name as an organization (o), organizational unit (ou), or domain component (dc) value. *For id-PIVI Hardware certificates, the affiliated organization name shall be present in the last organizational unit attribute in the distinguished name as follows: cn=Subscriber's full name, ou=Affiliated Organization Name, {Base DN} *For PIVI cardAuth certificates: serial number=UUID, ou=Affiliated Organization Name, {Base DN}
For certificates with no Affiliated Organization	"Unaffiliated" is present in the last organizational unit attribute in the distinguished name Entity CA name is present in the organizational unit attribute in the distinguished name.

	For PIVI Hardware certificates with no Affiliated Organization: cn=Subscriber's full mane, ou=Unaffiliated, ou=Entity CA's Name {Base DN} For PIVI cardAuth certificates with no Affiliated Organization: serial number=UUID, ou=Entity CA's Name {Base DN}

*These requirement shall not apply to CAs that issue PIV-I certificates to a single organization that is designated in the CA issuer name.

Certificates at the id-PIVI-ContentSigning assurance level shall clearly indicate the organization administering the CMS.

Certificates at the id-PIVI-CardAuth assurance level shall not contain the subscriber's common name in the subject distinguished name. Instead of a common name attribute, the distinguished name shall use the serialNumber attribute with a value that is unique to the card. PIV-I CardAuth certificates shall not include any other name in the subject alternative name extension.

Subscriber certificates that contain id-kp-emailProtection in the EKU shall include a subject alternative name extension that includes a rfc822Name.

For PIVI Hardware and PIVI-CardAuth, the identifier shall be encoded using the UUID string representation defined in Section 3 of RFC 4122 (e.g., "f81d4fae-7dec-11d0-a765-00a0c91e6bf6").

For Device Subscriber certificates that assert serverAuth in the Extended Key Usage, wildcard domain names are permitted in the dNSName value only if all sub-domains covered by the wildcard fall within the same application, cloud services, or system boundary within the scope of the sponsoring organization.

3.1.2 Need for Names to Be Meaningful

Names used in the certificates issued by the TBCA and/or Entity CAs must identify the person or object to which they are assigned.

When DNs are used, the directory information tree must accurately reflect organizational structures.

When DNs are used, the common name must respect name space uniqueness requirements, must not be misleading, and shall be easily understood by humans. For people, this will typically be a legal name. For equipment, this may be an IP address, fully-qualified domain name, URL, model name and serial number, or an application process. This does not preclude the use of pseudonymous certificates as defined in Section 3.1.3.

The subject name in CA certificates shall match the issuer name in the certificates issued by the CA, as required by RFC 5280.

When User Principal Names (UPN) are used, they must be unique and accurately reflect organizational structures.

Name space shall be limited as specified in Section 7.1.5.

3.1.3 Anonymity or Pseudonymity of Subscribers

CA certificates issued by the TBCA or Entity CAs shall not contain anonymous or pseudonymous identities.

DNs in End Entity certificates issued by Entity CAs may contain a pseudonym (such as a large number) as long as name space uniqueness requirements are met and the pseudonym is reversible.

CAs may issue role-based certificates that identify subjects by their organizational roles. The identified "role" shall meet the name space uniqueness requirements.

3.1.4 Rules for Interpreting Various Name Forms

The TPMO is responsible for controlling name space for the TBCA. Entity CAs must specify the party responsible and accountable for controlling its name space within its CP.

Rules for interpreting name forms shall be defined in certificate profiles located within a CP directly (e.g., Section 10) or included in the CP through reference.

Rules for interpreting email addresses are specified in RFC 5322.

Rules for interpreting PIV-I certificate UUID names are specified in RFC 4122.

3.1.5 Uniqueness of Names

Name uniqueness must be enforced by the TBCA and Entity CAs for the name space for which they have respectively been authorized.

The TOA is responsible for ensuring name uniqueness in certificates issued by the TBCA.

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

Name uniqueness is not violated when multiple certificates are issued to the same entity.

Practice Note: Relying party applications may assume a one-to-one relationship between a certificate and a distinguished name / subject alternative name. However, such applications may not be interoperable with PKIs that issue multiple certificates to the same entity thereby creating a one-to-many relationship if only the distinguished name and/or subject alternative names are verified by the Relying Party application.

The applicable CPS shall specify how name uniqueness will be ensured, including in circumstances where a Person or device has the same name as a Person or device who has been issued a certificate in the past. This includes circumstances where a Person or device has left the organization at the time the next Person or device applies for a certificate thereby guaranteeing

uniqueness of names over time.

3.1.6 Recognition, Authentication, & Role of Trademarks

No stipulation.

3.1.7 Name Claim Dispute Resolution

The TPMO in consultation with the TPMA shall resolve any name collisions or disputes regarding TBCA-issued certificates brought to its attention. The TBCA will not knowingly use trademarks in names unless the subject has the right to use that name.

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 that corresponds to the public key in the certificate request.

Practice Note: For signature keys, this may be done by the entity using its private key to sign a value and providing that value to the TBCA or Entity CA. The TBCA or Entity CA shall then validate the signature using the party's public key. The TPMA may allow other mechanisms that are at least as secure as those cited here.

In the case where a key is generated by the CA or RA either (1) directly on the party's hardware or software token; or (2) in a key generator that benignly transfers the key to the party's token, then proof of possession is not required.

3.2.2 Authentication of Organization Identity

Requests for TBCA, Entity CA, or Subscriber certificates in the name of an Affiliated Organization shall include the organization name, address, and documentation of the existence of the organization.

The TOA or Entity CA, as applicable, shall verify the information provided, the authenticity of the requesting representative, and the representative's authorization to act in the name of the organization.

3.2.3 Authentication of Individual Identity

Certificates at the id-PIVI assurance level shall only be issued to human subscribers.

Successful authentication binds together the process documentation, public key, applicant identity information, and applicant.

In addition to the processes described in this Section, Subscriber certificates may be issued based on an electronically authenticated request, using a valid signature or authentication certificate, and the associated private key, with the following conditions:

- The assurance level of the new certificate shall be at the same or lower assurance level as the certificate used to authenticate the request;
- Identity information in the new certificate shall match the identity information from the signature or authentication certificate;
- 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; and
- The next required initial identity authentication date remains unchanged.

3.2.3.1 Initial Identity Proofing of Human Subscribers

For the basic level of assurance, identity proofing may be in-person or may be performed remotely as provided in the table below. For all levels of assurance other than basic, identity proofing shall be performed in-person before a CA, RA, Trusted Agent, or an entity certified by a Government Entity as being authorized to confirm identities, as further clarified in the table below.

The applicant shall present suitable identity source documents. Suitable identity source documents vary according to level of assurance as follows:

Assurance Level	Identification Requirements
id-Basic	Identity may be established by in-person proofing before a Registration Authority or Trusted Agent; or remotely by verifying information provided by applicant including ID number and account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases that confirms: name, date of birth, address and other personal information in records are consistent with the application and sufficient to identify a unique individual. Address confirmation is achieved either by a) issuing credentials in a manner that confirms the address of record supplied by the applicant; or b) issuing credentials in a manner that confirms the ability of the applicant to receive telephone communications at a number associated with the applicant in records, while recording the applicant's voice.
id-PIVI id-PIVI-CardAuth	• Two unexpired identity source documents in original form • Identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, Employment Eligibility Verification • At least one document shall be a valid State or Federal Government-issued picture identification (ID)

All other assurance levels	• Either: 1) One unexpired National Government-issued or REAL ID Act issued Picture ID, or 2) Two Non-Federal Government IDs, one of which shall be a photo ID.

The TOA or Entity CA, and/or associated RAs shall ensure that the applicant's identity information is verified in accordance with the process established by the applicable CP and CPS.

Process information shall depend upon the certificate level of assurance and shall be addressed in the TBCA or Entity CPS. The documentation and authentication requirements vary depending upon the level of assurance. The TOA, Entity CAs or RAs, as applicable, shall record the process information set forth below for issuance of each certificate:

- The identity of the person performing the identification;
- A signed declaration by that person that he or she verified the identity of the applicant as required 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;
- If in-person or supervised remote[1] identity proofing is done, unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s), except where capturing such information violates local law, in which case, the TPMA will consider and approve other comparable procedures for collecting identity evidence;
- 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

[1] The minimum requirements associated with supervised remote identity proofing are described in NIST SP 800-63A, *Digital Identity Guidelines: Enrollment and Identity Proofing*, Section 5.3.3. The supervised remote process for PIV-I policies must have the capability of capturing an approved biometric.

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.

For certificates at the id-PIVI or id-PIVI-cardAuth assurance levels, the same requirements apply with the following modifications:

- Antecedent relationship method of identity proofing shall not be used;
- Identity proofing shall only be performed by a CA, RA, Trusted Agent, or parties solely authorized by Federal or State Entities. The certified entity shall forward the information collected from the applicant directly to the RA in a secure manner;
- An electronic facial image used for printing facial image on the card, as well as for performing visual authentication during card usage shall be collected. A new facial image shall be collected each time a card is issued;
- Two electronic fingerprints shall be collected to be stored on the card for automated authentication during card usage; and
- The principle of separation of duties shall be enforced such that the ability to identity proof, register, approve, and issue a credential requires at least two trusted roles.

3.2.3.2 Human Subscriber Identity Proofing via Antecedent Relationship

The following requirements shall apply when human subscriber identity is verified using antecedent relationship with the sponsoring organization that has applied to have the applicant issued a certificate:

1. The sponsoring organization's application shall contain a description of the relationship with the applicant, including a description of the initial identity proofing or qualifications and the on-going relationship, as well as the initial contact information for the applicant (e.g., name, email address, phone number, sponsoring organization);

2. The verifier shall use the information provided by the sponsoring organization to contact the applicant;

3. The applicant shall personally appear before a verifier (usually a Trusted Agent);

4. The applicant and the verifier shall have an established working[2] relationship with the sponsoring organization. The relationship shall be sufficient to enable the verifier to, with a high degree of certainty, verify that the applicant is the same person that was identity proofed. An example to meet this requirement is when the same company employs the

[2] An example of "established working relationship" is the person is employed by the sponsoring organization. Another example of "established working relationship" is the person is consultant to the sponsoring organization or is employed by a contractor of the sponsoring organization.

applicant and Trusted Agent and the company badge forms the basis for the applicant authentication;

5. The applicant shall present a valid sponsoring organization-issued photo ID. This photo ID shall have been issued based on previously performed in-person identity proofing using one valid National Government-issued Picture ID, or two valid non-National Government IDs, one of which shall be a recent photo ID (e.g., Driver's License);

6. The verifier shall record the following:

    a. Their own identity;
    b. Unique identifying number from the Identifier (ID) of the verifier;
    c. The date and time of the antecedent in-person identity proofing event;

    d. Unique identifying number from the applicant's sponsoring organization-issued photo ID;
    e. Date and time of the identity verification; and
    f. Date and time of sponsoring organization-issued photo ID, if applicable.

7. The verifier shall obtain the historical artifacts from the antecedent event, if any;

8. The verifier shall sign a declaration that he or she verified the identity of the applicant 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;

9. The applicant shall sign a declaration of identity using a handwritten signature or appropriate digital signature. This declaration shall be signed in the presence of the verifier; and

10. The identity of the entity providing confirmation of the antecedent identity proofing process shall be recorded and kept as part of the auditable record.

3.2.3.3 Human Subscriber Re-Proofing 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 according to the re-proofing provisions in this Section.

The re-proofing provisions are the same as those followed for the initial identity proofing (Section 3.2.3.1 or Section 3.2.3.2) with the following modifications:

- The validity period of the certificates issued using this process shall not exceed the identity-reproofing requirements in Section 3.3.1;

- Only one National Government-Issued Photo ID or non-National Government issued Photo ID (e.g., Driver's License, Passport) is required; and

- As applicable, 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. For certificates at the id-PIVI or id-PIVI-cardAuth assurance levels, a biometric match is mandatory.

Practice Note: As biometric authentication accuracy degrades with the time elapsed since initial collection, Entity PKIs may desire to update biometric(s) after a match has been made.

3.2.3.4 Identity Proofing Human Subscribers For Role-based Certificates

Human subscribers may be issued role-based certificates. These certificates will identify a specific role on behalf of which the subscriber is authorized to act rather than the subscriber's name. The role-based certificate can be used in situations where proof of delivery and assurance that the content of any message has not been changed in transit is required. The subscriber must hold an individual certificate in their own name issued by the same CA at the same or higher assurance level as the role-based certificate. A specific role may be identified in certificates issued to multiple subscribers (i.e. there may be four individuals carrying a certificate issued in the role of "*Chief Information Officer*" however, each of the four individual certificates will carry unique keys and certificate identifiers). In this situation, the signature key pair will be unique to each individual role-based certificate and the encryption key pair and encryption certificate may be shared. Role-based certificates shall be issued to individual subscribers and protected in the same manner as individual certificates.

The CA or RA shall validate that the individual either holds the role they are sponsored for or has been delegated the authority to sign on behalf of the role.

Practice Note: When determining whether a role-based certificate is warranted, consider whether the role carries inherent authority beyond the job title. Role-based 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: "*Watch Commander, Task Force 1*".

The procedures for issuing role-based tokens must comply with all other stipulations of this CP (e.g., 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 TOA and/or Entity CAs shall record the information identified in Section 3.2.3.1 for a sponsor associated with the role before issuing a role-based certificate. The sponsor must hold an individual certificate in his/her own name issued by the same CA at the same or higher assurance level as the role-based certificate.

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

- Sponsoring individuals for a role certificate;
- Recovering the private decryption key;
- Revoking individual role certificates;
- Maintaining a list of individuals who are assigned the role; and
- Maintaining a list of individuals who have possession or use of the private decryption key.

3.2.3.5 Authentication of Devices

Computing and communications devices (routers, firewalls, servers, etc.) may be named as certificate subjects. In such cases, the device must have a human sponsor. The sponsor is responsible for the security of the device private key and for providing the following registration information:

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

Aircraft, aircraft components, and aircraft on-board systems may be named as certificate subjects. In such cases, all of the requirements above apply and the sponsor shall also provide the following additional registration information:

- Relevant Aircraft National Registration Paperwork.

These certificates shall be issued only to devices under the issuing entity's control (i.e., require registration and validation that meets all issuing agency's requirements, as well as requiring re-validation prior to being re-issued).

Practice Note: An entity can issue to organizations not controlled or related to the entity's organization i.e. a different company.

In the case a human sponsor is changed, the new sponsor shall review the status of each device under his/her sponsorship to ensure it is still authorized to receive certificates. The CPS shall describe procedures to ensure that certificate accountability is maintained.

The registration information 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); or
- In person or supervised remote registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of Section 3.2.3.1.

3.2.4 Non-verified Subscriber Information

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

3.2.5 Validation of Authority

For cross-certification, the CA shall validate the requestor's authorization to act in the name of the organization.

Approval from the PMA of the organization issuing a CA certificate shall be obtained prior to issuing such certificate.

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

The TPMO and TPMA shall determine the criteria for cross-certification with the TBCA and shall approve a cross-certification criteria and methodology. Such methodology shall include the following verifications:

- CP-to-CP mapping has completed and found the CPs to be equivalent;
- PKI has successfully passed a compliance audit (see section 8 of this CP);
- Verification that Certificate Profiles and Certificates are compliant with the applicable CP;
- Verification that Certificate Status (e.g. CRL, OCSP) are compliant with the applicable CP; and
- Verification that CA certificates and Certificate Status information are published and available for Relying Parties.

Under no circumstance shall any certificate have more than one intentional trust path to the FBCA, irrespective of extension processing.

NOTE: Multiple trust paths created as a result of Certificate renewal or CA rekey do not violate the single trust path requirement.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-key

For a routine re-key, a CA shall be authenticated through use of a private key and corresponding valid certificate or one of the initial identity proofing processes described in Section 3.2.3.1 and 3.2.3.2. If it has been more than three years since a CA was identified as required in Section 3.2, identity shall be re-established through the initial identity proofing process.

Subscribers shall be authenticated through the use of the current signature key or one of the initial identity proofing processes describe in Section 3.2.3.1 and 3.2.3.2. If it has been more than nine years since the Subscriber was identified as required in Section 3.2, identity shall be re-established through the initial identity proofing process.

When current private key and corresponding valid certificate is used for identification and authentication purposes, the life of the new certificate shall not exceed the initial identity-proofing times specified in the paragraphs 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

After a certificate has been revoked, other than during a renewal, update, or to replace a lost/stolen/damaged credential, the Subscriber is required to go through the initial registration processes described in Section 3.2.3 to obtain a new certificate unless the Subscriber can be authenticated with a non-revoked certificate of equal or higher assurance issued from the same CA.

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 public key, regardless of whether the associated private key has been compromised.

3.5 IDENTIFICATION AND AUTHENTICATION FOR KEY RECOVERY REQUESTS

This section is applicable only for those Entity CAs that support key escrow and recovery of encryption private keys.

3.5.1 KRA Authentication

The KRA shall authenticate to the KED or DDS directly or using a public key certificate issued by the Entity's CA. When a public key certificate is used, it shall be on a FIPS 140 level 2 or higher validated hardware cryptographic module. The assurance level of the certificate shall be the same or greater than that of the certificate whose corresponding private key is being recovered.

3.5.2 KRO Authentication

The KRO shall authenticate to the KRA using a public key certificate issued by the Entity's CA. The assurance level of the certificate shall be the same or greater than that of the certificate whose corresponding private key is being recovered.

3.5.3 Subscriber Authentication

The Subscriber identity shall be established as specified in Section 3.3.1 above. Alternatively, if the authentication cannot be verified using the public key certificates issued by the associated PKI and for at least the given certificate policy assurance level, then the identity validation can use the steps outlined in Section 3.2.3.1.

For automated self-recovery, the Subscriber shall be authenticated to the KED using a valid public key certificate. The assurance level of the Subscriber certificate shall be equal to or greater than that of the certificate whose corresponding private key is being recovered.

3.5.4 Third-Party Requestor Authentication

The KRA or KRO shall verify the identity and authorization of the Requestor prior to initiating the key recovery request.

Third-Party Requestor identity authentication shall be commensurate with the assurance level of the certificate associated with the key being recovered. Identity shall be established using one of the following methods:

- Procedures specified in Section 3.2.3 for authentication of an individual identity during initial registration for the specified certificate policy assurance level (an assurance level equal to or greater than the assurance level of the certificate whose corresponding private key is being recovered); or
- Certificate-based authentication (e.g., digitally signed e-mail or client-authenticated Transport Layer Security (TLS)) that can be verified using current, valid (i.e., un-revoked) public key certificates at the requested certificate policy assurance level (an assurance level equal to or greater than the assurance level of the certificate whose corresponding private key is being recovered).

3.5.5 Data Decryption Server Authentication

The DDS shall authenticate to the KED directly using a public key certificate issued by the PKI. The assurance level of the certificate must be the same or greater than that of the highest assurance level encryption certificates issued by the PKI.

4. CERTIFICATE LIFE-CYCLE

Certificates and corresponding private keys must be managed safely at their initial creation through their full life-cycle.

4.1 APPLICATION

This section specifies requirements for initial application for certificate issuance.

The Certificate application process shall provide adequate information to:

- Establish the Applicant's authorization by the sponsoring organization to obtain a certificate;
- Establish and record the identity of the Applicant (per Section 3.2);
- Obtain the Applicant's public key and verify the Applicant's possession of the private key; and
- Verify the information included in the certificate.

For the TBCA, Entities seeking to cross-certify with the TBCA shall fulfill the requirements as specified in Section 3.2.6 and the applicable provisions of the following sections.

For Entity CA, the Entity PMA shall establish and publish its criteria and procedures describing how other Entities may apply for and receive a cross-certificate, how CA may subordinate, and how Subscribers may apply for certificate(s).

4.1.1 Submission of Certificate Application

For the TBCA, the certificate application shall be submitted to the TPMA by an authorized representative of the Entity CA.

For Entity CAs, their CP shall define submission processes for CAs and Subscribers.

4.1.2 Enrollment Process and Responsibilities

Entity CAs applying for cross-certification are responsible for providing accurate information in their certificate applications. Upon issuance the TBCA shall manually check the certificate to ensure each field and extension is properly populated with the correct information before the certificate is delivered to the Entity.

Subscribers shall be responsible for providing accurate information in their certificate applications.

If databases or other sources are used to confirm Subscriber attributes, the sources and associated information sent to a CA require:

- An auditable chain of custody for information obtained through one or more information sources; and
- All data received is protected and securely exchanged in a confidential

and tamper evident manner and protected from unauthorized access.

Entity CA CP shall describe the enrollment process and responsibilities for its cross-certified and subordinate CAs and Subscribers.

All communications among PKI authorities materially supporting the certificate application and issuance process shall be authenticated and protected from modification. Any electronic communication of shared secrets must be protected, and out-of-band communications shall protect the confidentiality and integrity of the data.

4.2 CERTIFICATE APPLICATION PROCESSING

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

4.2.1 Performing Identification and Authentication Functions

For the TBCA, the identification and authentication of the applicant shall be performed by the TOA.

