XTec Public Key Infrastructure X.509 Certificate Policy

Version 2.2

April 20, 2025

PAGE INTENTIONALLY LEFT BLANK

Signature Page

Kevin A Kozlowski

Digitally signed by Kevin A Kozlowski
Date: 2025.04.29 13:29:37 -04'00'

4/29/2025

XTec PKI Policy Authority

DATE

Revision History

Document Version	Document Date	Revision Details
1.0	March 31, 2015	Initial draft.
1.1	September 30, 2018	Updates to reflect changes to policies to add derived (see 1.2)
1.2	January 25, 2019	Updates to align CP and CPS OIDs with new derived OIDs
1.3	April 09, 2019	Updates to clarify: Added 1.1.3 to clarify relationships with other Entity PKIs Clarified Naming item in Section 3.1
1.4	March 4, 2020	Updates: Clarified Naming item in Section 3.1. Added additional name spaces that can be used under this CP.
1.5	December 16, 2021	Updates: Added new OIDs and identification requirements for PIV-C and PIV-C PWI Added new OIDs for AATL and XTec Operational certificates Cleaned up PIV-I policies Added RRSP requirements throughout Updated Section 5 on logging requirements and audit and log storage
1.5.1	March 1, 2022	Minor Updates to clarify verbiage around the following: - use of OIDs at Root; - CA/RA Termination; - PA responsibilities; - Background checks; - Sanctions for unauthorized actions; - Test Environment; - Training
2.0	January 8, 2024	Updates to fully align with FPKI Common CP and to create a single overarching policy for all XTec CAs not covered by FPKI Common directly.
2.1	October 25, 2024	Updates to align to FBCA CP
2.2	April 20, 2025	Updated to Align with changes to FBCA CP Version 3.6 Updates to Trusted Agent Definition and Key Recovery

Table of Contents

1. INTRODUCTION

XTec, Inc. (XTec) has implemented a comprehensive Public Key Infrastructure (PKI) to provide the services necessary to support entities that fall outside of the scope of the Federal PKI Shared Service Providers (FPKI SSP) as well as those that fall within the scope of the FPKI SSP. While those entities that fall within the scope of the FPKI SSP are governed by the *X.509 Certificate Policy for the U.S. Federal Common Policy Framework*, the XTec Public Key Infrastructure (XTec PKI) will be governed by this policy for all Certification Authorities (CAs) that operate underneath it. For those CAs that operate within the XTec PKI that assert Federal policy identifiers, they will be governed by the *X.509 Certificate Policy for the U.S. Federal Common Policy Framework* and operated under a Certificate Practices Statement that is approved both under that policy and under this policy and its governing authority.

The XTec PKI is designed to deliver shared service provider (SSP) PKI services to Federal and non-Federal organizations (e.g., State Government, Local Government, Educational institutions, Commercial Entity employees and contractors, as well as other organizations that may require such services).

This certificate policy (CP) includes twenty seven (27) policies including: policies for users with software cryptographic modules, policies for users with hardware cryptographic modules, policies for devices, policies for content signing for PIV Interoperable (PIV-I) and PIV Commercial (PIV-C), basic assurance policies, medium assurance policies, user authentication policies, and card authentication policies. Where a specific policy is not stated, the policies and procedures in this specification apply equally to all policies. Any use of the term “assurance” in this Certificate Policy shall not be construed to be a representation or warranty. Any representations, warranties, or liability for damages shall be specifically documented in separate written agreements and shall be appropriately titled as such.

The user policies apply to certificates issued to Federal and state government, local government, and commercial employees, contractors, and other affiliated personnel for the purposes of authentication, signature, and confidentiality. This CP was explicitly designed to support access to systems that have not been designated national security systems.

A PKI that uses this CP will provide the following security management services:

- Key generation/storage
- Certificate generation, modification, re-key, and distribution
- Certificate revocation list (CRL) generation and distribution
- Directory management of certificate related items
- Certificate token initialization/programming/management
- System management functions (e.g., security audit, configuration management, archive.)

Some of the policies require Non-Federal employees, contractors, and other affiliated personnel to use FIPS 140 validated cryptographic modules for cryptographic operations and the protection of trusted keys. The device policy also requires use of FIPS 140 validated cryptographic modules for cryptographic operations and the protection of trusted keys.

This policy does not presume any particular PKI architecture. The policy may be implemented through a hierarchical PKI or mesh PKI. Any CA that asserts this policy in certificates must obtain prior approval from the XTec PKI Policy Authority (XTecPA). CAs that issue certificates

under this policy may operate simultaneously under other policies. Such CAs must not assert the OIDs in this policy in certificates unless they are issued in accordance with all the requirements of this policy.

This policy establishes requirements for the secure distribution of self-signed certificates for use as trust anchors. These constraints apply only to CAs that chose to distribute self-signed certificates, such as a hierarchical PKI's root CA.

One of the goals of the XTec PKI is to facilitate interoperation between the PKI and other external PKI domains. In particular, this CP has been constructed to facilitate policy mapping with the Federal PKI Bridge CA (FBCA) CP.

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

1.1. Overview

1.1.1. Certificate Policy (CP)

Certificates issued under this policy contain a registered certificate policy object identifier (OID), which may be used by a relying party to decide whether a certificate is trusted for a particular purpose.

1.1.2. Relationship between the CP and the CPS

This 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. Each CA that issues certificates under this CP shall have a corresponding CPS. It is permissible to combine two CPS documents into one document if the CAs are related (e.g., a Root CA and its subordinate CA).

This CP also provides for the XTecPA to provide approval of the CPS for XTec managed CAs that operate under the *X.509 Certificate Policy for the U.S. Federal Common Policy Framework*. Additional approval from the Federal PKI Policy Authority will also be required for such CPS.