For Entity CAs, the identification and authentication of the Subscriber must meet the requirements specified for Subscriber authentication as specified in Sections 3.2, 3.3, and 3.4 of this CP. The Entity CP must identify the components of the Entity PKI (e.g., CA or RA) that are responsible for authenticating the Subscriber's identity in each case.

Before the issuance process completes, a Subscriber shall be required to sign a Subscriber agreement which includes the Subscriber's obligation to protect the private key and only use the certificate and private key for authorized purposes.

4.2.2 Approval or Rejection of Certificate Applications

For the TBCA, the TPMA may approve or reject a certificate application. See Section 1.3.1.3.

For Entity CAs, the applicable CPS shall define the organization that may accept or reject a certificate application.

4.2.3 Time to Process Certificate Applications

Individual Identity shall be confirmed no more than 30 days before initial certificate issuance.

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 corresponding 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 applicable CP and the corresponding CPS has been met.

While the Subscriber may do most of the data entry, 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 trusted 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, personnel controls, cryptographic security controls, computer security controls, and network security controls specified for the RA elsewhere in the applicable CP.

4.3.1 CA Actions during Certificate Issuance

The CA/RA shall verify the source of a certificate request before issuance. This includes verification of the following:

- The identity of the requestor;
- The authority of the requestor and the integrity of the information in the certificate request; and
- The attribute information received from the Subscriber before inclusion in a certificate.

The CA shall sign a certificate only after all verifications are completed and all requirements specified in the CP have been met.

CA certificates shall be checked to ensure that all fields and extensions are properly populated. After generation, verification, and acceptance, the CA certificates shall be posted in the CA repository system.

4.3.2 Notification to Subscriber of Certificate Issuance

CAs (or RA) shall notify the applicant (CA or Subscriber) of certificate issuance.

For PIV-I, Entity CAs must inform the Subscriber of the creation of a certificate and make the certificate available to the Subscriber.

4.4 CERTIFICATE ACCEPTANCE

Before a Subscriber can make effective use of its private key, a PKI Authority shall convey to the Subscriber its responsibilities as defined in Section 9.6.3.

4.4.1 Conduct constituting certificate acceptance

For the TBCA, conduct constituting acceptance shall be defined in the MTFSA between the TBCA and the cross-certifying Entity CA.

For Entity CA, conduct constituting acceptance shall be defined in the Entity's CP.

4.4.2 Publication of the Certificate by the CA

As specified in 2.2.1, all CA certificates shall be published in Repositories accessible over the Internet.

PIV-I authentication and card authentication certificate must not be distributed via public repositories. This CP makes no other stipulation regarding publication of Subscriber certificates.

4.4.3 Notification of Certificate Issuance by the CA to other entities

For the TBCA, notification of CA certificate issuance will be provided to the TPMA and to all Entities cross-certified with the TBCA according to the MTFSA.

For Entity CAs, the TPMA shall be notified at least two weeks and a day prior to the issuance of a new CA certificate or issuance of CA certificates external to the Entity's PKI domain. The notice period will begin to run upon written acknowledgement of the TPMA. In addition, all new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the CA certificate issuance shall be provided to the TPMA and FPKIPA within 24 hours following issuance.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers shall protect their private keys from access by other parties.

Subscribers and CAs shall use their private key as specified through certificate extensions, including the key usage, extended key usage extensions, and certificate policies in the associated certificate.

4.5.2 Relying Party Public key and Certificate Usage

Relying parties shall 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. Relying parties should process certificate and status information as specified in X.509 before relying on any certificate.

4.6 CERTIFICATE RENEWAL

Certificate renewal consists of issuing a new certificate with a new validity period and serial number while retaining all other information in the original certificate including the public key. The new certificate may include new issuer information (e.g., different CRL, distribution point, AIA, and signature from a different issuer key).

Frequent renewal of certificates may assist in reducing the size of CRLs.

After certificate renewal, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.6.1 Circumstance for Certificate Renewal

A certificate may be renewed if the private key has not reached the end of its validity period, has not been revoked or compromised, and the Subscriber name and attributes are unchanged.

Practice Note: Certificate renewal procedures are primarily for replacing OCSP Responder Certificates, SCVP Responder Certificates, Cross-Certificates, and other Device certificates where the certificate lifetime is purposely shorter than the private key lifetime. Renewal procedures are unlikely to be needed beyond these cases.

Certificates may also be renewed when the CA that issued the certificates is re-keyed.

PIV-I certificates must not be renewed, except during recovery from CA key compromise. In such cases, the renewed certificate must expire as specified in the original Subscriber certificate.

The validity period of the certificate and private key must meet the requirements specified in Section 5.6.

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

4.6.2 Who may request Renewal

For the TBCA, the Entity or TOA may request renewal of an Entity CA's cross-certificate.

For other CA certificates and Delegated OCSP responder certificates, the corresponding operating authority may request renewal.

CAs may perform renewal of subscriber certificates without a corresponding request, such as when the CA is re-keyed.

For Entity CAs that support renewal, such requests shall only be accepted from the following parties:

- Certificate subjects – for its certificate(s);
- PKI sponsors – for device certificate(s); and
- Role sponsors – for role certificates(s).

4.6.3 Processing Certificate Renewal Requests

For the TBCA, certificate renewal for reasons other than re-key of the TBCA shall be approved by the TPMA. The TPMO shall also approve and require an active MTFSA which does not expire prior to the new period of the renewed certificate.

When certificates are renewed due to 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 shall not be renewed. Certificate Renewal Requests shall be processed according to the requirements in Section 3.3.1. For renewal, however, the keys may not change.

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 consists of creating new certificates with a new and different private key (and serial number) and corresponding new and different public key, while retaining the remaining contents of the old certificate that describes the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key. Re-key of a certificate does not require a change to the subject Distinguished Name or subject Alternative Name(s) and does not violate the requirement for name uniqueness.

After certificate rekey, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.7.1 Circumstance for Certificate Re-key

Circumstances that require certificate re-key include nearing the maximum usage period of a private key, certificate expiration, loss or compromise, issuance of a new hardware token, and failure of a hardware token.

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.

CAs and RAs may initiate re-key of a Subscriber's certificates without a corresponding request from the Subscriber or Sponsor.

Section 5.6 establishes maximum usage periods for private keys for both CAs and Subscribers.

4.7.2 Who may request certification of a new public key

The TOA may request certification of a new public key for currently cross-certified Entity Principal CAs.

For Entity CA certificates and Delegated OCSP responder certificates, the corresponding operating authority may request re-key of its own certificate. For all other requests for re-key, such requests shall only be accepted as follows:

- A human Subject for its certificate(s);
- A PKI Sponsor for its device certificate(s); and
- A Role Sponsor for its role certificate(s).

4.7.3 Processing certificate Re-keying requests

CAs shall perform the identity proofing processes defined in Section 3.3.1 before performing re-key. Alternatively, the certificate could be automatically re-keyed by the CA based on an electronically authenticated request from the Subscriber as per Section 3.3.1.

Digitally signed Subscriber re-key requests shall be validated before the re-key requests are processed.

For the TBCA, the TOA shall also verify the validity period associated with the new certificate will not extend beyond the period of the MTFSA.

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

Certificate modification consists of creating new certificates with subject information (e.g., a name or email address) that differs from the old certificate. For example, an Entity CA may perform certificate modification for a Subscriber whose characteristics have changed (e.g., has just received a medical degree). The new certificate may have the same or different subject public key.

After certificate modification, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.8.1 Circumstance for Certificate Modification

CA certificates and Delegated OCSP responder certificates whose characteristics have changed (e.g., asserting a new policy OID, modification of SIA extension) may be modified. The new certificate may have the same or a different subject public key.

CAs may perform a certificate modification process in support of cases where one or more of the Subject's names have changed. Such circumstances include, but are not limited to name change from marriage, post nominal change, and email address change. In this case, the new certificate must have a different subject public key.

Subject must be entitled to continue with its existing certificate before certificate modification is performed.

4.8.2 Who may request Certificate Modification

For the TBCA, the TOA or the Entity CA may request certificate modification for currently cross-certified Entity CAs.

CAs and RAs may request certificate modification on behalf of their Subscribers.

For Entity CA certificates and Delegated OCSP responder certificates, the corresponding operating authority may request modification.

For Entity CAs that support certificate modification, such requests shall only be accepted as follows:

- A PMA for its CA certificate(s);
- A human Subject for its certificate(s);
- A PKI Sponsor for its device certificate(s); and
- A role sponsor for its role certificate(s).

4.8.3 Processing Certificate Modification Requests

For the TBCA, the validity period associated with the new certificate must not extend beyond the period of the MTFSA. CAs shall perform the identity proofing processes defined in Section 3.3.1 before performing re-key. However, evidence of the change to subject information shall be collected and verified as per Section 3.2 in all cases. If the modified certificate contains a new public key, the requirements specified in 4.7.3 apply.

If a Subscriber's authorizations or privileges change, and the modified certificate reflects the reduction in privileges or authorizations, 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 & 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.

For PIV-I, Medium Hardware, Medium, and Basic Assurance certificates, all CAs must publish CRLs.

For Entity CAs, the TPMA shall be notified at least two weeks and one day prior to the revocation of a CA certificate, whenever possible. The notice period will begin to run upon written acknowledgement by the TPMA. For emergency revocation, CAs shall follow the notification procedures in Section 5.7.

4.9.1 Circumstances for Revocation

For the TBCA and Entity CAs, 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.

If an organization terminates its relationship with an Entity CA and it no longer provides affiliation information, the Entity CA must revoke all certificates affiliated with that organization. CAs must also revoke certificates for key compromise upon receipt of an authenticated request from an appropriate entity as described herein.

The circumstances under which certificates issued by the TBCA will be revoked include:

- When the TPMA requests a TBCA-issued certificate be revoked. This will be the normal mechanism for revocation in cases where the TPMA determines that an Entity PKI does not meet the policy requirements or applicable MTFSA;
- When the TOA receives an authenticated request from a designated official of the Entity CA. Entity CA may request revocation for convenience. Entity CA shall request revocation if it cannot meet its obligations within this CP or the obligations corresponding to any "pass-through" policy OIDs asserted in its Cross-Certificate; and
- When the TBCA Operational personnel determine that an emergency has occurred that may impact the integrity of the certificates issued by the TBCA (e.g. key compromise, severe violation threatening to cross-certified parties). Under such circumstances, the following individuals may authorize immediate certificate revocation:
    - Chair, TPMA, or
    - Other personnel as designated by the Chair, TPMA.

  The TPMA shall meet as soon as practicable to review the emergency revocation.

The circumstances under which certificates issued by an Entity CAs shall be revoked include:

- The Subject or authorized party requests revocation;
- The identifying information or affiliation with an organization asserted in the DN is no longer valid. This can happen when the Subscriber is no longer affiliated with the sponsoring organization or when a wildcard certificate has been issued with a name where the PKI Sponsor does not exercise control over the entire namespace associated with the wildcard certificate. Entity CAs shall ensure in their agreements with Subscriber organizations that the Organization is required to notify the Entity CA of any changes to the Subscriber affiliation;
- The affiliation with an organization can no longer be confirmed (e.g. organization terminates relationship with CA);
- Privilege attributes asserted in the Subscriber's certificate are reduced;
- Content in a certificate is no longer valid (e.g. name, role, or privilege change);
- Subject can be shown to have violated the stipulations of its respective Subscriber Agreement, MTFSA, or this CP;
- Private key is compromised or suspected of compromise; and
- The CA fails to adequately adhere to the requirements of its CP or CPS.

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.

4.9.2 Who Can Request Revocation

A TBCA certificate may be revoked upon direction of the TPMA or upon an authenticated request by a designated official of the Entity CA (such official or officials shall be identified in the MTFSA as authorized to make such a request).

Entity CAs shall accept revocation requests as follows:

- From Subject for its certificates;
- From PKI Sponsor for its device certificates;
- From Role Sponsor for role certificates; and
- From designated officials of Affiliated Organizations for certificates limited to those asserting an affiliation with their organization.

Entity CAs may permit requests from other parties (e.g. RA, supervisors, Human Resources (HR), operational personnel).

The TBCA and Entity CAs are permitted to revoke the certificates they issue at the issuer's sole discretion. Where feasible, a written notice and brief explanation for the revocation will be provided to the Subscriber.

4.9.3 Procedure for Revocation Request

A revocation request shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (digitally or manually signed). Upon

receipt, the revocation request shall be authenticated and the corresponding certificate shall be revoked.

For the TBCA, the TOA shall authenticate the request and seek approval to revoke from the TPMA. TPMA approval is not necessary under emergency circumstances as defined in Section 4.9.1.

If a revocation is due to a certificate or system compromise or an Entity CA violation of the MTFSA, the TPMA will notify previously designated officials of all cross-certified entities.

For Entity CA:

- If a Subscriber leaves an organization and the hardware tokens cannot be retrieved, then all Subscriber Certificates associated with that token shall be revoked immediately for the reason of 'key compromise.'
- If a Subscriber's token is lost or stolen, then all Subscriber Certificates associated with that token shall be revoked immediately for the reason of 'key compromise.'
- 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) shall also be revoked. If it is determined that a private key used to authorize the issuance of one or more certificates may have been compromised, all certificates directly or indirectly authorized by that private key since the date of the actual or suspected compromise shall be revoked or shall be verified as appropriately issued.

Practice Note: This requirement pertains to credentials directly derived from an end entity certificate where the derived certificate is issued to the same Subscriber or device (e.g. FIPS 201-2 derived credentials)

- For all id-PIVI assurance levels, revocation of the Certificate is mandatory whenever a card is no longer valid. When possible, for credentials containing certificates issued at the id-MediumHardware, and id-MediumHardware-CBP assurance levels, Entity CAs (or delegate) shall collect, destroy, and record the destruction of the Subscriber's card whenever the card is no longer valid. Even where all the above conditions have been met, revocation of the associated certificates is recommended. Where subscribers use hardware tokens, revocation is optional if all the following conditions are met:
  - the revocation request was not for key compromise;
  - the hardware token does not permit the user to export the signature private key;
  - the Subscriber surrendered the token to the PKI;
  - the token was zeroized or destroyed promptly upon surrender; and
  - the token has been protected from malicious use between surrender and zeroization or destruction.

  In all other cases, revocation of the certificates is mandatory.

4.9.4 Revocation Request Grace Period

The revocation request grace period is the time available to the responsible party within which the responsible party must make a revocation request after reasons for revocation have been identified.

This CP does not allow a revocation grace period. Responsible parties must request revocation as soon as they identify the need for revocation.

In the case of CA key compromise, Entity CAs must request revocation within one hour of confirmation of the compromise.

4.9.5 Time within which CA must Process the Revocation Request

For the TBCA all revocation requests shall be processed within 24 hours of receipt of request.

Entity CAs will revoke Subscriber certificates as quickly as possible after receipt of a proper revocation request. Entity Online CAs will revoke certificates before the next CRL is published, except when the request is validated within two hours of CRL issuance. Revocation requests validated within two hours of CRL issuance shall be processed before the following CRL is published.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying parties are expected to verify the validity of certificates as specified in RFC 5280.

Although the CRL issued by the TBCA has a validity period of 30 days, the Relying Party shall check for a refreshed CRL every 24 hours to obtain the latest cross-certificate revocations reported.

In any case, use of revoked certificates could have damaging or catastrophic consequences in certain cases. The matter of how often new revocation data should be obtained and whether to rely upon a certificate whose revocation status is temporarily unavailable is a determination to be made by the Relying Party, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed.

4.9.7 CRL Issuance Frequency

CAs shall issue CRLs, even when no changes have occurred as specified herein. CRL issuance encompasses designating a CRL for activation, creation, and publication to replace the previous CRL.

For the TBCA and Entity CAs, the interval between CRLs shall not exceed the following:

Type of Issuance	Scope	CRL Issuance Frequency
Routine	Offline CAs* that do not issue end entity certificates except administration of the CA itself and CSS certificates	31 days

Type of Issuance	Scope	CRL Issuance Frequency
	All other CAs	24 Hours
Emergency	CA Key Compromise or Suspected Key Compromise	18 hours
	All other Key Compromise or Suspected Key Compromise	18 hours

*Offline CAs may incorporate locally attached network equipment such as an HSM or storage array. The CA system and any such locally attached network equipment must be completely isolated (air-gapped) from all other networks and computing systems.

CAs may be operated offline only if the CA issues:

- CA certificates,
- (optionally) CSS certificates.
- (optionally) end user certificates solely for the administration of the Entity CA, and
- (optionally) end-user certificates that contain the contentSigning EKU.

Entity CAs are required to notify the TOA upon Emergency CRL issuance for CA Key Compromise according to the requirements in the MTFSA between the TSCP and the cross-certified Entity.

4.9.8 Maximum Latency of CRLs

CRLs shall be published within 4 hours of generation. Furthermore, each CRL shall be published no later than the time specified in the nextUpdate field of the previously issued CRL for same scope.

For CAs that operate offline, pre-generated CRLs intended for publication more than 4 hours after generation must be protected in the same manner as the CA. All pre-generated CRLs not yet published must be securely destroyed whenever the CA revokes any certificate. The CPS must describe protections and processes used for generation and protection of any pre-generated CRLs.

If CRLs are pre-generated, either the thisUpdate field will be the date of generation and the nextUpdate value will be beyond the date of planned publication or the thisUpdate field will be the date at which the CRL becomes valid. CAs shall coordinate with Repositories to reduce the latency between the moment the CA desires the CRL to be published and the moment the CRL is available to Relying Parties within the applicable Repositories. The maximum latency between the moment a revocation request is validated and the moment the revocation information is published and available to Relying Parties shall be no greater than 24 hours.

4.9.9 On-line Revocation/Status Checking Availability

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

OCSP services must be designed and implemented to provide 99% availability overall and limit scheduled down-time to 0.5% annually, with resources sufficient to provide a response time of ten (10) seconds or less under normal operating conditions.

For certificates at the id-PIVI assurance levels, CAs shall support on-line status checking via OCSP [RFC 6960].

4.9.10 On-line Revocation Checking Requirements

Entity CAs are responsible for updating and maintaining their OCSP responder entries in the TOA's list and have sole discretion for which OCSP responders, if any they desire to include in the list. For certificates where revocation status online checking is not available, a CRL must be used.

4.9.11 Other Forms of Revocation Advertisements Available

A CA may also use other methods to publicize the certificates it has revoked. Any alternative method must meet the following requirements:

- The alternative method must be described in the CA's approved CPS;
- The alternative method must provide authentication and integrity services commensurate with the assurance level of the certificate being verified; and
- The alternative method must meet the issuance and latency requirements for CRLs stated in Sections 4.9.7 and 4.9.8.

A CA is not required to check for such forms of advertisements.

4.9.12 Special Requirements Related To Key Compromise

See Section 4.9.7.

4.9.13 Circumstances for Suspension

Suspension shall not be used by the TBCA.

Entity CAs that do not support suspension shall state so in their CP.

For Entity CAs, suspension is permitted for certificates issued at the id-PIVI, id-PIVI-cardAuth, id-MediumHardware, id-MediumHardware-CBP, and Basic assurance levels, in circumstances where the credential is temporarily unavailable to the Subscriber.

Practice Note: Relying parties may cache the CRL which suspends a certificate. This may result in unexpected delays where an un-suspended credential cannot be used by a Relying Party until the Relying Party downloads the latest CRL.

4.9.14 Who can Request Suspension

Entity CAs may accept suspension restoration requests as follows:

- From Subject
- From PKI Sponsor for its device certificate(s)
- From Role Sponsor for its role certificate(s)
- From designated officials of Affiliated Organizations for certificates limited to those asserting an affiliation with their organization
- From Supervisors, Human Resources
- From Operational Personnel
- From Entity CA (and RA)

The Entity CA CPS must describe under what circumstances certificates may be suspended and provide details for the corresponding sections below. CA shall not permit the Subject to unsuspend its own certificate(s), unless the Subject originally requested the suspension.

4.9.15 Procedure for Suspension and Restoration after Suspension Request

For an Entity CA that supports suspension, a suspension request shall identify the certificate to be suspended, the requestor, explain the reason for suspension, and allow the request to be authenticated (digitally or manually signed). Upon receipt, the suspension request shall be authenticated and the corresponding certificates shall be suspended.

Further, all suspended certificate serial numbers shall be populated on a full CRL within the timeframe specified in Section 4.9.7 and remain on the CRL until they are restored or expired. The reason code CRL entry extension shall be populated with “certificateHold,”

A restoration request shall identify the certificate to be restored, explain the reason for restoration, and allow the request and requestor to be authenticated (digitally or manually signed.) Upon receipt, the restoration request shall be authenticated and the corresponding certificates shall be restored.

In cases where the Subject is requesting restoration, the Subject shall be authenticated by following the processes defined in Section 3.2.3.

4.9.16 Limits on Suspension Period

For Entity CAs, a certificate may be suspended for up to 14 days. If the certificate has not been un-suspended within that period, the certificate shall be revoked for reason of key compromise. The Entity CA CPS must describe in detail how the maximum suspension period is enforced.

Certificates must not be published on a CRL with a reason code of “certificateHold” beyond the expiration date of the certificate.