1.1.3. Relationship Between the CP and other Entity CPs

The XTec Policy Authority may enter into relationships with other Entity PKIs. Each of these relationships will be documented in a Memorandum of Agreement (MoA) which will contain agreements for interoperation including the specific agreements for how levels of assurance asserted by each entity's CP are to be mapped.

The relationship between these CPs and this CP is asserted in CA certificates issued by a XTec PKI CA in the policyMappings extension.

All existing relationships are detailed in Memorandum of Agreements attached in Appendix B.

1.1.4. Scope

This CP applies to certificates issued to CAs, devices, Federal and Non-Federal employees, contractors and other affiliated personnel.

1.1.5. Interoperation with CAs Issuing under Different Policies

Interoperation with CAs that issue under different policies will be achieved through policy mapping and cross-certification based on an agreed to Memorandum of Agreement.

Note that interoperability may also be achieved through other means, such as trust lists, to meet local requirements.

1.2. Document Name and Identification

This CP provides substantial assurance concerning identity of certificate subjects. Certificates issued in accordance with this CP shall assert at least one of the following OIDs, identified in Table 1, in the certificate policy extension:

Table 1: Certificate Policy Identifiers

Policy Type	Policy Name	Policy OID
Basic	id-XTec-nfissp-basic-policy	::= {1.3.6.1.4.1.13862.821.2.1}
	id-XTec-PIVC-basic	::= {1.3.6.1.4.1.13862.821.19.1}
Medium Software	id-XTec-nfissp-medium	::= {1.3.6.1.4.1.13862.821.2.2}
	id-XTec-nfissp-mediumDevice	::= {1.3.6.1.4.1.13862.821.2.3}
	Id-XTec-ops-mediumDevice	::= {1.3.6.1.4.1.13862.821.1.3}
	id-XTec-nfissp-medium-derived	::= {1.3.6.1.4.1.13862.821.2.17}
	id-XTec-PIVC-medium	::= {1.3.6.1.4.1.13862.821.19.2}
	id-XTec-PIVC-mediumDevice	::= {1.3.6.1.4.1.13862.821.19.3}
	id-XTec-PIVC-medium-derived	::= {1.3.6.1.4.1.13862.821.19.7}
Medium Hardware	id-XTec-nfissp-mediumHardware	::= {1.3.6.1.4.1.13862.821.2.4}
	id-XTec-nfissp-medium-authentication	::= {1.3.6.1.4.1.13862.821.2.5}
	id-XTec-nfissp-medium-cardAuth	::= {1.3.6.1.4.1.13862.821.2.6}
	id-XTec-nfissp-mediumDeviceHardware	::= {1.3.6.1.4.1.13862.821.2.8}
	id-XTec-nfissp-medium-derivedHW	::= {1.3.6.1.4.1.13862.821.2.18}
	id-XTec-PIVC-mediumHardware	::= {1.3.6.1.4.1.13862.821.19.4}
	id-XTec-PIVC-mediumAuthentication	::= {1.3.6.1.4.1.13862.821.19.5}
	id-XTec-PIVC-cardAuth	::= {1.3.6.1.4.1.13862.821.19.6}
	id-XTec-PIVC-medium-derivedHardware	::= {1.3.6.1.4.1.13862.821.19.8}
Medium Hardware AATL	id-XTec-AATL-HardwareMFA	::= {1.3.6.1.4.1.13862.821.7.1}
	id-XTec-AATL-HardwareToken	::= {1.3.6.1.4.1.13862.821.7.2}
FIPS 201 PIV-I	id-XTec-nfissp-pivi-cardAuth	::= {1.3.6.1.4.1.13862.821.2.20}
	id-XTec-nfissp-pivi-hardware	::= {1.3.6.1.4.1.13862.821.2.7}

Policy Type	Policy Name	Policy OID
	id-XTec-nfissp-contentsigning	::= {1.3.6.1.4.1.13862.821.2.9}
PIV-C	id-XTec-PIVC-contentSigning	::= {1.3.6.1.4.1.13862.821.19.9}
Medium Hardware Operations	id-XTec-ops-mediumHardware	::= {1.3.6.1.4.1.13862.821.1.4}
	id-XTec-ops-mediumHardwareAuth	::= {1.3.6.1.4.1.13862.821.1.5}
	id-XTec-ops- mediumDeviceHardware	::= {1.3.6.1.4.1.13862.821.1.8}

The requirements associated with the medium-devices policy are identical to those defined for the medium-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 medium-device policy is restricted to devices and systems.

The requirements associated with all medium-hardware policies are identical to those defined for the medium-policy with the exception of subscriber cryptographic module requirements (see Section 6.2.1).

The requirements associated with pivi-hardware, nfissp-contentsigning are identical to medium-hardware except where specifically noted in the text and further described in Appendix A.

The requirements associated with pivc-mediumhardware, pivc-mediumauthentication and pivc-contentsigning are identical to medium-hardware except where specifically noted in the text.

In addition, the nfissp-contentsigning, and PIVC-contentSigning policy is reserved for certificates used by the Card Management System (CMS). The nfissp-contentsigning policy is reserved for certificates used by the CMS to sign the PIV-I card security objects and the PIVC-contentsigning policy is reserved for certificates used by the CMS to sign the PIV-C card security objects.

The policy arc identified by Id-XTec-ops are used only for credentials issued to devices that are used to support the internal operations of the CA environment.

1.2.1. **FBCA Interoperation**

Certificates issued to CAs may contain any or all of the OIDs listed in Table 1.