4.10 CERTIFICATE STATUS SERVICES

CAs or Enterprises are not required to support Certificate Status Services such as SCVP or OCSP, except for the id-PIVI, id-PIVI-cardAuth, and id-PIVI-ContentSigner assurance levels where OCSP is mandatory. See Section 4.9.9 for OCSP.

If additional certificate status services are supported, they must be described in the CPS.

4.10.1 Operational Characteristics

Where applicable, operational characteristics must be described in the CPS.

4.10.2 Service Availability

Relying Parties are bound to their obligations and the stipulations of this CP irrespective of the availability of Certificate Status Servers.

For the TBCA, mechanisms and procedures shall be designed to ensure Certificate Status Services are available for use 24 hours a day, 7 days a week, with a minimum of 99% availability overall per year.

Entity CAs that issue certificates at the id-PIVI, id-PIVI-ContentSigning, or id-PIVI-cardAuth assurance levels shall design their Certificate Status Services to comply with a similar requirement.

4.10.3 Optional Features

Where applicable, optional features must be described in the CPS.

4.11 END OF SUBSCRIPTION

Certificates that have expired prior to or upon end of subscription are not required to be revoked. Unexpired CA certificates shall always be revoked at the end of subscription.

4.12 KEY ESCROW & RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

The TBCA shall not perform any escrow or key recovery functions.

For Entity CAs, that support key escrow and recovery, key recovery requirements must be documented in a CP or KRP. The KRP may be a separate document or may be combined with the CP, Likewise, the KRPS may be a separate document or combined with the CPS.

Only Subscriber Encryption Keys may be escrowed.

When considering whether to allow recovery of mediumHardware keys in software, entities should weigh the risk of unauthorized decryption against the benefits of allowing recovery. The CP/KRP and CPS/KRPS shall define the circumstances and details under which key recovery in software is allowed.

Key Recovery policies and practices shall satisfy privacy and security requirements for CAs issuing and managing digital certificates under the Entity's CP.

In either case, the CPS/KRPS shall be analyzed for compliance with the CP/KRP by an independent compliance auditor under the following circumstances:

Circumstance	Key Escrow and Recovery Applicability
Private Key Corresponding to a Human Subscriber Encryption Certificate	Key Escrow and Recovery is mandatory.
Private Key Corresponding to a Device Subscriber Encryption Certificate	Key Escrow and Recovery is mandatory unless the data protected by the keys will not require recovery under any circumstances.

Escrowed keys in the KED shall be protected at a level of security no less than the level in which the keys were generated, delivered, and protected by the Subscriber.

4.12.1.1 Key Escrow Process and Responsibilities

If encryption key escrow is supported, subscriber encryption private keys must be protected during transit and storage using cryptography at least as strong as that of the key being escrowed.

Subscribers must be notified that the private keys associated with their encryption certificates will be escrowed.

4.12.1.2 Key Recovery Process and Responsibilities

Communications between the various key recovery participants (KED, DDS, KRA, KRO, Requestor, and Subscriber) must be secured from protocol threats such as disclosure, modification, replay, and substitution. The strength of all cryptographic protocols must be equal to or greater than that of the keys they protect.

During delivery, escrowed keys must be protected against disclosure to any party except the Requestor.

When any mechanism that includes a shared secret (e.g., a password) is used to protect the key in transit, the mechanism must ensure that the Requestor and the transmitting party are the only holders of this shared secret. Subscribers may use electronic or manual means to request their own escrowed keys from the KED. The Subscriber may submit the request to the KED, KRA or KRO. If the request is made electronically, the subscriber shall digitally sign the request or authenticate to a recovery service using an associated authentication or signature certificate with an assurance level equal to or greater than that of the escrowed key. Manual requests shall include proper identity verification by the KRA in accordance with Section 3.2.3.1.

Third-Party Requestors may use electronic or manual means to request the Subscribers' escrowed keys. The Requestor must submit the request to the KRA or KRO. If the request is made electronically, the Requestor must digitally sign the request using an authentication or signature certificate trusted by the recovering organization with an assurance level equal to or greater than that of the escrowed key.

Manual requests shall include proper identity verification by the KRA in accordance with Section 3.2.3.1.

DDSs shall use electronic means to request Subscribers' escrowed keys. Requests shall be authenticated as specified in Section 3.5.5.

Third party key recovery does not require revocation of a subscriber certificate. This does not prohibit Subscribers from requesting revocation of their own certificates for any reason.

4.12.1.2.1 Key Recovery through KRA

The KRA must provide access to a copy of an escrowed key only in response to a properly authenticated and authorized key recovery request. Such access requires the actions of at least two KRAs. All copies of escrowed keys must be protected 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, provided they comply with technical controls in Section 6.2.2.

> Practice Note: A combination of physical, procedural, and technical security controls can be used to enforce continuous two-person control during recovery and delivery of escrowed keys. The KRS should be designed to maximize the ability to enforce two-person control technically.

The KRA and KRO are not required to notify subscribers of a third-party key recovery and may be prohibited from notifying the subscriber in some use cases (e.g., law enforcement investigations).

4.12.1.2.2 Automated Self-Recovery

A current Subscriber's escrowed keys may be provided directly to the Subscriber without imposition of two-person control requirements. The KED must only provide escrowed keys to current Subscribers without two-person control upon:

- Verifying that the authenticated identity of the Requestor is the same as the Subscriber associated with the escrowed keys being requested;
- Sending notification to the Subscriber of all attempts (successful or unsuccessful) to recover the Subscriber's escrowed keys that are made by entities claiming to be the subscriber. If the KED does not have information (e.g., an e-mail address) necessary to send notification to the Subscriber of a key recovery request, then the KED must not provide the Subscriber with the requested key material using the automated recovery process;

  > Practice Note: Where possible, the e-mail address will be from the subject alternative name field of the certificate being recovered.

- Ensuring that the escrowed keys are being sent only to the authenticated Subscriber associated with the escrowed keys; and

- Ensuring that the escrowed keys are encrypted during transmission using cryptography of equal or greater strength than provided by the escrowed keys.

4.12.1.2.3 Key Recovery During Token Issuance

When a Subscriber (individual and/or role sponsor) is issued a new certificate on a hardware token, private key management keys for the Subscriber may be recovered as part of the issuance process by the KED using secure means, such as Global Platform Secure Channel Protocol, to inject the key history onto the hardware token directly.

4.12.1.2.4 Key Recovery by Data Decryption Server

A DDS must be under two-person control, as is required for any CA or KED. A DDS is permitted to automatically recover keys from the KED. The KED must perform the following activities prior to releasing the key:

- Authenticating the Requestor as a legitimate DDS;
- Verifying that the DDS is authorized to recover the escrowed key for the Issuing Organization to which the key belongs; and
- Ensuring that the escrowed keys are protected during transmission using cryptography or other means of equal or greater strength than provided by the escrowed keys.

In order to prevent any individual KRA, KRO or other trusted role from accessing subscriber encryption keys, a combination of physical, procedural, and technical security controls must be used to enforce continuous two-person control on the DDS. The DDS must be designed to maximize the ability to enforce two-person control technically.

4.12.1.3 Who Can Submit a Key Recovery Application

Subscriber may request recovery of their own escrowed keys. Key recovery may also be requested by internal Third-Party Requestor permitted by the Issuing Organization policy, and by authorized external Third-Party Requestors (e.g., law enforcement personnel with a court order from a competent court).

4.12.1.3.1 Requestor Authorization Validation

The KRA or the KRO, as an intermediary for the KRA, must validate the authorization of the Requestor. KRAs should consult with Issuing Organization management and/or legal counsel, as appropriate.

Issuing Organizations must determine internal notification requirements for External Third-Party key recovery requests and account for situations where the law requires the KED to release the Subscriber's private key without organizational notification.

Nothing in this document is intended to change the current procedures for obtaining information about individuals in connection with such requests.

4.12.1.3.2 Subscriber Authorization Validation

Current Subscribers are authorized to recover their own escrowed key material.

4.12.1.3.3 KRA Authorization Validation

The KED must verify that the KRA has appropriate privileges to obtain the keys for the identified Subscriber's organization.

4.12.1.3.4 KRO Authorization Validation

The KED or KRA must verify that the KRO is authorized to request keys for the identified Subscriber.

4.12.1.3.5 Data Decryption Server Authorization Validation

The KED must verify that the DDS recovery request falls within the organizational scope for which the DDS was established.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Entity CAs that support session key encapsulation and recovery shall identify the document describing the practices in the applicable CP/KRP and CPS/KRPS.

5. FACILITY MANAGEMENT & OPERATIONS CONTROLS

5.1 PHYSICAL CONTROLS

All physical control requirements specified herein apply equally to all CAs, CMSs, CSSs, KRSs, DDSs, associated HSMs, and any Remote Workstations (operated outside the secure enclave of the CA, CMS, CSS, DDS, or HSMs) that support them. RA workstations are not remote workstations as defined here and in Section 15 definition of "Remote Workstations."

5.1.1 Site Location & Construction

The location and construction of the facility housing CA and CMS (See Section 1.3.3), CSS, DDS, and associated HSMs, and sites housing Remote Workstations used to administer them, shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, shall provide robust protection against unauthorized access to equipment and records.

5.1.2 Physical Access

5.1.2.1 Physical Access for CA Equipment

CA equipment, including remote workstations used to administer the CAs, shall always be protected from unauthorized access. The security mechanisms shall be commensurate with the level of threat in the equipment environment.

The physical security requirements pertaining to CAs that issue only Basic Assurance certificates are:

- Ensure no unauthorized access to the hardware is permitted; and
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers.

The physical security requirements pertaining to all other CAs 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;
- Require two-person physical access control to both the cryptographic module and computer systems; and
- Provide at least three layers of physical access boundaries (e.g. perimeter, building, PKI room).

Removable cryptographic modules shall be deactivated prior to storage. When not in use, cryptographic modules, activation information used to access or enable cryptographic modules, and other sensitive CA equipment shall be placed in secure containers. Activation data shall

either be memorized, recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module or the removable hardware associated with remote workstations used to administer the CA.

A security check of the facility housing the CA, CMS, CSS, and DDS equipment or Remote Workstations used to administer them 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");
- Off-line CA equipment is shut down or HSMs are deactivated and securely stored;
- 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 persons 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 assert that all necessary physical protection mechanisms are in place and activated.

5.1.2.2 Physical Access for RA Equipment

RA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. The RA 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 equipment environment.

5.1.2.3 Physical Access for CSS Equipment

Physical access control requirements for CSS equipment (if implemented), shall meet the CA physical access requirements specified in 5.1.2.1. CSS equipment that does not have a private signing key and only distributes pre-generated OCSP responses is not required to meet the requirements in 5.1.2.1.

5.1.2.4 Physical Access for CMS Equipment

Physical access control requirements for CMS equipment containing a certificate at the id-PIVI-ContentSigner assurance level shall meet the CA physical access requirements specified in 5.1.2.1.

5.1.2.5 Physical Access for KED Equipment

Physical access control requirement for KED equipment that stores private keys shall meet the CA physical access requirements specified in Section 5.1.2.1.

5.1.2.6 Physical Access for DDS Equipment

Physical access control requirement for DDS equipment that stores private keys shall meet the CA physical access requirements specified in Section 5.1.2.1.

5.1.2.7 Physical Access for KRA and KRO Equipment

KRA and KRO equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. The KRA and KRO 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 equipment environment.

5.1.3 Power and Air Conditioning

CAs shall have sufficient backup capability to automatically lock out input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown.

Repositories shall be provided with Uninterrupted Power sufficient for a minimum of six hours operation in the absence of commercial power.

5.1.4 Water Exposures

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

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

5.1.5 Fire Prevention & Protection

Operational environment shall be equipped with temperature and smoke detectors, alarms, and a fire suppression system appropriate for computer equipment.

5.1.6 Media Storage

CA media shall be stored in a way that protects it from accidental damage (water, fire, electromagnetic) and unauthorized physical access.

5.1.7 Waste Disposal

Sensitive media and documentation that are no longer needed for operations shall be destroyed in a secure manner. For example, sensitive paper documentation shall be shredded, burned, or otherwise rendered unrecoverable.

5.1.8 Off-Site backup

On a periodic schedule, CAs shall create full system backups sufficient to recover full PKI services from a system failure. At least one full backup copy shall be stored at an off-site location separate from the CA equipment. Only the latest full backup needs to be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA.

For offline CAs, the backup must be performed each time the system is turned on or once per week, whichever is less frequent.

Requirements for CA private key backup are specified in Section 6.2.4.

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 to ensure the integrity of the CA is not weakened. The functions performed in these roles form the basis of trust for all uses of the PKI. 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. An auditable record shall be created identifying when personnel are added or removed from a trusted role, including the individual who added or removed them from the role. The individual who authorized a role assignment shall be traceable from the audit and archive records as indicated in Section 5.4 and 5.5. The requirements of this policy are defined in terms of four roles. (Note: the information derives from the Certificate Issuing and Management Components (CIMC) Profile.)

1. *Administrator* – authorized to install, configure, and maintain the CA or, optionally, KED or DDS; establish and maintain user accounts; configure profiles and audit parameters; and generate component keys.
2. *Officer* – authorized to request or approve certificates or certificate revocations.
3. *Auditor* – authorized to maintain audit logs.
4. *Operator* – authorized to perform system backup and recovery.

The following subsections provide a detailed description of the responsibilities for these primary trusted roles and secondary trusted roles, which are used at the CA, CMS, KRS, and CSS locations as appropriate. Irrespective of the titles and numbers of Trusted Roles, requirements for separation of duties and two-person control must be met as specified in Section 5.2.2 and 5.2.4.

5.2.1.1 Administrator

The administrator's role is responsible for:

- Installation, configuration, and maintenance of the CA, or KED or DDS as applicable;
- Establishing and maintaining CA system accounts;
- Configuring certificate profiles or templates and audit parameters;
- Generating and backing up CA keys; and
- Administrators shall not issue certificates to subscribers.

5.2.1.2 Officer

The officer's role is 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 Auditor

The auditor's role is responsible for:

- Reviewing, maintaining, and archiving audit logs; and
- Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with its CPS.

5.2.1.4 Operator

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

5.2.1.5 Registration Authority

The 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; and
- 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 CSS Roles

A CSS shall have at least the following roles:

The CSS Administrator shall be responsible for installation, configuration, and maintenance of the CSS;

- Establishing and maintaining CSS system accounts;
- Configuring CSS application and audit parameters; and
- Generating and backing up CSS keys.

The CSS Auditor shall be responsible for:

- Reviewing, maintaining, and archiving audit logs; and
- Performing or overseeing internal compliance audits to ensure that the CSS is operating in accordance with its CPS.

The CSS Operator shall be responsible for:

- The routine operation of the CSS equipment; and
- Operations such as system backups and recovery or changing recording media.

5.2.1.7 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 Auditor 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 CMS 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.

5.2.1.8 Key Recovery Roles

Due to the security implications and impacts to confidentiality services associated with key recovery, the number and location of Key Recovery Trusted Roles should be closely controlled.

Entity PKIs supporting key escrow and recovery shall specify which trusted roles cover the following key recovery responsibilities:

5.2.1.8.1 Key Recovery Agent (KRA)

The KRA shall have the following responsibilities:

- Authenticating requests and recovering copies of escrowed keys; and
- Distributing copies of recovered keys to the Requestor, as specified in Section 4.12.1.2.1.

5.2.1.8.2 Key Recovery Official (KRO)

Entity PKIs supporting key escrow and recovery may have KROs defined as Trusted Roles if they have privileged access to the KED. If the KRO does not have access to the KED, the KRO is not considered a Trusted Role but a KRO is considered a sensitive position. In all cases, if someone already in a Trusted Role is assigned to perform a KRO function, Separation of Roles shall be enforced per Section 5.2.4.

KROs shall be responsible for:

- Verifying a Requestor's identity and authorization to recover keys;
- Developing and executing key recovery requests on behalf of an authorized Requestor;
- Securely communicating key recovery requests to and receiving responses from the KRA; and
- Participating in the distribution of escrowed keys to the Requestor as provided in the relevant CPS or KRPS.

5.2.2 Number of Persons Required per Task

Only one person is required per task for CAs operating only at the Basic level of assurance.

For all other levels of assurance, two or more persons are required for the following tasks:

- CA, CMS (id-PIVI-ContentSigner), KED, or DDS key generation;
- CA and CMS (id-PIVI-ContentSigner) signing key activation;
- CA, CMS (id-PIVI-ContentSigner), KED, or DDS private key backup; and
- Issuance of certificates at the id-PIVI or id-PIVI-cardAuth assurance levels.

Where multiparty control for logical access is required, at least one of the participants shall be an Administrator. All participants must serve in a trusted role as defined in Section 5.2.1. Multiparty control for logical access shall not be achieved using personnel that serve in the Auditor Trusted Role.

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.

All Trusted Roles who operate a CMS shall be allowed access only when authenticated using a method commensurate with the id-PIVI assurance level.

5.2.4 Separation of Roles

Role separation, when required as set forth below, may be enforced either by the CA equipment, or procedurally, or by both means. No individual in a trusted role shall have more than one identity.

For the Basic level of assurance, individual personnel must be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume more than one role; however, no one individual shall assume both the Officer and Administrator roles. This may be enforced procedurally.

For all other levels of assurance, the CA, CMS, RA, and KRS software and hardware shall identify and authenticate its users and shall ensure that no user identity can assume both an Administrator and an Officer role, assume both the Administrator and Auditor roles, and assume both the Auditor and Officer roles.

Requirements for the separation of roles, and limitations on use of procedural mechanisms to implement role separation, are as follows:

- Individual personnel shall be specifically designated to the four roles defined in Section 5.2.1 above;
- Individuals who assume an Auditor role shall not assume any other role; and

> Practice Note: Persons in auditor role may perform backups limited to the audit logs and archive without being categorized as being in an operator trusted role.

- Individuals who assume an Officer role shall not assume an Auditor or Administrator role.

5.3 PERSONNEL CONTROLS

5.3.1 Background, Qualifications, Experience, & Security Clearance Requirements

Each Entity shall identify the set of individuals assigned to primary and secondary trusted roles, who are responsible and accountable for the operation of each CA, CMS, CSS, RA, and KRS in that Entity.

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 shall:

- Have successfully completed an appropriate training program;
- Have a favorable outcome from a background investigation that does not raise issues related to trustworthiness/integrity;
- Have demonstrated the ability to perform their duties;

- Have no other duties that would interfere or conflict with their duties for the trusted role;

- Have not been previously relieved of duties for reasons of negligence or non-performance of duties or any other reason that demonstrates a violation of trust;
- Have not been denied a security clearance, or had a security clearance revoked for cause;
- Have not been convicted of a legally reportable felony offense or serious crime; and
- Be appointed in writing by an approving authority.

In circumstances where satisfactory evidence of the above cannot be confirmed, an active clearance equal to or higher than U.S. Secret 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 may be used as an alternative.

For Federal Agency PKIs, regardless of the assurance level, all trusted roles must be held by U.S. citizens. For PKIs operated at Medium Assurance and Medium Hardware, each person filling a trusted role must also satisfy at least one of the following:

- 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; or
- For RA Administrator, Trusted Agents, and personnel appointed to the trusted roles for the CSSs, in addition to the above, the person may be a citizen of the country where the function is located.

For PKIs, other than Federal Agency PKIs, only operated at Basic, Medium-CBP, and Medium Hardware-CBP, there is no citizenship requirement or security clearance specified.

5.3.2 Background Check Procedures

Trusted Role Personnel (primary and secondary) shall, at a minimum, receive a favorable adjudication after undergoing a background investigation covering the following areas:

- Employment;
- Education;
- Place of residence;
- Law Enforcement; and
- References (for original investigation only).

The initial period of investigation must cover at least the last five years for each area, excepting the residence check which must cover at least the last three years and the employment check may be limited to the period of time the individual has been in the work-force. Regardless of the date of award, the highest educational degree shall be verified.

For Federal employees and cleared contractors:

- A national security eligibility (i.e., Confidential or above is granted after positive adjudication of a Tier 3 or Tier 5 investigation,
- A suitability determination is granted after positive adjudication of a Tier 2 or Tier 4 investigation, and
- A PIV credential eligibility is granted after a positive adjudication of a Tier 1 investigation.

In all cases, the reinvestigation period for a Trusted Role background check must not exceed 10 years. If a Trusted Role's national security eligibility, suitability determination, or PIV eligibility is ever suspended or revoked during their appointment, all CA access must be revoked until the security eligibility, suitability determination, or PIV eligibility is reinstated or a separate investigation is completed and adjudicated.

Practice Note: For non-Federal organizations, the qualifications of the adjudication authority and procedures utilized to satisfy these requirements must be demonstrated to the TPMA before cross certification with the TBCA.

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.

Background check procedures shall be described in the CPS.

Background check results shall not be released except as required in Section 9.3 and 9.4.

In circumstances where an interim clearance used to satisfy background check requirements is later found unfavorable, all certificates issued while the person had a trusted role shall be re-evaluated and possibly revoked at the discretion of the CA's PMA.

5.3.3 Training Requirements

All trusted roles shall receive comprehensive training in all operational duties they are expected to perform. Training shall cover the following:

- Security principles and mechanisms applicable to the trusted role;
- All PKI software versions in use by the trusted role;
- All duties the trusted role is expected to perform;
- Disaster recovery and business continuity procedures; and
- Stipulations of the applicable CP and CPS/KRPS.

Documentation shall be maintained identifying all personnel who received training and the level of training completed. Where competence was demonstrated in lieu of training, supporting documentation shall be maintained.

5.3.4 Retraining Frequency & Requirements

Individuals in trusted roles shall be aware of changes in the PKI operation. 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 software or hardware upgrade, changes in automated security systems, and relocation of equipment.

Documentation shall be maintained identifying all personnel who received training and the level of training completed.

5.3.5 Job Rotation Frequency & Sequence

Any job rotation procedures must provide for continuity and integrity of the PKI and job rotations shall be documented.

Job rotations shall comply with the role separation requirements of this CP and all access rights associated with a previous role must be terminated.

Individuals assuming an auditor role shall not audit their own work from a previous role.

5.3.6 Sanctions for Unauthorized Actions

The TPMA or Entity PMA shall take appropriate actions where personnel have performed actions not authorized in this CP.

5.3.7 Independent Contractor Requirements

Contractor personnel employed to perform trusted role functions shall meet the personnel requirements set forth in Section 5.3 as applicable.

Any PKI vendors must establish procedures to ensure that any subcontractors perform in accordance with the CP and the CPS/KRPS.

5.3.8 Documentation Supplied To Personnel

For the TBCA and Entity CAs, documentation sufficient to define duties and procedures for each trusted role shall be provided to the personnel filling that role. The documentation and procedures shall include the applicable portions of the CP and CPS/KRPS, relevant policies or contracts, and manuals as applicable.

5.4 AUDIT LOGGING PROCEDURES

Audit log files shall be generated for all events relating to the security of the CAs, CMS, CSSs, RAs, and KRSs. For CAs operated in a virtual environment, audit records must be generated for all applicable events on application software and all System Software Layers to support in-house audit reviews and third-party audits. Audit logs shall be reviewed to ensure that actions have been taken by authorized parties and for legitimate reasons. At a minimum, reviews must include

inspection of log entries, verification that there is no evidence of tampering with audit logs, and the completion of a root cause analysis for any alerts or irregularities.

Auditable Event	**Basic**	**All Other LOAs**
SECURITY AUDIT		
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	X	X
Any attempt to delete or modify the Audit logs	X	X
Obtaining a third-party time-stamp	X	X
IDENTIFICATION AND AUTHENTICATION		
Platform or CA successful and unsuccessful authentication attempts	X	X
The value of *maximum authentication attempts* is changed	X	X
The number of unsuccessful authentication attempts exceeds the *maximum authentication attempts* during user login	X	X
A person or device unlocks an account that has been locked as a result of unsuccessful authentication attempts	X	X
An person or device changes the type of authenticator, e.g., from password to biometrics	X	X
LOCAL DATA ENTRY		
All security-relevant data that is entered in the system	X	X
REMOTE DATA ENTRY		
All security-relevant messages that are received by the system	X	X
DATA EXPORT AND OUTPUT		
All successful and unsuccessful requests for sensitive and security-relevant information	X	X
KEY GENERATION		

Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	X	X
PRIVATE KEY LOAD AND STORAGE		
The loading of Component private keys used by the CA in the lifecycle management of certificates	X	X
All access to certificate subject private keys retained within the CA for key recovery purposes	X	X
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE		
All changes, including additions and deletions, to the trusted public keys, used by components of the CA to authenticate other components or authorize certificate lifecycle requests (e.g., RA or CMS trust stores)	X	X
SECRET KEY STORAGE		
The manual entry of secret keys used for authentication	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
CERTIFICATE REGISTRATION		
All records related to certificate request authorization, approval, and signature, whether generated directly on the CA or generated by a related external system or process	X	X
CERTIFICATE REVOCATION		
All records related to certificate revocation request authorization, approval, and execution, whether generated directly on the CA or generated by a related external system or process	X	X
CERTIFICATE STATUS CHANGE APPROVAL		
All records related to the approval or rejection of a certificate status change request, whether generated directly on the CA or generated by a related external system or process	X	X

CONFIGURATION		
Any security-relevant changes to the configuration of the component. The specific configuration items relevant to the environment in which the component operates must be identified and documented.	X	X
ACCOUNT ADMINISTRATION		
Roles and users are added or deleted	X	X
The access control privileges of a user account or a role are modified	X	X
CERTIFICATE PROFILE MANAGEMENT		
All changes to certificate profiles	X	X
CERTIFICATE STATUS SERVER MANAGEMENT		
All changes to CSS profile (e.g. OCSP profile)	X	X
REVOCATION PROFILE MANAGEMENT		
All changes to the revocation profile	X	X
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT		
All changes to the certificate revocation list profile	X	X
MISCELLANEOUS		
Record of appointment of an individual to a Trusted Role or removal from the Trusted Role, including a record of who added or removed them from the role	X	X
Designation of personnel for multiparty control	X	X
Installation of the Operating System	X	X
Installation of PKI Application	X	X
Installing hardware cryptographic modules		X
Removing hardware cryptographic modules		X

Destruction of cryptographic modules	X	X
System Startup	X	X
Logon Attempts to PKI Applications	X	X
Receipt of Hardware/Software		X
Attempts to set passwords	X	X
Attempts to modify passwords	X	X
Backing up internal database	X	X
Restoring internal database	X	X
File manipulation (e.g., creation, renaming, moving)		X
Posting of any material to a repository (including date and time)		X
Access to CA internal database		X
All certificate compromise notification requests	X	X
Loading tokens with certificates		X
Shipment and receipt of Tokens		X
Zeroizing tokens	X	X
Re-key of the Component	X	X
Configuration changes:		
- Hardware	X	X
- Software	X	X
- Operating System	X	X
- Patches	X	X
- Security Profiles		X
PHYSICAL ACCESS / SITE SECURITY		

Personnel Access to room housing component		X
Access to the Component		X
Known or suspected violations of physical security	X	X
ANOMALIES		
Software Error conditions	X	X
Software check integrity failures	X	X
Receipt of improper messages	X	X
Misrouted messages		X
Network attacks (suspected or confirmed)		X
Equipment failure	X	X
Electrical power outages		X
Uninterruptible Power Supply (UPS) failure		X
Obvious and significant network service or access failures		X
Violations of Certificate Policy	X	X
Violations of Certification Practice Statement	X	X
Resetting Operating System clock		X

A record of the review, all significant events, and any actions taken as a result of audit record reviews shall be explained in an audit log summary. This summary shall be retained as part of the long-term archive.

Whenever 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 and per Section 5.5.2.

5.4.1 Types of Events Recorded

All security auditing capabilities of the CA, CMS, CSS, RA and KRS operating system and CA, CMS, CSS, RA, and KRS applications required by this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. Where events cannot be automatically recorded, the CA shall implement manual procedures to satisfy this requirement.

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;
- Where the event occurred (e.g., on what systems or in what physical locations);
- Source of the event;
- Outcome of the event to include success or failure indicator;
- The identity of the entity and/or operator that caused the event;

A message from any source received by the CA requesting an action related to the operational state of the CA is an auditable event. Any request or action requiring the use of a private key controlled by the CA is an auditable event;

If out-of-band processes are used for authorization of certificate issuance, external artifacts from the process (e.g., form, email) shall be recorded; and

The CA and KRS shall record and audit the events identified in the table in 5.4 above, where applicable to the application and/or environment.

5.4.2 Frequency of Processing Log

Audit logs shall be reviewed at least every month, except for off-line CAs where the review shall be performed the longer between each month and when the system is activated. CSS, CMS, and KRS audit log processing frequency shall align with the CA audit log processing frequency.

Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting log entries, with a more thorough investigation of any alerts or irregularities in the log. Examples of irregularities include discontinuities in the logs and loss of audit data.

A statistically significant set of security audit data generated by CA, CMS, CSS, RA, and KRS since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity

Actions taken as a result of these reviews shall be documented.

An auditor trusted role shall explain all significant events in an audit log summary.

5.4.3 Retention Period for Audit Logs

Audit logs shall be retained on-site for the longer of when it is reviewed and 60 days. For CA, CMS, CSS, and KRS the individual who removes audit logs, either directly or through

supervision, shall be an auditor trusted role. For RA, the individual who removes audit logs shall be a system administrator who is not an RA.

5.4.4 Protection of Audit Logs

System configuration and procedures must be implemented together to ensure that:

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

Collection of the audit records from the CA system must be performed by, witnessed by, or under the control of trusted roles who are different from the individuals who, in combination, command the CA signature key.

For RA systems, the individual authorized to move or archive records may not hold an RA Trusted Role.

The person performing audit log archive need not have modify access, but procedures must be implemented to protect archived data from destruction prior to the end of the audit log retention period (note that deletion requires modification access).

The off-site storage location for audit logs shall be a safe, secure location separate from the location where the data was generated.

Practice Note: If a system over-writes audit logs after a given time, the audit log is not considered deleted or destroyed if the audit log has been backed up and archived.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up at least monthly, except for off-line CAs where the backup shall be performed the longer between monthly and when the system is activated. With sufficient system redundancy in place, backups for the offline TBCA CAs shall be performed at least every three months.

A copy of the audit log shall be sent off-site monthly.

The process for transferring the audit records to the backup environment shall be documented.

5.4.6 Audit Collection System (internal vs. external)

The audit log collection system may or may not be external to the CA, CMS, CSS, RA system or KRS. Automated audit processes shall be invoked at system (or application) startup and cease only at system (or application) shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the CA or KRS shall be suspended until the problem is remediated.

5.4.7 Notification to Event-Causing Subject

This CP imposes 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 policy.

Automated vulnerability scans, if executed, should be run no less frequently than required by the risk rating of the component.

The methodology, tools and frequency of vulnerability assessments must be documented.

Practice Note: The security audit data should be reviewed by the auditor for events such as repeated failed actions, requests for privileged information, attempted access of system files, requests for escrowed keys, attempted access of escrowed keys, unauthenticated responses, and other suspicious or unusual activity. The auditor should check for continuity of the security audit data.

5.5 RECORDS ARCHIVE

CA, CMS, CSS, RA, and KRS archive records shall be sufficiently detailed to allow verification that the PKI was properly operated as well as verify the validity of any certificate (including those revoked or expired) issued by the CA.

CAs and KRSs shall comply with their respective records retention policies in accordance with applicable law.

The primary objective of the CA archive is to prove the validity of any certificate (including those revoked or expired) issued by the CA in the event of dispute regarding the use of the certificate.

The primary objective of the KRS archive is reconstruction of key recovery activities, in case of dispute. Examples of disputes may include:

- Validation of key recovery requests;
- Validation of the identity of the recipient of an escrowed key;
- Verification of authorization to obtain the escrowed key copy;
- Verification of transfer of custody of escrowed keys to an authorized Requestor; and
- Establishment of the circumstances under which a copy of the escrowed key was provided.

5.5.1 Types of Events Archived

At a minimum, the following data shall be recorded for archive in accordance with each assurance level:

Data To Be Archived	Basic	All other Assurance Levels
Certificate Policy	X	X
Certification Practice Statement/Key Recovery Practice Statement	X	X
Contractual obligations	X	X
Other agreements concerning operations of the CA or KRS	X	X
System and equipment configuration	X	X
Modifications and updates to system or configuration	X	X
All records related to Certificate request authorization, approval and signature, whether generated directly on the CA or generated as part of a related external system or process	X	X
All records related to status changes (e.g., revocation, suspension and restoration) whether generated directly on CA or generated as part of a related external system or process	X	X
Subscriber identity Authentication data as per Section 3.2.3	X	X
Documentation of receipt and acceptance of certificates (if applicable)	X	X
Signed Subscriber Agreements	X	X
Documentation of receipt of tokens	X	X
All certificates issued or published	X	X
Record of Component Re-key	X	X
All CRLs issued and/or published	X	X

Data To Be Archived	Basic	All other Assurance Levels
All Audit Logs	X	X
Record of CA Re-Key	X	X
Other data or applications to verify archive contents	X	X
Audit summary reports generated by internal reviews and documentation generated during third-party audits	X	X
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	X	X
Any attempt to delete or modify the Audit Logs	X	X
Whenever the CA generates a key (not mandatory for single session or one-time use symmetric keys)	X	X
Access to certificate subject private keys retained for key recovery purposes	X	X
Changes to trusted public keys used or published by the CA, including certificates used for trust between the CA and other components, e.g., CMS, RA	X	X
Export of private and secret keys (keys used for a single session or message are excluded)	X	X
Approval or Rejection of a certificate status change request	X	X
Record of appointment of an individual to a Trusted Role or sensitive role or removal from that role, evidence of qualifications for the Trusted Role or sensitive role, the individual who appointed or removed them from the role (including their title	X	X

Data To Be Archived	Basic	All other Assurance Levels
or position in the PKI), and any specified term for the appointment		
Destruction of cryptographic modules	X	X
Certificate compromise notifications	X	X
Remedial action taken as a result of violation of physical security	X	X
Violations of Certificate Policy	X	X
Violations of Certification Practice Statement/Key Recovery Practice Statement	X	X
Documentation required by compliance auditors	X	X
Compliance Auditor reports	X	X

5.5.2 Retention Period for Archive

Archive retention periods begin at the key generation event for any CA. For CAs that leverage key-rollover procedures a new retention period begins for each subsequent key generation event.

> **Practice Note**: RA archive records can be retained for as long as business purposes require; however, this policy does not waive any organizational policies that may require the destruction of such records or otherwise limit their retention periods.

CAs will maintain all archived records related to that CA, in an accessible fashion, for 3 years after CA expiration or CA termination.

Individual RA records associated with certificate request authorization, certificate revocation, subscriber authentication, or subscriber certificate acceptance-shall be maintained for a minimum of 3 years after the subject certificate expiration date. Issuance of new certificates with extended validity periods (i.e., renewal, rekey or modification) supported by existing subscriber authentication records (i.e., authentication using an existing valid certificate) shall result in a new retention period for those initial records, based on the new certificate expiration date.

Practice Note: If the archive records are maintained separately from the CA, communication processes may be required to determine when archive records are no longer needed based on related public certificates.

Alternatively, the Entity may use whatever procedures have been approved by either the National Archives and Records Administration or other records retention laws and policies applicable to the Entity to determine data retention periods. Applications required to process the retained data shall also be maintained for the full data retention period.

RA system operations audit records, that include records that facilitate RA functions, must maintain relevant archives for a minimum of 3 years after RA system replacement or termination.

5.5.3 Protection of Archive

Only Auditors, as described in Section 5.2, or other personnel specifically authorized by the CA, are permitted to add or delete records from the archive. Deletion of records identified in Section 5.5.1 before the end of the retention period is not permitted under any circumstances. The contents of the archive must not be released except in accordance with Sections 9.3 and 9.4.

Archive media must be stored in a safe, secure storage facility geographically separate from the CA in accordance with its records retention policies. The transfer process between the backup environment and archive location must be documented.

In order to ensure that records in the archive may be referenced when required, the CA must do one of the following:

- Maintain the hardware and software required to process or read the archive records, or
- Define a process to transfer records to a new format or medium when the old format or medium becomes obsolete and verify the integrity of the records after transfer.

5.5.4 Archive Backup Procedures

The CPS or a referenced document shall describe how the records are backed up and how the archive backups are managed.

5.5.5 Requirements for Time-Stamping of Records

CA archive records shall be automatically time-stamped as they are created. The CPS shall describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard. The time precision shall be accurate enough to allow the sequence of events to be determined.

The CPS/KRPS 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)

Archive data may be collected in any expedient manner but shall be documented in the associated CPS/KRPS.

5.5.7 Procedures to Obtain & Verify Archive Information

Procedures detailing how to create, verify, package, transmit, and store archive information shall be defined in the CP, KRP, CPS or KRPS.

The contents of the archive shall not be released except in accordance with Sections 9.3 and 9.4.

Copies of records of individual transactions may be released upon request of any subscriber involved in the transaction or their legally recognized agents.

5.6 KEY CHANGEOVER

Unless the organization is ceasing certificate production, prior to the end of a CA's signing key validity period a new CA shall be established or a re-key on the existing CA shall be performed. This is known as key changeover. Upon key changeover, only the new key will be used for certificate signing purposes. The older, but still valid, public key will be available to verify old signatures until all certificates signed using the associated private key have also expired. If the old private key is used to sign CRLs that cover certificates signed with that key, then the old key must be retained and protected.

When a CA performs a key changeover and generates a new public key, the CA shall notify all CAs, RAs, and Subscribers relying on the CA's certificate that it has been changed. The CA shall also either:

- Generate a key rollover certificate, where the new public key is signed by the old private key or vice versa; or
- Obtain a new CA certificate for the new public key from each issuer of the current CA certificate(s).

The following table provides the maximum lifetimes for Certificates and associated Private Keys:

Certificate Type	2048 Bit Keys*		3072 and higher Bit Keys	
	Private Key	Certificate	Private Key	Certificate
Root CA/Bridge CA	30 years	30 years	30 years	30 years
Intermediate CA	10 years	10 years	10 years	10 years **
Issuing CA	10 years	10 years	10 years	10 years **
Identity or Signature End Entity	3 years	3 years	3 years	3 years
Encryption End Entity	unrestricted	3 years	unrestricted	3 years
Code Signer	3 years	8 years	3 years	8 years
Id-PIVI Content Signer	3 years	9 years	3 years	9 years***
OCSP Responder	3 years	120 days	3 years	120 days
SCVP Server	3 years	3 years	3 years	3 years
Device	3 years	3 years	3 years	3 years

*2048 bit keys have been deprecated and shall not be used for certificates that expire after 12/31/2030. As a result, the certificate and key lifetimes shall be limited as necessary to be in complicance with the end of life limitations. See practice note below.
** For purposes of determining key usage lifetime, it will commense on activation of the key pair.
*** Expiration of the Content Signing certificate must be later than the expiration of the Subscriber certificates on the same PIV-I credential.

Practice Note: Maximum lifetimes are also limited to the duration of acceptance for a cryptographic algorithm. See 6.1.5.

A CA cannot generate a Certificate for a Subscriber whose validity period would be longer than the CA Certificate validity period. The CA key pair shall be changed prior to the end of the validity period of the CA certificate in time to ensure that no certificate issued by the CA asserts a validity period that extends beyond the validity period of the CA certificate.

Practice Notes: CA software may automatically shorten the validity period of a Subscriber certificate such that it will not extend beyond the CAs certificate validity period.

CA signing key usage is determined in the context of the length of the validity periods of the certificates issued to and by the CA.

Certificates at the PIVI and CardAuth assurance levels shall not expire after the expiration date of the token as printed on the card body or encoded on the chip.

Expiration of the pivi-contentSigning certificate shall be later than the expiration of the PIVI hardware and PIVI cardAuth certificates.

CAs shall describe their key changeover procedures in the applicable CPS. Key changeover procedures will establish key rollover certificates where a certificate containing the old public key will be signed by the new private key, and a certificate containing the new public key will be signed by the old private key.

The validity period of the Subscriber certificate shall not exceed the routine re-key Identity Requirements as specified in Section 3.3.1.

After a CA performs a Key Changeover, the CA may continue to issue CRLs with the old key until all certificates signed with that key have expired. As an alternative, after all certificates signed with that old key have been revoked, the CA may issue a final long-term CRL using the old key, with a nextUpdate time passed the validity period of all issued certificates. This final CRL shall be available for all relying parties until the validity period of all issued certificates has passed. Once the last CRL has been issued, the old private signing key of the CA may be destroyed.

5.7 COMPROMISE & DISASTER RECOVERY

CAs shall have an incident handling procedure, which documents any security incidents. Security incidents include violation or threat of violation to the system, improper usage, malicious or anomalous activity and violations of the CP or CPS/KRPS.

5.7.1 Incident and Compromise Handling Procedures

If a CA or CSS detects a potential penetration it shall perform an investigation to determine the nature and extent of damage. If a CA or CSS key is suspected of compromise, the procedures in Section 5.7.3 shall be followed. Otherwise, the damage shall be assessed to determine if the remediation required will be to rebuild the impacted servers, revoke a set of certificates, and/or declare a CA or CSS key compromise.

The TBCA shall notify the members of the TPMA and all parties cross-certified with the TBCA if any of the following incidents occur:

- suspected or detected compromise of the TBCA systems;
- physical or electronic attempts to penetrate TBCA systems;
- denial of service attacks on TBCA components; and

- any incident preventing the TBCA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

This will allow member entities to protect their interests as Relying Parties.

The TOA shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the TBCA CPS.

In the event of an incident as described above, the TOA shall notify the FPKIPA within 24 hours of incident discovery, along with preliminary remediation analysis. Within 10 business days of incident resolution, TSCP shall post a notice on its public web page identifying the incident and provide direct notification to the FPKPA. The public notice shall 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 complete list of all certificates that were either issued erroneously or not compliant with the CP/CPS as a result of the incident; and
- A statement that the incident has been fully remediated.

The notification provided directly to the FPKIPA shall also include detailed measures taken to remediate the incident.

Entity CAs shall provide notice as required by the applicable MTFSA and whenever the revocation of a cross-certificate is planned.