This document includes three policies specific to the FIPS 201 Personal Identity Verification Interoperable Card. Certificates issued to PIV-I users supporting authentication, but not digital signature, shall contain id-XTec-nfissp-pivi-hardware. Certificates issued to users supporting authentication where the private key can be used without user authentication shall contain id-XTec-nfissp-medium-cardAuth. Entity certificates issued to a Card Management System (CMS) to sign the PIV-I card security objects shall contain id-XTec-nfissp-contentsigning. The id-XTec-nfissp-contentsigning policy OID is reserved for this specific purpose. An entity certificate asserting id-XTec-nfissp-contentsigning will be issued to a Card Management System (CMS) if the operator of the CMS has been authorized by the XTec PKI Policy Authority. This authorization shall only be completed after the CMS operator has completed testing to assure compliance with the requirements of the *Federal Identity, Credentialing, and Access Management Personal Identity Verification Interoperable (PIV-I), v1.1.0*.

Certificates issued to non-PIV-I users, other than devices, to support digitally signed documents or key management may contain either: id-XTec-nfissp-medium; id-XTec-nfissp-mediumHardware; id-XTec-nfissp-basic-policy; id-XTec-PIVC-medium; id-XTec-PIVC-medium-

derived; id-XTec-PIVC-mediumHardware; id-XTec-PIVC-mediumAuthentication; id-XTec-PIVC-medium-derivedHardware; id-XTec-AATL-HardwareMFA; id-XTec-AATL-HardwareToken; or id-XTec-PIVC-basic. Subscriber certificates issued to non-PIV-I devices under this policy shall include id-XTec-nfissp-mediumDevice or id-XTec-PIVC-mediumDevice.

Per CIO Council's document, cards issued under this policy, with the id-XTec-nfissp-pivi-hardware policy asserted, will be referred to as PIV Interoperable Cards. The generation of PIV Interoperable Cards is the responsibility of each individual non-federal organization (state and local governments or commercial entities). XTec PKI will only provide the PKI credentials that will be populated on the PIV Interoperable Cards issued by each non-federal organization.

NOTE: The FIPS 201 PIV Card is specific to the U.S. Federal Government. The CIO Council has released the following paper regarding interoperability between U.S. Federal Government PIV systems and non-federally issued identity cards: *Personal Identity Verification Interoperability For Non-Federal Issuers; Issued by Federal CIO Council; March 2009*

1.3. PKI Participants

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

1.3.1. PKI Authorities

1.3.1.1 XTec PKI Policy Authority (XTecPA)

The XTec PKI Policy Authority (XTecPA) is the custodian of the XTec Non-Federal Public Key Infrastructure X.509 Certificate Policy and is responsible for PKI policy administration including the approval of policy changes.

1.3.1.2 XTec PKI Operational Authority (XTecOA)

The XTec PKI Operational Authority (XTecOA) is responsible for oversight of the operational aspects of the CA, RA, CSS and directory services in place to support the operations of the XTec PKI.

1.3.2. Certification Authorities

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

- The certificate manufacturing process
- Publication of certificates
- Revocation of certificates
- Generation and destruction of CA signing keys
- Ensuring that all aspects of the CA services, operations, and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

This policy does not presume any particular PKI architecture. The policy may be implemented through a hierarchical PKI or mesh PKI. The CPS shall describe the PKI architecture for CAs operated under this CP.

It is the responsibility of the XTecPA to designate which CAs shall be cross-certified with external entity CAs as a “Principal CA”. A CA that is to be designated as a Principal CA:

- May be a self-signed CA; and
- Shall comply with the requirements of a Principal CA under the policies of any external entity to which it cross-certifies; and

A CA that issues subscriber certificates, referred to as an “Issuing CA”, shall not issue CA certificates, with the exception of cross-certificates as approved by the XTecPA.

1.3.3. Card Management Systems

The Card Management System is responsible for managing smart card token content. In the context of this policy, the CMS requirements are associated with the policies that are defined under the FIPS 201 PIV-I Policy Type, as identified in Table 1.

Entity CAs issuing PIV-I certificates are responsible for ensuring that all CMSs meet the requirements described in this document, including all requirements specified in Appendix A. In addition, the CMS shall not be issued any certificates that express the id-XTec-nfissp-pivi-hardware, id-XTec-PIVC-cardAuth or id-XTec-nfissp-medium-cardAuth policy OID.

1.3.4. Registration Authorities

The registration authorities (RAs) collect and verify each subscriber’s identity and information that is to be entered into the subscriber’s public key certificate. The RA performs its function in accordance with a CPS approved by the XTecPA. The RA is responsible for:

- Control over the registration process
- The identification and authentication process.

The CA reserves the right to audit records kept by delegated RAs to ensure the RAs’ processes and procedures are in compliance with this CP and any applicable CPS.

1.3.4.1 Trusted Agents

The Trusted Agent is a person, authorized by an existing RA, who satisfies all the trustworthiness requirements for an RA and who performs identity proofing as a proxy for the RA. The trusted agent records information from and verifies biometrics (e.g., photographs) on presented credentials for applicants who cannot appear in person at an RA. The CPS will identify the parties responsible for providing such services, and the mechanisms for determining their trustworthiness, including, but not limited to, vetting requirements and appropriate training and/or government appointments, such as a notary public.

The CPS must also detail how actions performed by a Trusted Agent are traceable to the individual holding the Trusted Agent role.

1.3.5. Certificate Status Servers

PKIs may optionally include an authority that provides status information about certificates on behalf of a CA through on-line transactions. In particular, PKIs may include OCSP responders to provide on-line status information. Such an authority is termed 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 include OCSP servers that are identified in the authority information access (AIA)

extension. OCSP servers that are locally trusted, as described in RFC 2560, are not covered by this policy.

1.3.6. Key Recovery Authorities

For organizations that have implemented a Key Recovery Authority, the applicable requirements for physical, personnel, and procedural security controls, technical security controls, and Compliance Audit are applied as follows:

- CA requirements are applied to the Key Escrow Database (KED) and to the Data Decryption Server (DDS);
- RA requirements are applied to the Key Recovery Agent (KRA) and KRA automated systems

1.3.6.1 Key Escrow Database

The KED is defined as 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 5.2.1.2 contains the description of trusted roles required to operate the KED.