Entity CMSs 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.

Entity CAs shall provide notice to the TPMA of the following;

- suspected or detected compromise of an Entity CA system;
- physical or electronic attempts to penetrate the Entity CA system or systems;
- denial of service attacks on Entity CA components;
- any incident preventing the Entity CA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL;
- suspected or detected compromise of a CMS; and
- suspected or detected compromise of an RA.

In the event of an incident as described above, the Entity CA shall notify the TPMA within 24 hours of incident discovery, along with preliminary remediation analysis. Within 10 business days of incident resolution, the Entity shall post a notice on its public web page identifying the incident and provide direct notification to the TPMA. The public notice shall 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 complete list of all certificates that were either issued erroneously or not compliant with the CP/CPS as a result of the incident; and
- A statement that the incident has been fully remediated.

The notification provided directly to the TPMA shall also include detailed measures taken to remediate the incident.

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

When CA or CSS computing resources, software, and/or data are corrupted, the CA or CSS shall respond as follows:

- Before returning to operation, ensure that the system's integrity has been restored;
- If the CA signature keys are not destroyed**,** CA operation shall be reestablished, giving priority to the ability to generate certificate status information within the CLR issuance schedule specified in Section 4.9.7;
- 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 notified immediately;
- If the ability to revoke Certificates is damaged, the CA shall re-establish revocation capabilities as quickly as possible in accordance with procedures set forth in the applicable CPS;
- If the CA's revocation capability cannot be recovered in a reasonable timeframe, the CA shall determine whether the 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 no longer trust the Root CA as a trust anchor.; and
- If the CA signature keys are destroyed, CA operation shall be reestablished as quickly as possible, giving priority to the generation of a new CA key pair.

In the event of an incident as described above, the TBCA shall post a notice on its web page identifying the incident and provide direct notification to the FPKIPA. For Entity CA/CSS in the event of an incident as described above, the Entity CA/CSS shall post a

notice on its web page identifying the incident and provide direct notification to the TPMA. See Section 5.7.1 for contents of the notice.

5.7.3 Private Key Compromise Procedures

5.7.3.1 CA Private Key Compromise Procedures

If a CA signature key is compromised or lost (such that compromise or loss is possible even though not certain):

- The CA shall immediately securely notify the TPMA and any entities known to be distributing the CA certificate (e.g., in a root store);
- The CA shall request revocation of any certificates issued to the compromised CA;
- A new CA key pair shall be generated by the CA in accordance with procedures set forth in Section 6.1;
- New CA certificates shall be issued to Entities in accordance with this CP;
- If the CA distributes its key in a self-signed certificate (e.g., Root CA), the new self-signed certificate shall be distributed as specified in Section 6.1.4; and
- The TBCA or Entity CA governing body shall also investigate what caused the compromise or loss, and what measures shall be taken to preclude recurrence.

5.7.3.2 KRS Private Key Compromise Procedures

In the event that the KED or DDS is compromised or suspected of compromise, the following operations shall be performed:

- Notify TPMA of the compromise;
- Provide detail concerning the root cause, operational impact, and initial remediation actions;
- Determine the extent of the compromise; and
- Gain concurrence from the TPMA, which will consult with the FPKIPA on planned resolution. This may include revocation of certificates associated with the compromised private keys stored in the KED or DDS.

If a KRA or KRO certificate is revoked due to compromise, the potential exists for some Subscribers' escrowed keys to have been exposed during a recovery process, and the following operations shall be performed:

- Audit record review by the audit administrator to identify all potentially exposed escrowed keys;
- Revocation of each of the potentially exposed escrowed keys, according to procedures specified in Section 4.9.3, including notifying each affected Subscriber of revocation; and
- Reissuance of the KRA or KRO authentication certificate.

5.7.4 Business Continuity Capabilities after a Disaster

The CA repository system shall be deployed to provide 24-hour, 365 day per year availability with a high level of repository reliability.

CAs shall have recovery procedures in place to reconstitute the CA after a failure.

In the case of a disaster whereby all of TBCA's installations are physically damaged and all copies of the CA Signing Key are destroyed as a result, the TPMA shall immediately notify the FPKIPA so that the FPKIPA can take appropriate action. The TBCA shall also follow the requirements for key compromise as defined in Section 5.7.3.

In the case of a disaster whereby all of an Entity CA's installations are physically damaged and all copies of the CA Signing Key are destroyed, the Entity PMA shall immediately notify the TPMA so that the TPMA can take appropriate action. The Entity CA shall also follow the requirements for key compromise as defined in Section 5.7.3.

5.8 CA, CMS, CSS & RA TERMINATION

In the event of termination of TBCA operations, whenever possible, the TPMA shall notify the FPKIPA at least two weeks prior to the termination of operations. For emergency termination, the TBCA shall follow the notification procedures specified in Section 5.7. Certificates signed by the TBCA shall be revoked and the TPMO shall advise entities that have entered into MTFSAs with the TSCP that the TBCA operation has terminated so they may revoke certificates they have issued to the TBCA. Prior to TBCA termination, the TOA shall provide all archived data to an archival facility. Any issued certificates that have not expired shall be revoked and a final long term CRL with the nextUpdate time past the validity period of all issued certificates shall be generated. This final CRL shall be available for all relying parties until the validity period of all issued certificates has passed. Once the last CRL has been issued, the private signing key(s) of the TBCA shall be destroyed.

Entities will be given as much advance notice as circumstances permit and attempts to provide alternative sources of interoperation will be sought in the event the TBCA is terminated.

In the event that an Entity CA terminates operation, the Entity shall:

- Whenever possible, provide notice to the TPMA at least two weeks and a day, which notice period will begin to run upon written acknowledgement of the TPMA, prior to termination of any CA operated by an Entity cross certified with the TPMA. For emergency termination, CAs shall follow the notification procedures in Section 5.7;
- Request revocation on a date certain of all cross-certificates issued to the Entity;

- The CA, CMS, CSS, RA, and KRS shall archive all audit logs and records prior to termination;
- The CA, CMS, CSS, RA, and KRS shall destroy all of its private keys upon termination;
- The CA, CMS, CSS, RA, and KRS shall transfer all archive records to an appropriate authority (e.g., the PMA responsible for the entity); and

- If a Root CA is terminated, the CA shall use secure means to notify the Subscribers to delete all trust anchors representing the terminated CA Technical Security Controls.

6. TECHNICAL SECURITY CONTOLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

Cryptographic keying material shall be generated in FIPS 140 validated cryptographic modules according to the following minimum requirements:

Entity Role / Certificate Profile	FIPS 140-2 Level	Hardware or Software	Key Storage Restricted to the Module on which the Key Was Generated
CA	3	Hardware	Yes
CMS **(Including CMS Master Key)**	2[3]	Hardware	Yes
CSS (e.g. OCSP, SCVP)	2	Hardware	Yes
RA	2	Hardware	Yes
Code Signing	2	Hardware	Yes
id-PIVI **id-PIVI-ContentSigning** **id-PIVI-CardAuth**	2	Hardware	Yes
id-mediumHardware **id-mediumHardware-CBP**	2	Hardware	Yes, for all certificate profiles except for End Entity Encryption
id-Basic **id-mediumSoftware** **id-mediumSoftware-CBP**	2	Software	No

[3] Unless the CMS is considered a key server within the CA CP/CPS, in which case FIPS 140-2

Key generation events should use the configuration that was the basis of the FIPS or another approved standard (e.g. FIPS Mode, equivalent international standard as approved by the PMA). If the required keys cannot be generated while in an approved configuration, the specific configuration and reason of the use of a different method should be documented by the CA.

Random numbers shall be generated within FIPS 140 Level 2 validated hardware cryptographic modules for id-MediumHardware, id-MediumHardware-CBP, id-PIVI, id-PIVI-ContentSigner, and id-PIVI-CardAuth.

When Private Keys are not generated on the cryptographic module to be used, originally generated Private Keys shall be destroyed after they have been transferred to the replacement cryptographic module. This does not prohibit a key generating module from being repurposed. This does not prohibit the key generating module to act as the key escrow module.

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

Multiparty control requirements in Section 5.2.2 apply.

An independent third party shall validate the execution of the key generation.

Practice Note: This may be through witnessing key generation directly or by examining the signed and documented record of the key generation.

For CMS, activation of the CMS Master Key shall require strong authentication of Trusted Roles. Key diversification operations shall occur on the Hardware Security Module (HSM). Use of these keys requires PIV-I Hardware or commensurate. The diversified keys shall only be stored in hardware cryptographic modules that support certificates issued at the id-PIVI assurance levels. 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

CAs shall generate their own Key Pair and therefore do not need Private Key delivery.

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

When CAs or RAs generate keys on behalf of the Subscriber, then the private key must be delivered securely to the Subscriber. Private keys may be delivered electronically or may be

---

Level 3 is required.

delivered on a hardware cryptographic module. In all cases, the following requirements must 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 key to the Subscriber;
- The private key must be protected from activation, compromise, or modification during the delivery process;
- The Subscriber shall acknowledge receipt of the private key(s); and
- 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 must 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. Activation data shall be delivered using a separate secure channel.
    - For shard key applications, organizational identities, and network devices, see also Section 3.2.

The CA (or RA) must maintain a record of the subscriber acknowledgement of receipt of the cryptographic module.

6.1.3 Public Key Delivery to Certificate Issuer

Where key pairs are generated by the Subscriber, CMS, or RA, the public key and the Subscriber's identity must 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 must be at least as strong as the Subscriber Key Pair.

6.1.4 CA Public Key Delivery to Relying Parties

When a CA updates its signature key pair, the CA shall distribute the new public key in a secure fashion. The new public key may be distributed in a self-signed certificate, in a key rollover certificate, or in a new CA (e.g., cross-) certificate obtained from the issuer(s) of the current CA certificate(s).

Self-signed certificates shall be conveyed to relying parties in a secure fashion to preclude substitution attacks.

Acceptable methods for self-signed certificate delivery include:

- The CA loading a self-signed certificate onto tokens delivered to Relying Parties via secure mechanisms;
- Secure distribution of self-signed certificates through secure out-of-band mechanisms;
- Comparison of the hash of the self-signed certificate against a hash value made available via authenticated out-of-band sources (note that hashes posted in-band along with the certificate are not acceptable as an authentication mechanism); and

- Loading certificates from web sites secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded. The web site certificate shall not be issued by a CA subordinated to the self-signed CA.

Practice Note: EV-SSL and EV-TLS certificates stored in a FIPS 140-2 Level 3 HSM are considered equivalent to id-MediumHardware and id-PIVI assurance levels and are accepted for the purposes of trust anchor distribution.

Key rollover certificates are signed with the CA's current private key, so secure distribution is not required.

Practice Note: To ensure the availability of the new public key, the key rollover certificates should be distributed using repositories.

CA Certificates that are signed by another CA's current private key are protected, so secure distribution is not required.

6.1.5 Key Sizes

If the security of a particular algorithm becomes compromised, the TPMA or TPMO may require CAs to revoke affected certificates, according to the terms of the applicable MTFSA.

All certificates, CRL, OCSP Responses, and cryptographic network protocols (e.g. TLS) materially relied on or issued by the PKI shall use the following key sizes and algorithms:

Cryptographic Function	**Issued on or by 12/31/2030**	**Expires after 12/31/2030**
Signing (per FIPS 186-5)	2048 bit RSA Or 256 bit prime field or 233 bit binary field ECDSA	3072 or 4096 bit RSA Or 256 bit prime field or 283 bit binary field ECDSA
Asymmetric Encryption (Per PKCS1 for RSA and per 800-56A for ECDH)	2048 bit RSA Or 256 bit prime field or 233 bit binary field ECDH	3072 or 4096 bit RSA Or 256 bit prime field or 283 bit binary field ECDH
Symmetric Encryption	3 Key TDES (Deprecated; may be used until 12/31/2023) or AES	AES

The hashing algorithm used for certificates, CRL, and OCSP Responses shall meet the following minimum requirements:

id-Medium, id-Medium-CBP, id-MediumHardware, id-MediumHardware-CBP			
Scope		**Issued before or on- 12/31/2030**	**Issued after 12/31/2030**
Certificates		SHA-224 or SHA-256	SHA-384
CRL		SHA-224 or SHA-256	SHA-384
Pre-Signed OCSP Responses		SHA-224 or SHA-256	SHA-384
id-PIVI, id-PIVI-ContentSigner, id-PIVI-cardAuth			
Certificates, CRLs, OCSP Reponses (pre-signed and non-pre-signed)		SHA-256	NA

CRLs, OCSP Responder Certificates, and OCSP Responses shall use the same or better signature algorithm, key size, and hash algorithm used for the certificate that is being validated.

All end-entity certificates at the id-PIVI, id-PIVI-CardAuth, and id-PIVI-ContentSigner assurance levels shall contain public keys and algorithms that conform to [NIST SP 800-78].

KED and DDS keys shall be equal to or stronger than the keys being escrowed.

6.1.6 Public Key Parameters Generation and Quality Checking

RSA keys and prime numbers shall be generated and tested in accordance with FIPS 186-5.

ECDSA and ECDH keys shall be generated in accordance with FIPS 186-5. Curves in FIPS 186-5 shall be used.

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

Public keys that are bound into certificates shall be certified for use in signing or encrypting, but not both, except as specified below. The use of a specific key is determined by the key usage extension in the X.509 certificate. The following table describes the rules for asserting key usage extensions:

Human Subscriber	
Key Use	**Key Usage Extensions**
Identity	Set: digitalSignature bit only
Digital Signature	Set: digitalSignature, nonRepudiation bits Not Set: keyEncipherment, keyAgreement bits
Encryption	Set: keyEncipherment, dataEncipherment (optional)
Key Agreement	Set: keyAgreement
Device	
Key Use	**Key Usage Extensions**
Identity	Set: digitalSignature, keyEncipherment (optional) –Dual use only used for SSL/TLS web device certs
CA	
Key Use	**Key Usage Extensions**
Issuing Certificates	Set: cRLSign, keyCertSign bits
CSS	
Key Use	**Key Usage Extensions**
Signing OCSP Responses	Set: digitalSignature, nonRepudiation bits

For End Entity PIV-I certificates issued after June 30, 2019, the Extended Key Usage extension shall always be present and shall not contain *anyExtendedKeyUsage* {2.5.29.37.0}, Extended Key Usage OIDs shall be consistent with key usage bits asserted.

If a certificate is used for authentication of ephemeral keys, the Key Usage bit in the certificate must assert the digital signature and/or nonrepudiation bits and may or may not assert the Key Encryption and Key Agreement depending on the public key in the certificate.

Certificates at the id-PIVI-ContentSigning assurance level shall only include an extended key usage of *id-fpki-pivi-content-signing* (see Section 10.22).

Extended key usage OIDs shall be consistent with the key usage bits set. See Section 10.22 for additional requirements pertaining to extended key usage.

6.2 PRIVATE KEY PROTECTION & CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards & Controls

The relevant standard for cryptographic modules is FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*. The TPMA may determine that other comparable and equivalent validation, certification, or verification international standards are sufficient.

Cryptographic modules shall be validated to the FIPS 140-2 level identified in Section 6.1.1 or higher. Additionally, the TPMA reserves the right to review technical documentation associated with any cryptographic modules under consideration for use by CAs.

PIV-I Cards are PKI tokens that have private keys associated with certificates asserting policies mapped to PIV-I hardware or PIV-I-cardAuth. See Section 12 for PIV-I requirements.

6.2.1.1 Custodial Subscriber Key Stores

Custodial Subscriber Key Stores hold keys for a number of Subscriber certificates in one location. When a collection of private keys for Subscriber certificates is held in a single location, there is a higher risk associated with compromise of that cryptographic module than that of a single Subscriber. Cryptographic modules for Custodial Subscriber Key Stores shall be no less than FIPS 140 Level 2 Hardware. In addition, authentication to the Cryptographic Device to activate the private key associated with a given certificate shall require authentication commensurate with the assurance level of the certificate.

6.2.2 Private Key Multi-Person Control

Use of a CA private signing key or id-PIVI-ContentSigning key shall require action by multiple persons as set forth in Section 5.2.2 of this CP.

6.2.3 Private Key Escrow

Under no circumstances shall a signature key be escrowed.

For human subscribers, private keys used for encryption shall be escrowed.

Subscriber private dual use keys shall not be escrowed. If a device has a separate key management key certificate, the key management key may be escrowed.

For devices, private keys used for encryption shall be escrowed except where the encrypted data will not need to be recovered.

Escrow, when required, shall be completed prior to certificate issuance.

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Private Signature Key

CA private signature keys shall be backed up under multi-person control, as specified in Section 5.2.2.

A copy of the CA private signature key shall be stored at or near the CA location and offsite.

Procedures for key backup shall be defined in the applicable CPS.

All copies of the CA private signature key shall be accounted for and protected in the same manner as the original.

6.2.4.2 Backup of Subscriber Private Signature Key

At the id-Basic, id-MediumHardware, id-MediumHardware-CBP, id-PIVI, and id-PIVI-cardAuth assurance levels, Subscriber private signature keys may not be backed up or copied.

At the id-Medium and id-Medium-CBP assurance levels , Subscriber private signature keys may be backed up or copied but must be held in the Subscriber's control. Backed up subscriber private signature keys shall not be stored in plain text form outside the cryptographic module.

Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module.

6.2.4.3 Backup of Subscriber Key Management Private Keys

Backed up Subscriber key management keys shall not be stored in plain text form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module.

6.2.4.4 Backup of CSS Private Key

CSS private keys may be backed up. If backed up, all copies shall be accounted for and protected in the same manner as the original.

6.2.4.5 Backup of id-PIVI-ContentSigning Key

Keys at the id-PIVI-ContentSigning assurance level shall be backed up under multi-person control, as specified in Section 5.2.2.

A copy of the key shall be stored at or near the CMS location and off site.

All copies of the id-PIVI-ContentSigning private signature key shall be accounted for and protected in the same manner as the original.

Procedures for key backup shall be defined in the applicable CPS.

6.2.4.6 Backup of Device Private Keys

Device private keys may be backed up or copied but must be held under the control of the device's human sponsor or other authorized administrator. Backed up device private keys shall not be stored in plaintext form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the device's cryptographic module.

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, CMS, & CSS private keys may be exported from the cryptographic module in accordance with key backup procedures as described in Section 6.2.4.

At no time shall a CA, CMS, or CSS private key exist in plain text outside the cryptographic module.

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 if the keys are not accessible without an authentication mechanism that is in compliance with the FIPS 140-2 rating of the

cryptographic module. The cryptographic module storing the key shall be at least as strong as that required in Section 6.1.1.

6.2.8 Method of Activating Private Keys

The user must be authenticated to the cryptographic module before the activation of any private key(s). 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 id-PIVI-cardAuth user activation of the private key is not required.

6.2.9 Methods of Deactivating Private Keys

Cryptographic modules that have been activated shall be protected from unauthorized access. After use, the 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.

CA, CMS, and CSS Hardware cryptographic modules shall be removed and stored in a secure container when not in use.

6.2.10 Method of Destroying Private Keys

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 likely be accomplished by executing a “zeroize” command. For CA, RA, CMS, and CSS private signature keys, the keys shall be destroyed by individuals in Trusted Roles.

Physical destruction of hardware is not generally required.

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 shall be 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 & Installation

The activation data used to unlock private keys, in conjunction with any other access control, 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.

For Medium Assurance and above, RA and Subscriber activation data may be user-selected. For CAs, activation data shall either be biometric data or satisfy the policy enforced at/by the cryptographic module. The strength of the activation data must meet or exceed the requirements for authentication mechanisms stipulated for Level 2 in [FIPS 140].

For PIV-I Hardware and PIVI-cardAuth, in the event activation data can be reset by an issuer after a card is locked, after a successful authentication of the Subscriber. This authentication must be conducted in accordance with FIPS 201, Section 2.9.3 by a Trusted Agent of the issuer.

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 shall be:

- Memorized;
- biometric in nature; or
- recorded and secured at the level of assurance associated with the activation of the cryptographic module and shall not be stored with the cryptographic module.

The protection mechanisms shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as defined in the applicable CPS.

To protect against repeated guessing attacks, data protection shall include a temporary lock-out mechanism and termination of applications after a specified number of log-in attempts. The number of attempts allowed shall be specified in the Entity CP or CPS.

Activation data that is transmitted shall be transported via an appropriately protected channel that is distinct in time and place from the associated cryptographic module.

6.4.3 Other Aspects of Activation Data

CA, CMS, CSS, and RA shall change activation data whenever the token is re-keyed or returned for maintenance.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

CA, CMS, CSS, KED, DDS, and RA shall provide computer security functionality through operating system, software, and physical safeguards. The CA and its ancillary parts shall include

the following functionality (these functions pertain to all System Software Layers, where applicable):

- Require authenticated logins;
- Manage privileges of users to limit users to their assigned roles;
- Provide Discretionary Access Control;
- Generate and archive audit records for all transactions (see Section 5.4);
- Restrict access control to CA services and PKI roles;
- Enforce separation of duties for PKI roles;
- Require identification and authentication of PKI roles and associated identities;
- Prohibit object re-use;
- Require use of cryptography for session communication and database security;
- Require a trusted path for identification and authentication;
- Enforce domain integrity boundaries for security critical processes;
- Require self-test security related CA services;
- Support recovery from key or system failure; and
- CAs shall have a recovery mechanism for keys and the CA system.

For remote workstations used to administer the CAs, KEDs, and DDSs, the computer security functions listed below are required:

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- generate and archive audit records for all transactions; (see Section 5.4);
- enforce domain integrity boundaries for security critical processes;
- provide residual information protection; and
- require recovery from system failure.

All communications between any PKI trusted role and the CA must be authenticated and protected from modification.

When CA equipment is hosted on evaluated platforms in support of computer security assurance requirements then the system (hardware, software, operating system) shall, when 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.

CA equipment shall be configured with a minimum of the required accounts, and network services.

6.5.2 Computer Security Rating

No stipulation for TBCA.

Entity CAs shall identify any Computer Security Rating requirements.

6.6 LIFE-CYCLE SECURITY CONTROLS

6.6.1 System Development Controls

The System Development Controls for CA, CMS, CSS, KRS, including Remote Workstations that administer to the CA, CMS, CSS, and KRS are as follows:

- For commercial off-the-shelf software, the software shall be designed and developed under a formal, documented development methodology;
- Where open-source software has been utilized, the Entity CA shall demonstrate that security requirements were achieved through software verification & validation and structured development/lifecycle management;
- Procured Hardware and software shall be purchased and shipped 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);
- Custom developed hardware and software shall be developed in a controlled environment and the development process shall be defined and documented;
- Hardware (e.g. HSM, Computers, and Firewalls) 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, including all System Software Layers, shall be dedicated to operating and supporting the CA (i.e., the system and services dedicated to the issuance and management of certificates). There shall be no other applications; hardware devices, network connections, or component software installed which is not part of the PKI operation, administration, monitoring, and security compliance of the system. CA hardware and system software layers may support multiple CAs and their supporting systems, provided all systems have comparable security controls and are dedicated to the support of the CA in compliance of the same CP;
- All System Software Layers shall operate in the same security zone as the CA;
- Proper care shall be taken to prevent malicious software from being loaded onto the equipment. Software required to perform PKI operations shall be obtained from authorized sources. Except for offline CAs, CA, and RA Hardware and software shall be scanned for malicious code on first use and periodically thereafter; and
- Hardware and software updates shall be purchased or developed in the same manner as original equipment and be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of the CA, CMS, CSS, KED, and KRS equipment as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the CA, CMS, CSA, KED and KRS software or configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance of the CA, CMS, CSS, KED and KRS equipment. The CA, CMS, CSS, KED and KRS software, when first loaded, shall be verified as being supplied from the vendor, with no modifications, and be the version intended for use.

6.6.3 Life Cycle Security Ratings

CAs shall identify any life cycle security control requirements in the applicable CP.

6.7 NETWORK SECURITY CONTROLS

Root CAs and their internal PKI repositories shall be offline.

Online CAs, CMSs, CSSs, KRSs and Remote Workstations used to administer them, and RAs, and directories containing CA and CRL publications (or distribution) points shall employ appropriate security controls to protect against denial of service and intrusion. Such measures shall include the use of guards, firewalls, and filtering routers. Networking equipment shall turn off unused network ports and services. Any network software present shall be necessary for PKI operations.

Protection of CA and KRS equipment shall be provided against known network attacks.

Any boundary control devices used to protect the network on which 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.

Any remote workstation used to administer the CA must use a Virtual Private Network (VPN) to access the CA. The VPN must be configured for mutual authentication, encryption, and integrity. If mutual authentication is shared secret based, the shared secret must be changed at least annually, must be randomly generated, and must have entropy commensurate with the cryptographic strength of certificates issued by the PKI being administered. The CA shall permit remote administration only after successful multi-factor authentication of the Trust Role at a level of assurance commensurate with that of the CA.

6.8 TIME STAMPING

All CA, CMS, and CSS equipment 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 this time service shall be used for establishment of the following times:

- Initial validity time of a Subscriber's Certificate;
- Revocation of a Subscriber's Certificate;
- Posting of CRL Updates and CRL validity time;
- OCSP or other CSS responses; and
- Audit Log Timestamps.

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, see Section 5.4.1.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

PIV-I authentication, card authentication and content signing certificates shall conform to the relevant profile worksheets in the FBCA-PROF.

All other certificates shall be compatible with X.509 Certificate and CRL Extensions Profile FBCA-PROF.

7.1.1 Version Numbers

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

7.1.2 Certificate Extensions

All CA use of standard certificate extensions shall comply with RFC 5280.

CA certificates shall not include critical private extensions. When used in Subscriber certificates, critical private extensions shall be interoperable in their intended community of use.

Entity CAs that use PIV-I Certificates shall comply with relevant worksheets from FBCA-PROF and the associated CSS certificates shall also comply with FBCA-PROF.

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. Section 10 contains the certificate formats.
Interoperability testing shall be completed by testing a representative set of end user applications for successful certificate usage.

7.1.3 Algorithm Object Identifiers

Certificates issued by CAs shall identify the signature algorithm using one of the following OIDs:

Signature Algorithm	Object Identifier
sha256WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 } (1.2.840.113549.1.1.11)
sha384WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12 } (1.2.840.113549.1.1.12)
Sha512WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13 } (1.2.840.113549.1.1.13)

Id-RSASSA-PSS	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10 } (1.2.840.113549.1.1.10)
ecdsa-with-SHA256	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2 } (1.2.840.10045.4.3.2)
ecdsa-with-SHA384	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 } (1.2.840.10045.4.3.3)
edsa-with-SHA512	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4 } (1.2.840.10045.4.3.4)

The PSS padding scheme OID is independent of the hash algorithm. The hash algorithm is specified as a parameter (for details, see PKCS#1). The following are approved hash algorithms:

id-sha256	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1 } (2.16.840.1.101.3.4.2.1)
id-sha384	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 2 } (2.16.840.1.101.3.4.2.2)
id-sha512	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3 } (2.16.840.1.101.3.4.2.3)

Certificates issued by CAs shall identify the cryptographic algorithm associated with the subject public key using one of the following OIDs:

Public Key Algorithm	**Object Identifier**
rsaEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 } (1.2.840.113549.1.1.1)
id-ecPublicKey	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1 } (1.2.840.10045.2.1)

When non-CA certificates issued on behalf of federal agencies contain an elliptic curve public key, the parameters shall be specified as one of the following named curves:

Curve	Object Identifier
ansip256r1	{ iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7 } (1.2.840.10045.3.1.7)
ansip384r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 34 } (1.3.132.0.34)

For id-PIVI, id-PIVI-cardAuth, and id-PIVI-contentSigning assurance levels, signature algorithms are limited to those identified by NIST SP 800-78.

7.1.4 Name Forms

The subject and issuer fields of the certificate shall be populated with an X.500 Distinguished Name. Distinguished names shall be composed of standard attribute types found in RFC 5280.

CA Subject and Issuer Name Form

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.

End Entity Name Form

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, email, etc.
	Optional	OU	0…N	As needed
	Required	O	1	Issuer name, e.g., “O=XYZ Inc” within an authorized name space
	Required	C	1	Country name, e.g., “C=US” within an authorized name space
2	Required	See Content description	1…N	Additional naming attributes for uniquely identifying the subject including common name, serialNumber, email, etc.
	Optional	OU	0…N	As needed
	Optional	O	0…1	Issuer name, e.g., “O=XYZ Inc” within an authorized name space
	Required	DC	1	Domain name, e.g., “DC=xyzinc” within an authorized name space
	Required	DC	1…N	Domain root label(s), e.g., “DC=com” or “DC=com, DC=au”, etc. within an authorized name space

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

CA certificates issued by the TBCA may have name constraints asserted to limit the name space of the Principal CAs to the scope appropriate for their domains. In circumstances where the TBCA does not assert name constraints, Entity CA shall disclose to the TBCA the name space appropriate for their domains and evidence that such domains are in fact appropriate.

Entity CAs may assert critical or non-critical name constraints beyond those specified in the Certificate Profiles enumerated in Section 10.

7.1.6 Certificate Policy Object Identifier

Except for Self-Signed Root CA, all CA and Subscriber Certificates issued under this CP shall assert one or more of the certificate policy OIDs listed in Section 1.2. When a CA asserts a policy OID (for both CA certificates and issued end entity certificates), it shall also assert all policy OIDs corresponding to the lower assurance levels defined in this CP.

Certificates issued for PIV-I card authentication or PIV-I content signing must not express any other policy OIDs.

Delegated OCSP Responder certificates must assert all policy OIDs for which they are authoritative.

7.1.7 Usage of Policy Constraints Extension

Certificates issues by the TBCA shall assert the policy constraints extensions to inhibit policy mapping.

Certificates issued by TBCA to other Bridge CAs shall assert inhibit policy mapping with a skipCerts value of 1.

CAs may assert policy constraints in CA certificates only where specifically allowed in the Certificate Profiles in this CP (See Section 10. to ensure interoperability).

For Subordinate CA certificates *inhibitPolicyMappings*, skipCcerts shall be set to 0.

7.1.8 Policy Qualifiers Syntax & Semantics

Certificates issued under this CP may contain policy qualifiers such as user notice, policy name, and CP and CPS pointers as identified in RFC 5280.

Certificate issued by Entity PKIs may contain policy qualifiers identified in RFC 5280.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Processing semantics for the critical Certificate Policy extension shall conform to X.509 certification path processing rules. Certificate shall contain a non-critical certificate policies extension.

7.1.10 Inhibit Any Policy Extension

CAs may assert *inhibitAnyPolicy* in CA certificates. When present, this extension may be marked critical. Skip certs must 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 integrate value of ‘1’).

7.2.2 CRL Entry Extensions

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

Section 10. contains the CRL profiles.

7.3 OCSP PROFILE

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

If implemented, CSS must sign responses using algorithms designated for CRL signing.

All CSSs shall accept and return SHA-2 hashes in the CertID and responderID fields. CSS may accept and return additional hash algorithms within the CertID fields. CSSs shall not return any response containing a hash algorithm in the CertID that differs from the -CertID in the request.

7.3.1 Version Number

The version number for request and responses shall be v1.

7.3.2 OCSP Extensions

Responses shall support the nonce extension. Critical OSCP extensions shall not be used.

8. COMPLIANCE AUDIT & OTHER ASSESSMENTS

CAs shall have a compliance audit mechanism in place to ensure that the requirements of this CP their CP, KRP, CPS and KRPS, as applicable, are being implemented and enforced.

CAs shall be responsible for ensuring audits are conducted for all PKI functions regardless of how or by whom the PKI components are managed and operated.

8.1 FREQUENCY OF AUDIT OR ASSESSMENTS

Entity PKIs shall be subject to a PKI compliance audit at least once per year for High, Medium Hardware, PIV-I Card Authentication, and Medium Assurance, and at least once every two years for Basic Assurance. The audit shall include all CAs, as well as CSSs, CMSs, RAs, KRSs, and supporting repositories. Where a status server is specified in certificates issued by a CA, the status server shall be subject to the same compliance audit requirements as the corresponding CA. For example, if an OCSP server is specified in the authority information access extension in certificates issued by a CA, that server must be reviewed as part of that CA's compliance audit.

The Entity PMAs have the right to require periodic and aperiodic compliance audits or inspections of subordinate CA, RA, or KRS operations to validate that the subordinate entities are operating in accordance with the security practices and procedures described in their respective CPS or KRPS as applicable. Further, the TPMA has the right to require aperiodic compliance audits of Entity PKIs (and, when needed, their subordinate CAs) that interoperate with the TPMA. The TPMA shall state the reason for any aperiodic compliance audit.

On an annual basis, for each PIV Card Issuer (PCI) configuration used (as defined by the FIPS 201 Evaluation Program), one populated, representative PIV-I card shall be submitted to the FIPS 201 Evaluation Program for testing.

8.2 IDENTITY & QUALIFICATIONS OF ASSESSOR

The external independent auditor must demonstrate competence in the field of compliance audits and at the time of the audit, the applicable CP. The external independent auditor must perform such compliance audits as a regular ongoing business activity.

.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The external independent 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 external independent auditor may not have served the entity in developing or maintaining the entity's PKI Facility, associated IT and network systems, or CPS. The TPMA shall determine whether an external independent auditor meets this requirement.

In the event an entity chooses to engage external independent auditor services internal to its parent organization, it shall undergo an audit from an external third-party audit firm no less often than every third year.

8.4 TOPICS COVERED BY ASSESSMENT

The purpose of an external independent compliance audit of a PKI shall be to verify that an entity and its CAs and RAs are complying with the requirements of the applicable CP, CPS, and MTFSAs. Components other than the CA may be audited fully or by using a representative sampling. The audit shall also include a compliance analysis assessment that the applicable CPS adequately addresses the requirements of the applicable CP.

If the auditor uses statistical sampling, all PKI components, PKI component managers and operators shall be considered in the sample. The samples shall vary on an annual basis.

A full compliance audit for the PKI covers all aspects within the scope identified herein.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

For the TBCA, when the external independent auditor finds a discrepancy between how the TBCA is designed or is being operated or maintained, and the requirements of this CP, the MTFSAs, or the applicable CPS, the following actions shall be performed:

- The external independent auditor shall document the discrepancy and provide a copy to the TPMO;
- The TPMO will provide a copy of the discrepancy documentation to the TPMA Chair and report the findings and planned corrective action to the TPMA;
- The TPMA shall determine what further notifications or actions are necessary to meet the requirements of this CP and the MTFSAs, and then proceed to make such notifications and take such actions without delay; and
- Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the TPMA may direct the TPMO to take additional actions as appropriate, including temporarily halting operation of the TBCA.

For Entity CAs, when the external independent auditor finds a discrepancy between how the CA is designed or is being operated or maintained, and the requirements of the Entity CP, any applicable MTFSAs, or the applicable CPS, the following actions shall be performed:

- The external independent auditor shall document the discrepancy;
- The external independent auditor shall notify the Entity of the discrepancy;
- The Entity shall notify the TPMA without delay and provide a remediation plan;
- The Entity PKI shall determine what further notifications or actions are necessary to meet the requirements of the Entity CP, CPS, and any relevant MTFSA provisions; and
- The Entity PKI shall proceed to make such notifications and take such actions without delay.

When the TPMA receives a report of audit deficiencies from an Entity PKI, the TPMA may direct the PMO to take additional actions to protect the level of trust in the infrastructure.

8.6 COMMUNICATION OF RESULTS

On an annual basis, the Entity PKI PMA shall submit a compliance audit package to the TPMA. This package shall be prepared in accordance with the "Compliance Audit Requirements" document and shall 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 used in the assessment.

For TBCA cross-certifications established with another Bridge (e.g., cross-certification with the FBCA), the TPMO shall submit a compliance audit package to that Bridge's Management Authority (e.g., the FPKIMA) in compliance with the relevant MTFSA provisions.

Additionally, where necessary, the results shall be communicated as set forth in Section 8.5 above.

Practice Note: Components of the PKI may be audited separately. In such cases, the compliance audit package may include multiple audit reports (e.g. one per component) or the audit results may be aggregated by the CA compliance auditor..

9. OTHER BUSINESS & LEGAL MATTERS

9.1 CERTIFICATE ISSUANCE/RENEWAL FEES

CAs may set reasonable fees for issuance and renewal transactions provided that such fees are in accordance with the terms of the MTFSA.

9.1.1 Certificate Access Fees

CAs shall not charge fees for accessing a certificate (e.g. PKI Repository Access).

9.1.2 Revocation or Status Information Access Fee

CAs shall not charge fees for accessing revocation or status information (e.g. PKI Repository Access, OCSP Responder Requests).

9.1.3 Fees for other Services

CAs may set reasonable fees for other services provided that such fees are in accordance with the terms of the MTFSA between CAs and subject to applicable law.

9.1.4 Refund Policy

No stipulation.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

Entities who are CA, CMS, CSS, or RA shall maintain reasonable levels of insurance coverage to address all foreseeable liability obligations to the other Entities as defined in Section 1.3.

9.2.2 Other Assets

Entities who are CA, CMS, CSS, or RA shall maintain reasonable and sufficient financial resources to maintain operations and fulfill obligations.

9.2.3 Insurance/warranty Coverage for End-Entities

Any party may offer protection to end entities beyond the protections stated in this CP.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

CA information identified in Section 2 that does not require protection shall be made available. Organizations can determine the organization information that it will make publicly available.

Entities shall handle confidential information according to the terms of the applicable MTFSA between parties.

Entities 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 it would for its own most confidential information.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

CA, CMS, RA that collect, store, process, or disclose Personally Identifiable Information (PII) and Personal Information (PI) shall adhere to a written privacy policy that is readily available to Subscribers and subject to applicable law.

9.4.2 Information treated as Private

CA, CMS, RA shall protect all subscriber PII/PI from unauthorized disclosure. The TBCA shall also protect PII/PI for Entity personnel collected to support cross-certification and MTFSA requirements from unauthorized disclosure. The contents of the archives maintained by the TOA shall not be released except as required by law.

For Entity CAs, collection of PII/PI shall be limited to the minimum necessary to validate the identity of the Subscriber. This may include attributes that correlate identity evidence to authoritative sources. The RA shall provide explicit notice to the Subscriber regarding the purpose for collecting and maintaining a record of the PII/PI necessary for identity proofing and the consequences for not providing the information. PII/PI collected for identity proofing purposes shall not be used for any other purpose.

9.4.3 Information not deemed Private

Information included in certificates is not considered private and is not subject to protections outlined in Section 9.4.2 but shall not be sold to a third party.

9.4.4 Responsibility to Protect Private Information

Private information must be stored securely and may be released only in accordance with other stipulations in Section 9.4.

All information collected as part of the identity-proofing process shall be protected to ensure confidentiality and integrity. In the event that an Entity terminates PKI activities, the Entity shall be responsible for disposing of or destroying sensitive information, including PII/PI, in a secure manner, and maintaining its protection from unauthorized access until destruction.

9.4.5 Notice and Consent to use Private Information

CA, CMS, and RA are not required to provide any notice or obtain the consent of the Subscriber or Entity personnel to release private information in accordance with the stipulations of Section 9.4.

9.4.6 Disclosure Pursuant to Judicial/Administrative Process

CAs shall disclose privacy information in judicial or administrative circumstances according to their privacy policy (See Section 9.4.1) and applicable law.

9.4.7 Other Information Disclosure Circumstances

None.

9.5 INTELLECTUAL PROPERTY RIGHTS

Entities operating under this policy shall not knowingly violate intellectual property rights held by others.

9.5.1 Property Rights in Certificates and Revocation Information

CAs shall retain the property rights to certificates and revocation information they issue.

CAs grant permission to reproduce their certificates and revocation information they issue on a non-exclusive and royalty-free basis.

9.5.2 Property Rights in the CPS

For the TBCA, this CP is owned by TSCP. and the corresponding CPS is owned and/or licensed to TSCP

For Entity CAs, property rights for their CP and corresponding CPS shall be defined in its CP.

9.5.3 Property Rights in Names

Certificate applicants retain all rights to their names (e.g. trademarks, corporate name, and personal name).

9.5.4 Property Rights in Keys

The subject of a certificate retains the rights and intellectual property associated with the corresponding private key.

9.6 REPRESENTATIONS & WARRANTIES

The obligations described below pertain to the TBCA (and, by implication, to the TOA), and to Entity CAs, which either interoperate with the TBCA or are in a trust chain up to a Principal CA that interoperates with the TBCA.

The obligations applying to Entity CAs pertain to their activities as issuers of certificates. These obligations include obligations affecting interoperability with the TBCA such as reviews or audits by the TPMA or independent auditor.

Additional representations and warranties may be included in MTFSA.

9.6.1 CA Representations and Warranties

The TBCA represents and warrant that to its knowledge:

- All TBCA signing keys which pertain to unrevoked certificates are protected, have never been compromised, and are being maintained in a manner consistent with this CP;

- The TBCA's Subscribers, if any, have been obligated to a Subscriber agreement which includes Subscriber representation and warrants. Further, the Subscriber agreement includes a representation and warranty from the Subscriber that the information 1) they have provided to the CA and 2) that is in their certificate is true and accurate;
- The TBCA has an Agreement with all Affiliated Organizations for which it presently has unrevoked certificates. The Agreement incorporates the applicable obligations from this CP and assigns them to the Affiliated Organization;
- The unrevoked certificates issued by the TBCA are being used for authorized and legal purposes; and
- The TBCA PKI repository, CRL, and Certificate Status Services (e.g. OCSP) are being maintained in a manner consistent with this CP.

Entity CA shall represent and warrant similarly in their CP. For Entity CAs issuing PIV-I certificates, they shall maintain an agreement with the Affiliated Organization specifying the obligations related to authorizing affiliation with Subscribers.

9.6.2 RA Representations and Warranties

RAs shall represent and warrant that to their knowledge the requirements imposed on the RA in the applicable CP have been met.

Practice Note: CAs retain the full accountability for the obligations in this CP pertaining to CMS, CSS, and RA even if a role is performed by a 3rd party. Therefore, it is recommended that CA flow-down representations and warrant requirements to its suppliers.