1.3.6.2 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). DDSs do 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 on organizational operations.

1.3.6.3 Key Recovery Agent

A KRA is an individual who is authorized, as specified in the applicable Practice Statement (KRPS or CPS), to recover an escrowed key. The KRAs have high level, sensitive access to the KED and are considered Trusted Roles (see Section 5.2.1). KRAs can recover large numbers of keys, the number and location of KRAs should be closely controlled.

A KRA will confirm validity and completeness of requests prior to taking any action. After confirmation is made the KRA will recover copies of the requested keys and distribute these to the Requestor in a protected manner as described in 4.12.1.3.

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

1.3.6.4 Key Recovery Official

A Key Recovery Official (KRO) may optionally be used to support key recovery requestor identity verification and authorization validation tasks.

A KRO is NOT a Trusted Role but has the responsibilities to:

- Verify a Requestor’s identity and authorization per this policy;
- Assist authorized requestors to build valid key recovery requests;

- Ensure the use of secure communications for key recovery requests to and responses from a KRA; and
- As needed participate in the delivery of escrowed keys to the identified Requestor, ensuring the processes are used are those defined in the appropriate CPS or KRPS.

1.3.7. Key Recovery Requestors

For organizations that have implemented Key Recovery the organization will interact with entities, either internal or external, dependent on implementation, who will request access to escrowed keys.

A Requestor is the person 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 organization. Any individual who can demonstrate a verifiable authority and a need to obtain a recovered key may be considered a Requestor.

1.3.7.1 Internal Third-Party Requestor

An Internal Third-Party Requestor is any Requestor who is in the Subscriber's supervisory chain or otherwise authorized to obtain the Subscriber's key for the Issuing Organization, that is the organization on behalf of which the CA issues certificates to subscribers.

1.3.7.2 External Third-Party Requestor

An External Third-Party Requestor is someone outside the Issuing Organization, such as an investigator, with a court order or other legal instrument to obtain the decryption private key of the Subscriber.

1.3.8. Subscribers

The user policies apply to certificates issued to state government, local government, and commercial employees, contractors, and other affiliated personnel for the purposes of authentication, signature, and confidentiality. The term "agency" is used to specify the state government, local government, or commercial entity that employs the subscriber.

A subscriber is the entity whose name appears as the subject in a certificate. The subscriber asserts that he or she uses the key and certificate in accordance with the certificate policy asserted in the certificate, and does not issue certificates. CAs are sometimes technically considered "subscribers" in a PKI. However, the term "subscriber" as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information.

There may be a subset of human subscribers that can 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 and are issued in the interest of supporting accepted business practices. The role-based certificate can be used in situations where non-repudiation is desired. Normally, role-based certificates are issued in addition to an individual subscriber certificate. A specific role may be identified in certificates issued to multiple subscribers, however, the key pair will be unique to each individual role-based certificate (i.e. there may be four individuals carrying a certificate issued in the role of "Secretary of Commerce" however, each of the four individual certificates will carry unique keys and certificate identifiers). Roles for which role-based certificates may be issued are limited to those that are held by a unique individual within

an organization (e.g. *Chief Information Officer, GSA* is a unique individual whereas *Program Analyst, GSA* is not).

1.3.9. 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.

1.3.10. Relying Parties

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

For this certificate policy, the relying party may be any entity that wishes to validate the binding of a public key to the name (or role) of a subscriber.

1.3.11. Remote Signing Service Provider (RSSP)

The private keys for multiple subscribers may be stored on a remote signing service provider, or RSSP, based on a hardware security module (HSM) interfaced to a server. This permits the subscribers to access their credentials from multiple workstations and locations. For the purposes of this CP, any centralized aggregation of subscriber private keys must comply with the requirements for a RSSP as specified in this CP.

1.3.12. Other Participants

The CAs and RAs operating under this CP may require the services of other security, community, and application authorities, such as compliance auditors and attribute authorities. The CPS will identify the parties responsible for providing such services, and 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 the CA will vary significantly. Organizations 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 organization for each application and is not controlled by this CP.

This CP is intended to support the use of validated public keys to access Federal, State or local government systems that have not been designated national security systems. While a validated public key is not generally sufficient to grant access the key may be sufficient when supplemented by appropriate authorization mechanisms.

Credentials issued under this CP may be used for

- Signing
- Encryption
- Client Authentication
- Key establishment.

Other uses of a certificate are allowed if the Relying Parties can rely on the certificate for that purpose, and the usage is not prohibited by law, or this CP, or the CPS under which the certificate was issued.

Credentials issued under the medium software policies are intended to meet the requirements for Level 3 authentication, as defined by the OMB E-Authentication Guidance. [E-Auth] Credentials issued under the medium hardware and FIPS 201 PIV policies meet the requirements for Level 4 authentication, as defined by the OMB E-Authentication Guidance [E-Auth].

Credentials issued under the AATL policies (1.3.6.1.4.1.13862.821.7.x) are intended to meet the requirements for use in Adobe Approved Trust List (AATL) program, as defined in *Adobe Approved Trust List Technical Requirements Version 2.0, June 2017*.

Credentials issued under the XTec Operations policies, id-XTec-ops, identified under the policy arc, 1.3.6.1.4.1.13862.821.1.x, are intended for use by RAs and systems within the PKI architecture. These policies are not to be used by non-role holder subscribers.

Credentials issued under a basic policy are intended to provide 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.