9.6.3 Subscriber Representations and Warranties

Before being issued the certificate. the Subscriber shall be required to sign a Subscriber Agreement containing the requirements the Subscriber shall meet respecting protection of the private key and use of the certificate. Specifically, the Subscriber agreement shall obligate the Subscriber to the following:

- Accurately represent themselves in all communications with the PKI authorities;
- The identity and affiliation information in the Subscriber's certificate is accurate;
- The Subscriber is the sole user of the key corresponding to Subscriber's certificate(s) except in key recovery scenarios;
- Protect their private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements and local procedures;
- Promptly notify the appropriate CA upon suspicion of loss or compromise of their private keys. Such notification shall be made directly or indirectly through mechanisms consistent with the issuing CA's CPS;
- Abide by all the terms, conditions, and restrictions levied on the use of their private keys and certificates; and

- Acknowledge that any information contained within a certificate is not considered private.

A PKI Sponsor shall assume the Subscriber obligations for devices.

9.6.4 Relying Parties Representations and Warranties

Any time a Relying Party uses or otherwise relies on a Certificate, it represents and warrants that it shall:

- Use the Certificate for the purpose for which it was issued as defined in the key usage and enhanced key usage certificate extensions;
- Perform status checks as set forth in section 4.9.6, Revocation Checking Requirements for Relying Parties;
- Check each Certificate for validity, using procedures described in the X.509 standard [ISO 9594-8], prior to reliance;
- Establish trust in the CA who issued a Certificate by verifying the Certificate path in accordance with the guidelines set by the X.509 Version 3 Amendment; and
- 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.

Practice Note: Application upgrades may modify data structures in a manner that invalidates a previously captured and stored digital signature.

9.6.5 Representations and Warranties of Affiliated Organizations

Affiliated Organizations shall authorize the affiliation of subscribers with the organization and shall inform the Entity CA of any severance of affiliation with any current subscriber.

9.6.6 Representations and Warranties of other Participants

If key escrow and recovery are supported, Third-party key recovery Requestors shall formally acknowledge and agree to the obligations described here, prior to receiving a recovered key:

- The Third-Party Requestor shall protect Subscribers' recovered key(s) from compromise. The Third-Party Requestor shall use a combination of computer security, cryptographic, network security, physical security, personnel security, and procedural security controls to protect their keys and recovered Subscribers' keys.
- The Third-Party Requestor shall destroy or surrender Subscribers' keys when no longer required (i.e., when the data has been recovered).
- The Third-Party Requestor shall request and use the Subscriber's escrowed key(s) only to recover Subscriber's data they are authorized to access.
- The Third-Party Requestor shall accurately represent themselves to all entities during any key recovery service.
- When the request is made, the Third-Party Requestor shall provide accurate identification and authentication information at least to the same level required for issuing new PKI

certificates at the level of the key being requested (e.g., the Third-Party Requestor sends a digitally signed request using the credential issued by the Entity PKI at the same or higher assurance level as the key being recovered).

- The Third-Party Requestor shall protect information concerning each key recovery operation.
- Upon receipt of the recovered key(s), the Third-Party Requestor shall sign an acknowledgement of agreement to follow the law and the subscriber's organization policies relating to protection and release of the recovered key. Such agreement should include the following attestations:

    - Third Party Requestor has been accurately represented their identity to all key recovery entities,
    - Third Party Requestor has truthfully described the reason(s) for the key recover request,
    - Third Party Requestor has a legitimate and official need to obtain the requested key(s),
    - Third Party Requestor has received the recovered key(s),
    - Third Party Requestor shall use the recovered key only for the stated purpose(s),
    - Third Party Requestor shall protect the recovered key from unauthorized access. When no longer required, the Third-Party Requestor shall either destroy the key(s) and inform the organization of destruction per agency requirements, or return any recovered key(s) stored on hardware to the organization.
    - Third Party Requestor agrees to be bound by applicable laws, and regulations concerning the protection of the recovered key(s) and any data recovered using the key(s).

9.7 DISCLAIMERS OF WARRANTIES

To the extent permitted by applicable law, this CP, and MTFSA, other agreements may contain disclaimers of all warranties.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, TSCP, LLC. DISCLAIMS 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 TSCP, LLC. AND ITS CUSTOMERS UNDER SEPARATE AGREEMENTS: (A) CERTIFICATES ISSUED BY TSCP, LLC ARE PROVIDED "AS IS", AND TSCP, LLC., 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 AND COMPLETENESS 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 TSCP, LLC. CERTIFICATES, ANY SERVICES PROVIDED BY TSCP, LLC,

OR THE VALIDATION OF ANY DIGITAL SIGNATURES LIES WITH THE APPLICABLE PARTICIPANT.

9.8 LIMITATIONS OF LIABILITY

Limitation of Liability between TSCP, LLC and the Entity shall be defined in MTFSA.

OTHERWISE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL TSCP, LLC BE LIABLE FOR ANY INDIRECT DAMAGES OF ANY KIND, INCLUDING CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE, ANY COSTS, EXPENSES, OR LOSS OF PROFITS, OR OTHER DAMAGES WHATSOEVER ARISING OUT OF OR RELATED TO THIS CP, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
IN NO EVENT SHALL TSCP, LLC BE LIABLE FOR ANY USAGE OF CERTIFICATE THAT EXCEEDS THE LIMITATIONS OF USAGE STATED UNDER THIS CP OR THAT IS NOT IN COMPLIANCE WITH THIS CP AND ASSOCIATED CPS.

TSCP, LLC SHALL NOT BE LIABLE FOR ANY DAMAGE ARISING FROM THE COMPROMISE OF A SUBSCRIBER'S PRIVATE KEY OR ANY LOSS OF DATA.

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

9.9 INDEMNITIES

9.9.1 Indemnification by Entity CA

To the extent permitted by applicable law, Entity CAs agree to indemnify and hold TSCP, LLC harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind including reasonable attorney's fees that TSCP, LLC may incur as a result of:

- Falsehood or misrepresentation of fact by the other Entity CA in the applicable contractual agreements;
- Failure by the Entity 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;
- Entity CA's failure to protect their CA Private Key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Entity CA Private Key; or
- Entity CA's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

Any applicable agreement may include additional indemnity obligations.

9.9.2 Indemnification by Relying Party

To the extent permitted by applicable law, and any applicable contractual agreements, Relying Party agrees to indemnify and hold TSCP, LLC. harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind including reasonable attorneys' fees that TSCP, LLC may incur as a result of:

- The Relying Party's failure to perform the obligations of a Relying Party;
- The Relying Party's reliance on a Certificate that is not reasonable under the circumstances;
- The Relying Party's reliance on a "pass-through" certificate policy OID; or
- The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

Any applicable contractual agreement with TSCP, LLC may include additional indemnity obligations.

9.10 TERM & TERMINATION

9.10.1 Term

This CP has no specified term.

9.10.2 Termination

Termination of this CP is at the discretion of the TPMO. This CP survives termination of any MTFSA or other agreement.

9.10.3 Effect of Termination and Survival

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

9.11 INDIVIDUAL NOTICES & COMMUNICATIONS WITH PARTICIPANTS

Unless otherwise specified in an MTFSA, CAs shall use commercially reasonable methods for communications commensurate with the sensitivity of the communication.

For Entity CAs, any planned change to the infrastructure that has the potential to affect the TPMA operational environment shall be communicated to the TPMA at least two weeks and a day prior to implementation, which notice period will begin to run upon written acknowledgement by the TPMA. All new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the change shall be provided to the TPMA within 24 hours following implementation.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

The TPMA shall review this CP at least once every year.

Corrections, updates, or suggested changes to this CP shall be communicated to every Entity CA. Such communications must include a description of the change, a change justification, and contact information for the person requesting the change.

This CP and amendments to it become effective once approved by the TPMA, by the TPMO, and published into the TSCP, LLC PKI Repository.

9.12.2 Notification Mechanism and Period

For the TBCA, proposed changes to this CP shall be distributed electronically to TPMA members and observers in accordance with the TPMA Charter. The CP approved by the TPMA and TPMO shall be published into the TSCP, LLC PKI Repository.

9.12.3 Circumstances under which OID must be changed

The TBCA shall change OIDs if the TPMA determines that a change in the CP reduces the level of assurance provided.

For Entity CA, no stipulation.

9.13 DISPUTE RESOLUTION PROVISIONS

Dispute resolutions provisions shall be defined in MTFSA between TSCP, LLC and the Entity.

Otherwise, any dispute in connection with this CP shall be resolved by binding arbitration in accordance with the rules of the American Arbitration Association in effect at the time of the dispute. The arbitration rules shall be used as follows:

- One or more parties is a non-US Entity: International Rules
- Otherwise: Commercial Rules

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 attorneys' 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 in 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 CP.

9.14 GOVERNING LAW

Subject to any limits appearing in applicable law, the construction, validity, performance, and effect of certificates issued under this CP shall be governed by Delaware law (statute, case law or regulation) irrespective of other choice of law provisions in MTFSA and without a requirement to establish nexus in the state of Delaware. The choice of law provision only applies to the terms directly in this CP and is made to ensure uniform procedures and interpretation regardless of where a party is located. MTFSAs incorporating this CP by reference may have their own governing law provisions.

9.15 COMPLIANCE WITH APPLICABLE LAW

The TBCA and Entity CAs shall comply with all applicable law.

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 any of its obligations under this CP, without prior written consent of the other party. Such consent shall not be unreasonably withheld.

9.16.3 Severability

Should it be determined by a court of competent jurisdiction that a provision or set of provisions in this CP is incorrect or invalid, the other sections of this CP shall remain in effect.

9.16.4 Enforcement (Attorney Fees/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

TSCP, LLC 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.

TSCP, LLC HAS NO LIABILITY FOR ANY DELAYS, NONDELIVERIES, NON-PAYMENTS, MIS-DELIVERIES OR SERVICE INTERRUPTIONS CAUSED BY ANY THIRD-PARTY ACTS OR THE INTERNET INFRASTRUCTURE OR ANY NETWORK EXTERNAL TO TSCP, LLC.

9.17 OTHER PROVISIONS

No stipulation.

10. CERTIFICATE, CRL, AND OCSP PROFILES

10.1 TBCA TO PCA CROSS 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	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Subject Public Key Information	4096 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	Sha384 WithRSAEncryption {1 2 840 113549 1 1 12}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as in PKCS-10 request from the TBCA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the PCA)
Key Usage	c=yes; keyCertSign, cRLSign,
Certificate Policies	c=no; {applicable policies}
Policy Mapping	c=no; {applicable policy mappings}
Basic Constraints	c=yes; cA=True; path length constraint absent
Name Constraints	c=yes; Optional, permitted subtrees for DN, RFC 822, and DNS name forms
Policy Constraint	C=no; *inhibitPolicyMappings*, skip certs = 1
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for p7c file containing Certificates issued to the TBCA, may be followed by LDAP URL pointer to the caCertificate attribute of the TBCA PKI Repository entry; may contain id-ad-ocsp access method entry with HTTP URL for the TBCA OCSP Responder
CRL Distribution Points	c = no; http://crl.one.digicert.com/tscpbcasha384.crl
Inhibit anyPolicy	c=no; skipCerts = 0
Policy Constraint	C=no; *inhibitPolicyMappings*, skip certs = 1

10.2 PCA TO TBCA CROSS CERTIFICATE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as in PKCS-10 request from the PCA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the TBCA)
Key Usage	c=yes; keyCertSign, cRLSign,
Certificate Policies	c=no; {applicable 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 for DN, RFC 822, and DNS name forms
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for p7c file containing Certificates issued to PCA, may be followed by LDAP URL pointer to the caCertificate attribute of the PCA PKI Repository entry; may contain id-ad-ocsp access method entry with HTTP URL for the PCA OCSP Responder
CRL Distribution Points	c = no;
Inhibit anyPolicy	c=no; skipCerts = 0
Policy Constraint	C=no; *inhibitPolicyMappings*, skip certs = 1

10.3 TBCA TO ANOTHER BRIDGE CROSS 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	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Subject Public Key Information	4096 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	Sha384 WithRSAEncryption {1 2 840 113549 1 1 12}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as in PKCS-10 request from the TBCA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from Bridge)
Key Usage	c=yes; keyCertSign, cRLSign,
Certificate Policies	c=no; {applicable 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 for DN, RFC 822, and DNS name forms
Policy Constraints	c=no; *inhibitPolicyMapping* skipCerts = 1
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for p7c file containing Certificates issued to TBCA, may be followed by LDAP URL pointer to the caCertificate attribute of the TBCA PKI Repository entry; may contain id-ad-ocsp access method entry with HTTP URL for the TBCA OCSP Responder
CRL Distribution Points	c = no; http://crl.one.digicert.com/tscpbcasha384.crl
Inhibit anyPolicy	c=no; skipCerts = 0
Policy Constraint	C=no; inhibitPolicyMappings, skip certs = 1

10.4 ANOTHER BRIDGE TO TBCA CROSS CERTIFICATE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as in PKCS-10 request from the Bridge)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the TBCA)
Key Usage	c=yes; keyCertSign, cRLSign
Certificate Policies	c=no; {applicable 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 for DN, RFC 822, and DNS name forms
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for p7c file containing Certificates issued to Bridge, may be followed by LDAP URL pointer to the caCertificate attribute of the Bridge PKI Repository entry; may contain id-ad-ocsp access method entry with HTTP URL for the Bridge OCSP Responder
CRL Distribution Points	c = no;
Inhibit anyPolicy	c=no; skipCerts = 0
Policy Constraint	C=no; *inhibitPolicyMappings*, skip certs = 1

10.5 SELF-SIGNED ROOT CERTIFICATE / TRUST ANCHOR

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	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Subject Public Key Information	4096 bit RSA key modulus or greater, rsaEncryption {1 2 840 113549 1 1 1} Practice Note: 4096 bit lengths are increasingly prevalent for offl CAs within the community and Relying Parties may need to inter with such key lengths.
Issuer's Signature	Sha384 WithRSAEncryption {1 2 840 113549 1 1 12}
Extension	**Value**
Subject Key Identifier	c=no; Octet String (same as in applicable PKCS-10 request)
Key Usage	c=yes; keyCertSign, cRLSign, DigitalSignature, nonRepudiation
Basic Constraints	c=yes; cA=True; path length constraint absent

Practice Note: Additional extensions may be required by relying parties. For example, certain Gatelink implementations require the CRL-DP extension to be asserted.

10.6 POLICY CA OR ISSUING CA CERTIFICATE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus or greater, rsaEncryption {1 2 840 113549 1 1 1} Practice Note: 4096 bit lengths are increasingly prevalent for offl CAs within the community and Relying Parties may need to inter with such key lengths.
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in superior CA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the subordinate CA)
Key Usage	c=yes; keyCertSign, cRLSign, DigitalSignature, nonRepudiation
Certificate Policies	c=no; {applicable policies}
Basic Constraints	c=yes; cA=True; path length constraint absent or as desired by superior CA
Name Constraints	c=yes; optional, permitted subtrees for DN, RFC 822, and DNS name forms
Policy Constraints	optional; c= no;
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for p7c file containing Certificates issued to superior CA, may be followed by LDAP URL pointer to the caCertificate attribute of the superior CA PKI Repository entry; may contain id-ad-ocsp access method entry with HTTP URL for the superior CA OCSP Responder
CRL Distribution Points	c = no;

10.7 HUMAN 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}
Issuer Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in issuing CA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request, or calculated by the Issuing CA according to RFC 5280 method 1, or other method
Key Usage	c=yes; DigitalSignature
Extended Key Usage	c=no; per Section 10.22
Certificate Policies	c=no; {applicable policies}
Subject Alternative Name	c=no; (Optional unless asserting id-PIVI assurance level) URI urn:uuid:<128 bit GUID> (Optional) others
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for p7c file containing Certificates issued to issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the issuing CA PKI Repository entry; may contain id-ad-ocsp access method entry with HTTP URL for the issuing CA OCSP Responder unless asserting id-PIVI assurance level, in which case mandatory
CRL Distribution Points	c = no;

10.8 HUMAN 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}
Issuer Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 & Generalized Time thereafter
Subject Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Required Extensions	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in issuing CA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request, or calculated by Issuing CA according to RFC 5280 method 1, or other method
Key Usage	c=yes; DigitalSignature, nonRepudiation
Extended Key Usage	c=no; per Section 10.22
Certificate Policies	c=no; {applicable policies}
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for p7c file containing Certificates issued to issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the issuing CA PKI Repository entry; may contain id-ad-ocsp access method entry with HTTP URL for the issuing CA OCSP Responder unless asserting id-PIVI assurance level, in which case mandatory
CRL Distribution Points	c = no;
Optional Extensions	**Value**
Subject Alternative Name	c=no; Any name types may be present. *** If application (s) using certificates from this certificate profile use this extension, then this extension is required with the values specified below: (Mandatory) RFC822 email address (Optional) URI urn:uuid:<128 bit GUID> (Optional) others

Practice Note: Some applications expect an email address in the Subject Alternative Name field. Not having an email address in the field may cause problems as a result.

10.9 HUMAN 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}
Issuer Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in issuing CA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request, or calculated by the Issuing CA according to RFC 5280 method 1, or other method
Key Usage	c=yes; (Mandatory) keyEncipherment (Optional) dataEncipherment
Extended Key Usage	c=no; per Section 10.22
Certificate Policies	c=no; {applicable policies}
Subject Alternative Name	c=no; (Mandatory) RFC822 email address (Optional) URI urn:uuid:<128 bit GUID> (Optional) others
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for p7c file containing Certificates issued to issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the issuing CA PKI Repository entry; may contain id-ad-ocsp access method entry with HTTP URL for the issuing CA OCSP Responder unless asserting id-PIVI assurance level, in which case mandatory
CRL Distribution Points	c = no;

10.10ID-PIVI-CARDAUTH CERTIFICATE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	sn=<GUID> with applicable DN prefix
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in issuing CA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request, or calculated by the Issuing CA according to RFC 5280 method 1, or other method)
Key Usage	c=yes; (Mandatory) digitalSignature
Extended Key Usage	c=yes; per Section 10.22
Certificate Policies	c=no; {applicable policies}
Subject Alternative Name	c=no; (Mandatory) URI urn:uuid:<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, may be followed by LDAP URL pointer to the caCertificate attribute of the issuing CA PKI Repository entry; shall contain id-ad-ocsp access method entry with HTTP URL for the issuing CA OCSP Responder
CRL Distribution Points	c = no;

10.11 ID-PIVI-CONTENTSIGNER CERTIFICATE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in issuing CA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request, or calculated by the Issuing CA according to RFC 5280 method 1, or other method)
Key Usage	c=yes; (Mandatory) digitalSignature
Extended Key Usage	c=no; per Section 10.22
Certificate Policies	c=no; {applicable policies}
Subject Alternative Name	optional; 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, may be followed by LDAP URL pointer to the caCertificate attribute of the issuing CA PKI Repository entry; shall contain id-ad-ocsp access method entry with HTTP URL for the issuing CA OCSP Responder
CRL Distribution Points	c = no;

10.12 CODE SIGNER CERTIFICATE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in issuing CA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request, or calculated by the Issuing CA according to RFC 5280 method 1, or other method)
Key Usage	c=yes; (Mandatory) digitalSignature (Optional) nonRepudiation
Extended Key Usage	c=no; per Section 10.22
Certificate Policies	c=no; {applicable policies}
Subject Alternative Name	c=no; DN of the person controlling the code signer private key
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for p7c file containing Certificates issued to issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the issuing CA PKI Repository entry; may contain id-ad-ocsp access method entry with HTTP URL for the issuing CA OCSP Responder
CRL Distribution Points	c = no;

10.13 DEVICE SUBSCRIBER CERTIFICATE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 subject DN conforming to section 7.1.4 of this CP cn={ Host URL | Host IP Address | Host Name }
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in issuing CA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request, or calculated by the Issuing CA according to RFC 5280 method 1, or other method)
Key Usage	c=yes; (Mandatory) digitalSignature (Optional) keyEncipherment
Extended Key Usage	c=no; per Section 10.22
Certificate Policies	c=no; {applicable policies}
Subject Alternative Name	c=no; (Mandatory) Host URL | IP Address | Host Name
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for p7c file containing Certificates issued to issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the issuing CA PKI Repository entry; may contain id-ad-ocsp access method entry with HTTP URL for the issuing CA OCSP Responder
CRL Distribution Points	c = no;

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}
Issuer Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 CA DN of role conforming to section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in issuing CA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request, or calculated by the Issuing CA according to RFC 5280 method 1, or other method)
Key Usage	c=yes; DigitalSignature
Extended Key Usage	c=no; per Section 10.22
Certificate Policies	c=no; {applicable policies}
Subject Alternative Name	c=no; (Mandatory) DN of the person controlling the role signing private key (Optional) RFC822 email address (Optional) others
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for p7c file containing Certificates issued to issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the issuing CA PKI Repository entry; may contain id-ad-ocsp access method entry with HTTP URL for the issuing CA OCSP Responder
CRL Distribution Points	c = no;

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}
Issuer Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 CA DN for role conforming to section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in issuing CA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request, or calculated by the Issuing CA according to RFC 5280 method 1, or other method)
Key Usage	c=yes; (Mandatory) keyEncipherment
Extended Key Usage	c=no; per Section 10.22
Certificate Policies	c=no; {applicable policies}
Subject Alternative Name	c=no; (Mandatory) RFC822 email address (Optional) others
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for p7c file containing Certificates issued to issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the issuing CA PKI Repository entry; may contain id-ad-ocsp access method entry with HTTP URL for the issuing CA OCSP Responder
CRL Distribution Points	c = no;

10.16 OCSP RESPONDER CERTIFICATE

The following table contains the OCSP Responder Certificate profile assuming that the same CA using the same key as the Subscriber Certificate issues the OCSP Responder Certificate.

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 subject DN conforming to section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in issuing CA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request, or calculated by the Issuing CA according to RFC 5280 method 1, or other method)
Key Usage	c=yes; (Mandatory) digitalSignature, nonRepudiation
Extended Key Usage	c=no; per Section 10.22
Certificate Policies	c=no; {applicable policies}
Subject Alternative Name	c=no; HTTP URL for the OCSP Responder
No Check id-pkix-ocsp-nocheck {1 3 6 1 5 5 7 48 1 5}	c=no; Null

10.17 PKCS 10 REQUEST FORMAT

Field	Value
Version	V1 (0)
Subject Distinguished Name	Unique X.500 subject DN conforming to section 7.1.4 of this CP
Subject Public Key Information	4096 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Subject's Signature	Sha384 WithRSAEncryption {1 2 840 113549 1 1 12}
Extension	**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 or excluded subtrees as appropriate for DN, RFC 822, and DNS name forms

10.18 FULL CRL PROFILE

Field	Value
Version	V2 (1)
Issuer Signature Algorithm	Sha384 WithRSAEncryption {1 2 840 113549 1 1 12}
Issuer Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
thisUpdate	Expressed in UTC Time for dates until end of 2049 and Generalized Time thereafter
nextUpdate	Expressed in UTC Time for dates until end of 2049 and Generalized Time thereafter
Revoked certificates list	0 or more 2-tuple of certificate serial number and revocation date Expressed in UTC Time for dates until end of 2049 and Generalized Time thereafter
Issuer's Signature	Sha384 WithRSAEncryption {1 2 840 113549 1 1 12}
CRL Extension	**Value**
CRL Number	c=no; monotonically increasing integer
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 unless circumstances were for reasons of key compromise or CA compromise
Hold Instruction	c=no; optional. id-holdinstruction-reject may be present only if reason code is certificateHold

10.19 DISTRIBUTION POINT CRL PROFILE

Field	Value
Version	V2 (1)
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
thisUpdate	Expressed in UTC Time for dates until end of 2049 and Generalized Time thereafter
nextUpdate	Expressed in UTC Time for dates until end of 2049 and Generalized Time thereafter
Revoked certificates list	0 or more 2-tuple of certificate serial number and revocation date Expressed in UTC Time for dates until end of 2049 and Generalized Time thereafter
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
CRL Extension	**Value**
CRL Number	c=no; monotonically increasing integer
Authority Key Identifier	c=no; Octet String (same as in Authority Key Identifier field in certificates issued by the CA) (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 (not relative name). The following fields shall all be absent: onlySomeReasons, indirectCRL, onlyContainsAttributeCerts
CRL Entry Extension	**Value**
Reason Code	c=no; optional unless circumstances were for reasons of key compromise or CA compromise
Hold Instruction	c=no; optional. id-holdinstruction-reject may be present only if reason code is certificateHold

10.20 OCSP REQUEST PROFILE

Field	Value
Version	V1 (0)
Requester Name	(Mandatory) DN of the requestor
Request List	List of certificates in accordance with RFC 6960
Request Extension	**Value**
None	None
Request Entry Extension	**Value**
None	None

10.21 OCSP RESPONSE PROFILE

Field	Value
Version	V1 (0)
Response Status	As specified in RFC 6960
Response Type	Id-pkix-ocsp-basic {1 3 6 1 5 5 7 48 1 1}
Responder ID	Octet String (same as subject key identifier in Responder Certificate)
Produced At	Generalized Time
List of Responses	Each response will contain certificate id, certificate status, thisUpdate, nextUpdate. The OCSP responder shall use thisUpdate and nextUpdate from the CA CRL. If the certificate is revoked, the OCSP responder shall provide the revocation time and reason corresponding to that asserted in the CA CRL entry extension.
Request List	List of certificates in accordance with RFC 6960
Request Extension	**Value**
Nonce	c=no; Same value as asserted in the request if it was present in the request
Response Entry Extension	**Value**
None	None

10.22 EXTENDED KEY USAGE

Certificate Type	Required EKU	Optional EKU	Prohibited EKU
CA	None	None	All
OCSP Responder	id-kp-OCSPSigning {1 3 6 1 5 5 7 3 9}	None	All Others
Human Subscriber Identity	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} (Last two only if using a hardware assurance level)	None	All Others
Human Subscriber & Role Signature	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}	None	All Others
Human Subscriber & Role Encryption	id-kp-emailProtection {1.3.6.1.5.5.7.3.4}	Any EKU that is consistent with the application for which it will be used	All Others
Code Signing	id-kp-codesigning {1 3 6 1 5 5 7 3 3}	Life-time Signing {1.3.6.1.4.1.311.10.3.13}	All Others
Device Authentication, 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
Device Signature	None	Any EKU that is consistent with the application for which it will be used	All Others
Device Encryption	None	None	All
id-PIVI-cardAuth	id-PIV-cardAuth {2.16.840.1.101.3.6.8}	None	All Others
id-PIVI-ContentSigning	id-fpki-pivi-content-signing {2.16.840.1.101.3.8.7}	None	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
Time Stamp Authority	id-kp-timestamping {1 3 6 1 5 5 7 3 8}	None	All Others
Web Client	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
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
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

11. PKI REPOSITORY PROFILES

This section defines the interoperability profile for a PKI Repository as defined in Section 2.

11.1 PROTOCOL

A PKI Repository shall implement the HTTP protocol for accessing Certificates and CRL. Implementing the LDAPv3 protocol is optional.

11.2 AUTHENTICATION

No authentication shall be used to read Certificate and CRL. For X.500 Directory Server System, a 'none' authentication shall be sufficient.

11.3 NAMING

For X.500 Directory Server System:

- CA Certificates shall be stored in the entry that appears in the Certificate subject name.
- The issuedByThisCA element of crossCertificatePair shall contain the Certificate(s) issued by a CA whose name the entry represents.
- CRLs shall be stored in the Directory in the entry that appears in the CRL issuer name.

11.4 OBJECT CLASS

For X.500 Directory Server System:

- Entries that describe CAs shall be defined by organizationUnit or organizationalRole structural object class. These entries shall also be a member of pkiCA cpCPS auxiliary object classes.
- 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

For X.500 Directory Server System:

- CA entries shall be populated with the caCertificate, crossCertificatePair, certificateRevocationList, cpCPS attributes, as applicable.
- User entries may be populated with userCertificate attribute containing encryption certificate. Signature certificate need not be published to the PKI Repository.

12. SMARTCARD PROFILES

12.1 PIV-I SMARTCARD PROFILE

The id-PIVI assurance levels enable issuers to issue cards that are interoperable from both a policy and technology perspective with Federal PIV Card. This smartcard profile defines the specific requirements of a PIV-I Smart Card. It relies heavily on relevant specifications from the National Institute of Standards and Technology (NIST).

The following requirements shall apply to PIV-I Smart Cards:

1. To ensure interoperability with Federal systems, PIV-I Cards shall use a smart card platform that is on GSA's FIPS 201 Evaluation Program Approved Product List (APL) and uses the PIV application identifier (AID). Card stock that has been removed from the APL may continue to be issued for no more than one year after GSA approved replacement card stock is available. PIV-I cards issued using the deprecated card stock may continue to be used until the current subscriber certificates expire, unless otherwise notified by the TPMA, FPKIPA, or FPKIMA.
2. PIV-I Cards shall conform to [NIST SP 800-73-3[4]].
3. The mandatory X.509 Certificate for Authentication shall be issued under a policy that is cross certified with the TBCA id-PIVI policy OID.
4. The X.509 Certificate for Signature, when used, shall be issued under a policy that is cross certified with the TBCA id-PIVI policy OID.
5. The X.509 Certificate for Key Management, when used, shall be issued under a policy that is cross certified with the TBCA id-PIVI or id-MediumHardware policy OID.
6. The mandatory X.509 Certificate for Card Authentication shall be issued under a policy that is cross certified with the TBCA id-PIVI-cardAuth policy OID.
7. The digital signature certificate that is used to sign objects on the PIV-I Card (e.g., CHUID, Security Object) shall contain a policy OID that has been mapped to the TBCA id-PIVI-contentSigner policy OID.
8. The Authentication, Signature, Key Management, Card Authentication, and Content Signer Certificates shall conform to the applicable profiles in Section 10.
9. PIV-I Cards shall contain an electronic representation (as specified in SP 800-73 and SP 800-76) of the Cardholder Facial Image printed on the card.
10. PIV-I Cards shall contain an electronic representation (as specified in SP 800-73 and SP 800-76 of the Cardholder's fingerprints collected at the time of issuance.
11. Visual distinction of a PIV-I Card from that of a Federal PIV Card is required to ensure no suggestion of attempting to create a fraudulent Federal PIV Card. At a minimum, images or logos on a PIV-I Card shall not be placed entirely within Zone 11, *Agency Seal*, as defined by [FIPS 201].

[4] Special attention should be paid to UUID requirements for PIV-I.

12. The PIV-I 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 exists; otherwise the issuer of the card; and
    d. Card expiration date.
13. PIV-I Cards shall have an expiration date not to exceed 6 years of issuance.
14. Expiration of the PIV-I Card should not be later than expiration of the id-PIVI-contentSigner certificate on the card.
15. The PIV-I Content Signing certificate and corresponding private key shall be managed within a trusted Card Management System as defined throughout this CP.
16. At issuance, the RA shall activate and release the PIV-I Card to the subscriber only after a successful 1:1 biometric match of the applicant against the biometrics collected in Section 3.2.3.
17. PIV-I Cards may support card activation by the card management system to support card personalization and post-issuance card update. To activate the card for personalization or update, the card management system 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 set to be specific to each PIV-I Card. That is, each PIV-I Card shall contain a unique card management key. Card management keys shall meet the algorithm and key size requirements stated in Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification. [SP800-78]
18. On an annual basis, for each PCI configuration used (as defined by the FIPS 201 Evaluation Program), one populated, representative sample PIV-I Card shall be submitted to the FIPS 201 Evaluation Program for testing.

13. BIBLIOGRAPHY

The following documents were used in part to develop this CP:

ABADSG	Digital Signature Guidelines, 1996-08-01. http://www.abanet.org/scitech/ec/isc/dsgfree.html
AUDIT	FPKI Compliance Audit Requirements http://www.idmanagement.gov/documents/fpki-compliance-audit-requirements
CIMC	Certificate Issuing and Management Components Family of Protection Profiles, version 1.0, October 31, 2001.
FBCA-PROF	Federal Bridge Certification Authority (FBCA) X.509 Certificate and CRL Extensions Profile https://www.idmanagement.gov/docs/fpki-x509-cert-profiles-fbca.pdf
FIPS 140-2	Security Requirements for Cryptographic Modules May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
FIPS 186-5	Digital Signature Standard (DSS), FIPS 186-5, February 3,2023. https://csrc.nist.gov/publications/detail/fips/186/5/final
FIPS 201	Personal Identity Verification (PIV) of Federal Employees and Contractors http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf and http://csrc.nist.gov/publications/drafts/fips201-2/Draft_NIST-FIPS-201-2.pdf
FOIA	5 U.S.C. 552, Freedom of Information Act. http://www.law.cornell.edu/uscode/5/552.html
FPKI-E	Federal PKI Version 1 Technical Specifications: Part E-X.509 Certificate and CRL Extensions Profile, 7 July 1997
ISO9594-8	Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 1997.
ITMRA	40 U.S.C. 1452, Information Technology Management Reform Act of 1996 http://www.law.cornell.edu/uscode/40/1452.html
NAG69C	Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999.
NIST SP 800-63-3	Digital Identity Guidelines https://csrc.nist.gov/publications/detail/sp/800-63/3/final
NIST SP 800-73	Interfaces for Personal Identity Verification (4 Parts) http://csrc.nist.gov/publications/PubsSPs.html

NIST SP 800-76	Biometric Data Specification for Personal Identity Verification http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf
NIST SP 800-78	Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV) http://csrc.nist.gov/publications/nistpubs/800-78-2/sp800-78-2.pdf
NSD42	National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990. http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt (redacted version)
NS4005	NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997.
NS4009	NSTISSI 4009, National Information Systems Security Glossary, January 1999.
PIV-I Profile	X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards, Date: April 23 2010, Reference Link: http://www.idmanagement.gov/documents/piv-i-x509-certificate-and-certificate-revocation-list-crl-extensions-profile
PKCS#12	Personal Information Exchange Syntax Standard, April 1997. ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf
RFC 2510	Certificate Management Protocol, Adams and Farrell, March 1999.
RFC 3647	Certificate Policy and Certification Practices Framework, Chokhani and Ford, Sabett, Merrill, and Wu, November 2003.

14. ACRONYMS AND ABBREVIATIONS

AID	Application Identifier
CA	Certification Authority
CARL	Certificate Authority Revocation List
CMS	Card Management System
COMSEC	Communications Security
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Object Registry
CSS	Certificate Status Server
DDS	Data Decryption Server
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ERC	Enhanced Reliability Check
FAR	Federal Acquisition Regulations
FBCA	Federal Bridge Certification Authority
FPKIMA	Federal Public Key Infrastructure Management Authority
FED-STD	Federal Standard
FIPS PUB	(US) Federal Information Processing Standard Publication
FPKI	Federal Public Key Infrastructure
FPKI-E	Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile
FPKISC	Federal PKI Steering Committee

FPKIPA	Federal PKI Policy Authority
GPEA	Government Paperwork Elimination Act of 1998
GSA	General Services Administration
HTTP	HyperText Transfer Protocol
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector
ITU-TSS	International Telecommunications Union – Telecommunications System Sector
KED	Key Escrow Database
KRA	Key Recovery Agent
KRO	Key Recovery Official
KRP	Key Recovery Policy
KRPS	Key Recovery Practice Statement
KRS	Key Recovery System
LDAP	Lightweight Directory Access Protocol
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OCSP	Online Certificate Status Protocol

OID	Object Identifier
MTFSA	Master Trust Framework Service Agreement
PCA	Principal CA
PI	Personal Information
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV-I	Personal Identity Verification – Interoperable
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SCA	Subordinate CA
SHA-2	Secure Hash Algorithm, Version 2
S/MIME	Secure Multipurpose Internet Mail Extension
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TSDM	Trusted Software Development Methodology
UPN	User Principal Name
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
U.S.C.	United States Code
UUID	Universally Unique Identifier (defined by RFC 4122)

VME	Virtual Machine Environment

15. GLOSSARY

Access	Ability to make use of any information system (IS) resource. [NS4009]
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Affiliated Organization	Organizations that authorize affiliation with Subscribers of PIV-I certificates.
Applicant	The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]
Archive	Long-term, physically separate storage.
Attribute Authority	An entity, recognized by the FPKIPA or comparable Entity body as having the authority to verify the association of attributes to an identity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]

Backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
Binding	Process of associating two related elements of information. [NS4009]
Biometric	A physical or behavioral characteristic of a human being.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]. As used in this CP, the term "Certificate" refers to 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 CARLs or CRLs.
Certification Authority Revocation List (CARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates that have been revoked.
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 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]
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.
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. Same as CSS (Certificate Status Server)
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. [NS4009]
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by the National Institute of Standards and Technology.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
Cross-Certificate	A certificate used to establish a trust relationship between two Certification Authorities.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]

Cryptoperiod	Time span during which each key setting remains in effect. [NS4009]
Data Decryption Server (DDS)	An automated system that obtains subscriber private keys from the Key Escrow Database or other Data Decryption Server to support decryption of data entering and leaving the Enterprise. An example of data would be an 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.
Encrypted Network	A network that is protected from outside access by NSA approved high-grade (Type I) cryptography. Examples are SIPRNET and TOP SECRET networks.
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.
Entity	For the purposes of this document, "Entity" refers to an organization, corporation, community of interest, or government agency with operational control of a CA.
Entity CA	A CA that acts on behalf of an Entity and is under the operational control of an Entity. The Entity may be an organization, corporation, or community of interest. For the Federal Government, an Entity may be any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Federal Government.

FBCA Management Authority (FPKIMA)	The Federal Public Key Infrastructure Management Authority is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the Federal Bridge Certification Authority.
Federal Public Key Infrastructure Policy Authority (FPKIPA)	The FPKIPA is a federal government body responsible for setting, implementing, and administering policy decisions regarding inter Entity PKI interoperability that uses the FBCA.
Firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
High Assurance Guard (HAG)	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.
Hypervisor	Computer software, firmware or hardware that creates and runs virtual machines. A hypervisor uses native execution to share and manage hardware, allowing for multiple environments which are isolated from one another, yet exist on the same physical machine. Also known as an isolation kernel or a virtual machine monitor.
Information System Security Officer (ISSO)	Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, from design through disposal. [NS4009]
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. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intermediate CA	A CA that is subordinate to another CA and has a CA subordinate to itself.
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the

	subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]
Key Escrow Database	The function, system, and subsystems that maintain the key escrow repository and respond to key escrow and key recovery requests from one or more Key Recovery Agents, as specified by this policy.
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 (KRA)	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, as specified by this policy.
Key Recovery Official (KRO)	An individual authorized to authenticate and submit key recovery requests to the Key Recovery Agent on behalf of a requestor, as specified in this policy.
Key Recovery Policy (KRP)	A key recovery policy is a specialized form of administrative policy that ensures the protection and recovery of key management private keys (i.e., decryption keys) held in escrow. A key recovery policy addresses all aspects associated with the storage and recovery of key management certificates. A Key Recovery Policy can stand on its own or be incorporated into a Certificate Policy (CP).
Key Recovery Practice Statement (KRPS)	A statement of the practices that a key recovery system employs in protecting and recovering key management private keys, in accordance with the specific requirements specified in the relevant KRP. A Key Recovery Practice Statement can stand on its own or be incorporated into a Certificate Practice Statement (CPS).
Key Recovery System	The KRS provides the computer system hardware, software, staff, and procedures to escrow private keys securely and recover them when appropriate.

Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community.
Memorandum of Understanding (MOU)	Agreement between the FPKIPA and an Entity allowing interoperability between the Entity Principal CA and the FBCA.
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).
Naming Authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
National Security System	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. 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. In the federal government PKI they are used to uniquely identify each of the seven policies and cryptographic algorithms supported.
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.
Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.
PKI Sponsor	An individual who represents a device or group in all certificate life-cycle activities. A PKI Sponsor asserts that the certificate and associated private key are being used in accordance with the subscriber and certificate specific obligations in this CP.
Policy Management Authority (PMA)	The individual or group that is responsible for the creation and maintenance of Certificate Policies and Certification Practice Statements, and for ensuring that all Entity PKI components (e.g., CAs, CSSs, CMSs, and RAs) are audited and operated in compliance with the entity PKI CP. The PMA evaluates non-domain policies for acceptance within the domain, and generally oversees and manages the PKI certificate policies. For the FBCA, the PMA is the FPKIPA.
Principal CA	The Principal CA is a CA designated by an Entity to interoperate with the FBCA. An Entity may designate multiple Principal CAs to interoperate with the FBCA.
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)	A person or 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.
Remote Workstation	A "remote workstation" is a dedicated system used to access the system hosting the CA or the CA itself, CMS, CSS, KRS, and associated equipment through external networks for maintenance and administration. A remote workstation is not connected via a dedicated network and as such must be protected as a logical extension of the CA, CMS, CSS, and KRS as specified in Sections 5 and 6 of this CP. Remote workstations do not include consoles within the CA's security perimeter or RA workstations.
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.
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.
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 a device, which is utilized by the applicant/Subscriber in order to ensure the remote identity proofing process employs physical, technical, and procedural measures to 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 NIST SP 800-63A Section 5.3.3; 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.
System High	The highest security level supported by an information system. [NS4009]
System Software Layer	A layer of software that manages lower layer hardware and software resources and provides services through well-defined interfaces to the higher layers of software. Examples of system software layers are virtual machines, hypervisors, operating systems, and any containerized architectures.

Technical non-repudiation	The contribution of public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
Trust List	Collection of trusted certificates used by Relying Parties to authenticate other certificates.
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. [NS4009]
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.
Virtual Machine Environment	An emulation of a computer system (in this case, a CA) that provides the functionality of a physical machine and a platform-independent environment. It consists of a host (virtual machine) and isolation kernel (hypervisor) and provides functionality needed to execute entire operating systems. At this time, allowed VMEs are limited to Hypervisor type virtual environments. Other technology, such as Docker Containers, is not permitted.

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. [FIPS1401]

16. ACKNOWLEDGEMENTS

The TSCP developed this CP based on RFC 3647 and the original FBCA Certificate Policy.