1.4.2. Prohibited Certificate Uses

Certificates that assert id-XTec-nfissp-pivi-cardAuth, id-XTec-PIVC-cardAuth or id-XTec-nfissp-medium-cardAuth shall only be used to authenticate the hardware token containing the associated private key and shall not be interpreted as authenticating the presenter or holder of the token.

Certificates shall not be issued to a Card Management System (CMS) that assert id-XTec-nfissp-pivi-hardware, id-XTec-PIVC-cardAuth or id-XTec-nfissp-medium-cardAuth.

Certificates that assert id-XTec-nfissp-pivi-hardware, id-XTec-PIVC-mediumHardware or id-XTec-nfissp-mediumHardware shall not be issued to non-human subscribers.

1.5. Policy Administration

1.5.1. Organization Administering the Document

The XTec Policy Authority 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 XTec Policy Authority (XTecPA), whose address can be found below:

XTec Policy Authority

11180 Sunrise Valley Drive, Suite 310

Reston, VA 20191

XTecPA@xtec.com

1.5.3. Person Determining CPS Suitability for the Policy

The XTecPA shall approve the CPS for each CA that issues certificates under this policy.

For CAs that have a CPS managed by this policy that operate under the FPKI Common Policy, the CPS must be approved by the FPKIPA as well as the XTecPA.

1.5.4. CPS Approval Procedures

The XTecPA shall make the determination that a CPS complies with this policy. The CA and RA must meet all requirements of an approved CPS before commencing operations. In some cases, the XTecPA may require the additional approval of an external authority. The XTecPA will make this determination based on the nature of the system function, the type of communications, or the operating environment.

For CAs that have a CPS managed by this policy that operate under the FPKI Common Policy, the CAs are required to meet all requirements of the FPKI Common Policy. Such CAs will not be issued any waivers.

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

1.6. Definitions and Acronyms

1.6.1. List of Definitions

Authority Revocation List: A list of revoked Certification Authority cross-certificates and root certificates.

Activation Data*: Data values, other than Keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a passphrase, or a manually-held Key share).

CA Certificate: A Certificate for one CA's Public Key issued by another CA.

CA Private Signing Key: The Private Key corresponding to a Public Key listed in a CA Certificate and is used to sign XTec PKI Commercial PKI certificates.

CA Private Primary Key: The Private Key used to sign CA Certificates and corresponds to the Key signed by XTec Certificate Services Root CA Key.

Certificate: A computer-based record or electronic message that identifies the issuing Certificate Authority, the name or identity of the Subscriber, contains the Public Key of the Subscriber, lists a validity period, is digitally signed by a Certification Authority, and has

meaning given in this Certificate Policy and applicable standards. A Certificate includes not only the actual information contained within, but also all documents expressly referenced or incorporated into the Certificate.

Certificate Revocation List (CRL): A list of Certificates revoked prior to the expiration of their Validity Periods

Certification Authority (CA): An entity that creates, issues, manages and revokes Certificates

Certificate Policy*: A named set of rules that indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of Certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range.

Certification Practice Statement (CPS)*: A statement of the practices that a Certification Authority employs in issuing, managing, revoking, and renewing or Re-Keying Certificates.

Cryptomodule: Either software, a device, or a utility that generates Key Pairs, stores cryptographic information, and/or performs cryptographic functions.

Digital Signature, Digitally Sign: The transformation of an electronic record by one person using a Private Key and Public Key Cryptography so that another person having the transformed record and the corresponding Public Key can accurately determine whether the transformation was created using the Private Key that corresponds to the Public Key and whether the record has been altered since the transformation was made.

Distinguished Name (DN): The unique identifier for a Subscriber so that s/he can be located in a directory based on the ITU/CCITT X.500 (e.g. the DN for a Subscriber might contain the following attributes: common name (cn), e-mail address (mail), Organization name (o), Organizational unit (ou), locality (l), state (st) and country (c)).

End Entity: A Subscriber and/or authorized Relying Party.

Issue Certificates, Issuance: The act performed by a CA in creating a Certificate listing with the CA as “Issuer,” and notifying the Applicant of the contents and that the Certificate is ready and available for Acceptance.

Issuing Certification Authority (Issuing CA)*: In the context of a particular Certificate, the issuing CA is the CA that issued the Certificate (see also Subject Certification Authority).

Key Generation: The process of creating a Key Pair.

Key Pair: Two mathematically related Keys (a Private Key and the corresponding Public Key), with the following properties:

- one Key can encrypt a communication only capable of decryption by the other Key; and
- deriving or discovering one Key from the other Key is computationally infeasible, assuming likely circumstances including the availability of text encrypted by either of the Keys.

Lightweight Directory Access Protocol (LDAP): A client-server protocol used for accessing X500 directory services over a computer network.

Object Identifier (OID): The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the PKS established by

this CPS, they are used to uniquely identify Certificates issued under this CPS and the cryptographic algorithms supported.

Online Certificate Status Protocol (OCSP): A protocol that is used to provide real-time validation of a Certificate's status. An OCSP responder is used to respond to Certificate status requests and can issue one of three responses: Valid, Invalid, Unknown. An OCSP responder replies to Certificate status requests on the basis of CRLs (Certificate Revocation Lists) provided to it by certification authorities.

Operational Period: A Certificate's actual term of validity, beginning with the start of the Validity Period and ending with the earlier of:

- the end of the Validity Period disclosed in the Certificate, or
- the revocation date of the Certificate.

Private Key: The sensitive Key in the Key Pair protected by the Subscriber and kept secret. The Private Key creates Digital Signatures or decrypts data previously encrypted using the corresponding Public Key.

Public Key: The non-sensitive Key in the Key Pair disclosed by the Subscriber holding the corresponding Private Key. The Public Key verifies Digital Signatures created using the corresponding Private Key, or encrypts data meant for decryption with the corresponding Private Key.

Public Key Cryptography: A type of cryptography also knows as asymmetric cryptography. This cryptography uses a Key Pair rather than a single Key to secure the authentication and/or confidentiality of data.

Public Key Infrastructure (PKI): The architecture, technology, practices, and procedures that support operation of a security system employing Certificates and Public Key Cryptography.

Public Key Service (PKS): This is identical with Public Key Infrastructure, with the word Service used to emphasis on leveraging the environment to service XTec PKI Commercial customers.

Registration Authority (RA): An individual or organization responsible for verifying the identity of a Subscriber or, in the case of another Business Unit, a Designated Certificate Holder.

Relying Party[1]: A recipient of a Certificate who acts in reliance on that Certificate and/or any digital signatures verified using that Certificate.

Repository: An online system maintained by an Issuing CA for storing and retrieving Certificates and other information relevant to Certificates, including information relating to Certificate validity or revocation.

Revoke (a Certificate): To invalidate a Certificate permanently from a specific time onward. Revocation includes listing the Certificate in a set of revoked Certificates or other directory or database of revoked Certificates (e.g. inclusion in a CRL). The system also prevents users from accessing revoked Certificates once connected to the central infrastructure.

[1] *Taken from the standard for Certificate Policies (RFC 3647)

Request For Comments (RFC): Document series used as the primary means for communicating information about the Internet. Some RFCs are designated by the IAB as Internet standards. Most RFCs document protocol specifications such as Telnet and FTP.

Subject Certification Authority: In the context of a particular CA-Certificate, the subject CA is the CA whose Public Key is certified in the Certificate (see also Issuing certification authority).

Subject Name: The specific field in a Certificate containing the Distinguished Name (DN) for the Subscriber.

Subscriber: A subject of a Certificate who is issued a Certificate.

Subscriber Agreement: An agreement between a CA and a Subscriber that establishes the right and responsibilities of the parties regarding the issuance and management of Certificates.

Token: A Cryptomodule consisting of a hardware object (e.g. a “smart card”), often with memory and a microchip.

Trusted Role: The execution of these roles requires adherence to policy and procedures to prevent the introduction of security problems. The functions of Trusted Roles form the basis of trust for the entire PKS.

Validity Period: The intended term of validity of a Certificate, beginning with the date of Issuance (“Valid From” or “Activation” date), and ending with the earlier of two dates: the expiration date indicated in the Certificate (“Valid To” or “Expiry” date) or the revocation date asserted in the revocation list specified as the CRL Distribution Point within the certificate.

x.500: A series of computer networking standards covering electronic directory services. These services include Directory Access Protocol (DAP), Directory System Protocol (DSP), Directory Information Shadowing Protocol (DISP), and Directory Operational Bindings Management Protocol (DOP).

x.509: An International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) standard for Public Key Infrastructure which specifies standard formats for public key certificates and certification path validation.

XTec PKI Commercial PKI Certificate: A Certificate issued pursuant to this Certificate Policy.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

All CAs that issue certificates under this policy are obligated to post all CA certificates issued by or to the CA and CRLs issued by the CA in a directory that is publicly accessible through the Lightweight Directory Access Protocol (LDAP) and Hypertext Transport Protocol (HTTP). Specific requirements are found in *Shared Service Provider Repository Service Requirements* [SSP-REP]. CAs may optionally post subscriber certificates in this directory in accordance with agency or organizational policy, except as noted in section 9.4.3. To promote consistent access to certificates and CRLs, the repository shall implement access controls to prevent unauthorized modification or deletion of information.

Posted certificates and CRLs may be replicated in additional repositories for performance enhancement. Such repositories may be operated by the CA or other parties (e.g., State or local government agencies or subscribers' organizations).

The publicly accessible repository system must be designed and implemented so as to provide an overall availability of 99% and limit scheduled downtown to no more than 0.5% annually.

2.1.1. Repository Obligations

A variety of mechanisms may be used for posting information into a repository. The repository obligations shall include:

- X.500 Directory Server System that is also accessible through the Lightweight Directory Access Protocol (LDAP, version 3), or Hypertext Transfer Protocol (HTTP),
- Availability of the information as required by the certificate information posting and retrieval stipulations of this CP, and
- Access control mechanisms when needed to protect repository availability and information as described in later sections.

2.2. Publication of Certification Information

2.2.1. Publication of Certificates and Certificate Status

All CAs that issue CA certificates must publish all CA certificates it issues in a file available via a publicly accessible HTTP URI. This URI must be asserted in the Subject Information Access (SIA) extension in all valid certificates issued to the CA. The file must be a certs-only Cryptographic Message Syntax file that has an extension of .p7c.

With the exception of self-signed certificates, all CA certificates must be published by the Subject CA in a file available via a publicly accessible HTTP URI. This URI must be asserted in the Authority Information Access (AIA) extension in all valid certificates issued by the Subject CA. The file must be:

- a certs-only Cryptographic Message Syntax file that has an extension of .p7c, or
- a single DER encoded certificate that has an extension of .cer

All CAs that issue certificates under this policy must publish the latest CRL covering all unexpired certificates via a publicly accessible HTTP URI until such time as all issued

certificates have expired. This URI must be asserted in the CRL distribution point extension of all certificates issued by that CA, with the exception of Online Certificate Status Protocol (OCSP) responder certificates that include the id-pkix-ocsp-nocheck extension.

A Certificate Status Server (CSS) provides status information about certificates on behalf of a CA through on-line transactions.

CAs must include a CSS in the form of a delegated OCSP service, as described in [RFC 6960], to provide on-line status information for Subscriber certificates via a publicly accessible HTTP URI in the AIA extension. The operations of the OCSP service are within the scope of this CP.

Pre-generated OCSP responses may be created by the CSS and distributed to OCSP servers. OCSP responses, like CRLs, are publicly distributable data. OCSP servers that lack OCSP response signing capability have the same security requirements as a repository hosting CRLs.

OCSP services that are locally trusted, as described in [RFC 6960], are not covered by this policy.

All certificates must contain only valid Uniform Resource Identifiers (URIs) that are publicly accessible by relying parties.

2.2.2. Publication of CA Information

The XTec PKI Non-Federal PKI (XTec PKI) CP shall be publicly available on the XTec web site.

Practice Note: There is no requirement for the publication of CPSs of CAs that issue certificates under this policy, however, CAs that must make their CPS available for review by the XTec PA and, where appropriate, the FPKIPA. These CPS may be redacted to protect sensitive information.

2.3. Time or Frequency of Publication

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

Publication requirements for CRLs are provided in sections 4.9.7 and 4.9.12.

2.4. Access Controls on Repositories

The CA shall protect repository information not intended for public dissemination or modification. CA certificates and CRLs in the repository shall be publicly available through the Internet.

Access to other information in the CA repositories shall be determined pursuant to the authorizing and controlling statutes, within contractual agreements that specify these requirements or by subscribers' organizations based upon their policies and practices. The CPS shall detail what information in the repository shall be exempt from automatic availability and to whom, and under which conditions the restricted information may be made available.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

3.1.1. Types of Names

For certificates issued under all policies, excluding FIPS 201 PIV-I policies, the CA shall assign X.501 distinguished names to all subscribers. These distinguished names may be in either of two forms: a geo-political name or an Internet domain component name. Each relative distinguished name shall contain a single attribute type and value pair, with the exception of `serialNumber` and `commonName`.

Directory strings shall be encoded as `printableString`. Common name may be encoded as `UTF8`, if it cannot be properly encoded as `printableString`.

Conventions used within this section include:

- Square brackets [ ] which indicate fields that must be present
- Angled brackets < > which indicates fields that may be present
- Italicized lettering indicates variables. An example would be *firstname lastname* which indicate two variables that would be set at the time of issuance or definition

Certificates issued under this policy may be issued under one of four (4) Directory Address prefixes, these are identified as:

- c=US, o=XTec
- c=US, o=AuthentX
- c=US, o=XTec Incorporated
- c=US, o=XTec PIV-I SSP

Throughout this document the Directory Address Prefix will be identified as [*DirAddressPrefix*]

All geo-political distinguished names assigned to state government, local government, or commercial employees, with a specific affiliation, shall be in the following directory information tree (DIT):

- [DirAddressPrefix], ou=[shared CA], ou=[state/local government or company name], <ou=department>, <ou=agency>, <ou=structuralcontainer>

All geo-political distinguished names assigned to a State Government that may request that a separate issuing CA be created solely for their use, shall be in the following DIT:

- c=US, o=[state government name], <ou=department>, <ou=agency>, <ou=structuralcontainer>

All geo-political distinguished names assigned to entities, with no specific affiliation, shall be in the following DIT:

- [DirAddressPrefix], ou=[shared CA], ou=Unaffiliated, <ou=structural_container>

The organizational units *department* and *agency* appear when applicable and are used to specify the state government, local government, or commercial entity that employs the subscriber. At least one of these organizational units must appear in the DN. The additional

organizational unit *structural_container* is permitted to support local directory requirements, such as differentiation between human subscribers and devices. This organizational unit may not be employed to further differentiate between subcomponents within an agency.

The distinguished name of the state government, local government, or commercial employee subscriber shall take one of the following forms:

- [DirAddressPrefix], ou=[shared CA], ou=[state/local government or company name], <ou=department>, <ou=agency>, <ou=structuralcontainer>, cn=nickname lastname
- [DirAddressPrefix], ou=[shared CA], ou=[state/local government or company name], <ou=department>, <ou=agency>, <ou=structuralcontainer>, cn=firstname initial. lastname
- [DirAddressPrefix], ou=[shared CA], ou=[state/local government or company name], <ou=department>, <ou=agency>, <ou=structuralcontainer>, cn=firstname middlename lastname

Where a State Government may request that a separate issuing CA be created solely for their use, the distinguished name of the state government employee subscriber shall take one of the following forms:

- c=US, o=[state government name], <ou=department>, <ou=agency>, <ou=structuralcontainer>, cn=nickname lastname
- c=US, o=[state government name], <ou=department>, <ou=agency>, <ou=structuralcontainer>, cn=firstname initial. lastname
- c=US, o=[state government name], <ou=department>, <ou=agency>, <ou=structuralcontainer>, cn=firstname middlename lastname

The distinguished name of subscribers with no specific affiliation shall take one of the following forms:

- [DirAddressPrefix], ou=[shared CA], ou=Unaffiliated, <ou=structural_container>, cn=nickname lastname
- [DirAddressPrefix], ou=[shared CA], ou=Unaffiliated, <ou=structural_container>, cn=firstname initial. lastname
- [DirAddressPrefix], ou=[shared CA], ou=Unaffiliated, <ou=structural_container>, cn=firstname middlename lastname

In the first name forms, *nickname* may be the subscriber's first name, a form of the first name, middle name, or pseudonym (e.g., Buck) by which the subscriber is generally known. A generational qualifier, such as "Sr." or "III", may be appended to any of the common name forms specified above. For unaffiliated subscribers, the Structural container will be used to guarantee uniqueness of the DN.

Common name fields shall be populated as specified above.

Distinguished names based on Internet domain component names shall be in the following directory information tree(s):

- dc=org0, <dc=org1>, …, <dc=orgN>, <ou=structural_container>

The default Internet domain name for the agency, [*orgN*.]…[*org0*].gov or [*orgN*.], shall be used to determine DNs. The first domain component of the DN for state and local governments will be dc=gov. At a minimum, the *org0* and *org1* domain components must appear in the DN. The

org1 to *orgN* domain components appear, in order, when applicable and are used to specify the entity that employs the subscriber. Internet domain naming will not be utilized for unaffiliated subscribers.

The distinguished name of the state government, local government, or commercial employee subscriber shall take one of the following forms:

- dc=org0, <dc=org1>, …, <dc=orgN>, <ou=structural_container>, cn=nickname lastname
- dc=org0, <dc=org1>, …, <dc=orgN>, <ou=structural_container>, cn=firstname initial. lastname
- dc=org0, <dc=org1>, …, <dc=orgN>, <ou=structural_container>, cn=firstname middlename lastname

The CA may supplement any of the name forms for users specified in this section by including a dnQualifier, serial number, or user id attribute. When any of these attributes are included, they may appear as part of a multi-valued relative distinguished name (RDN) with the common name or as a distinct RDN that follows the RDN containing the common name attribute. Generational qualifiers may optionally be included in common name attributes in distinguished names based on Internet domain names. For names assigned to employees, generational qualifiers may be appended to the common name. For names assigned to state government, local government, or commercial contractors and other affiliated persons, generational qualifiers may be inserted after *lastname*.

Signature certificates issued under id-XTec-nfissp-mediumHardware may be issued with a common name that specifies an organizational role, such as the head of an agency, as follows:

- [appropriate DIT as defined above], cn=[*role within department/agency*]

The combination of organizational role and agency must unambiguously identify a single person. (That is, widely held roles such as *Computer Scientist* or *Procurement Specialist* cannot be included since they do not identify a particular person. *Chief Information Officer*, *AgencyX* could be included as it specifies a role held by a single person.)

Where the [department/agency] is implicit in the role (e.g., Secretary of Commerce), it should be omitted. Where the role alone is ambiguous (e.g., Chief Information Officer) the department/agency must be present in the common name. The organizational information in the common name shall match that in the organizational unit attributes.

Practice Note: In the case of “Chief Information Officer”, use of department or agency or organization in the common name is redundant but is included for usability purposes. Display of the common name is widely supported. Other attributes may or may not be presented to users.

Devices that are the subject of certificates issued under this policy shall be assigned either a geo-political name or an Internet domain component name. Device names shall take one of the following forms:

- [appropriate DIT as defined above], cn=[*device name*]

where *device name* is a descriptive name for the device. Where a device is fully described by the Internet domain name, the common name attribute is optional.

This policy does not restrict the directory information tree for names of CAs and CSSs. However, CAs that issue certificates under this policy shall have distinguished names. CA and

CSS distinguished names may be either a geo-political name or an Internet domain component name.

CA and CSS geo-political distinguished names shall be composed of any combination of the following attributes: country; organization; organizational unit; and common name. Internet domain component names are composed of the following attributes: domain component; organizational unit; and common name.

3.1.1.1 FIPS 201 PIV-I Policies

For certificates issued under id-XTec-nfissp-pivi-hardware, assignment of X.500 distinguished names is mandatory and distinguished names shall follow either the rules specified above or the rules specified below for including a non-NULL subject DN in id-XTec-nfissp-pivi-cardAuth. Certificates issued under id-XTec-nfissp-pivi-hardware shall include a subject alternative name, which contains the following:

- UUID from the CHUID of the PIV-I card encoded as a URI
- the User Principal Name (UPN) as identified with the OID 1.3.6.1.4.1.311.20.2.3.

Certificates issued under id-XTec-nfissp-pivi-cardAuth shall include a subject alternative name extension that includes a unique smart card number that is comparable to the pivFASC-N name type used in FIPS 201 PIV Cards. The value for this name shall be the smart card number of the subject's PIV card.

Certificates issued under id-XTec-nfissp-pivi-cardAuth shall not include any other name in the subject alternative name extension but may include a non-NULL name in the subject field. If included, the subject distinguished name shall take one of the following forms:

for affiliated subscribers;

- [appropriate DIT as defined above], serialNumber=*UUID*

for unaffiliated subscribers;

- [appropriate DIT as defined above], ou=Unaffiliated*,* <ou=*structural_container*>, serialNumber=*UUID*

where the UUID shall be encoded within the serialNumber attribute using the UUID string representation defined in Section 3 of RFC 4122.

Practice Note: FIPS 201 PIV-I Cards include what is known as the Federal Agency Smart Card Number (FASC-N) [PACS] in order to uniquely identify each smart card. Non-federal organizations must generate a similar smart card numbering scheme. This numbering scheme must meet the requirements specified in *Personal Identity Verification Interoperability For Non-Federal Issuers; Issued by Federal CIO Council; July 2017*. This numbering scheme may be based on the FASC-N format, with the additions noted below.

The FASC-N is not designed to insure uniqueness for non-federal issuers. For non-federal issuers, additional tag length value (TLV) elements must be specified to insure uniqueness of the smart card number. If a FASC-N Agency Code of 9999 is present in the smart card number, then the DUNS TLV record in the CHUID container will indicate the identity of the card issuer. It is anticipated that the Tag 30 TLV record will always exist for industry compatibility for PACS that use the System Code and Card Number as a card identifier.

For issuers not defined in SP 800-87, a smart card number can be constructed using an Agency Code of 9999; however, this will not provide uniqueness of the smart card number for interaction

with federal agency applications. If a non-federal issuer has a requirement for federal interoperability, then a sponsoring agency may assign a specific System Code(s) to the issuer. When an Agency Code of 9999 is specified, an issuer must include an additional TLV record in the CHUID, such as the DUNS, to insure uniqueness of the CHUID. It is the responsibility of the sponsoring agency to maintain records of specific System Code assignments for both internal and external issuers of FASC-Ns.

This policy does not mandate any particular method for encoding the smart card number within the serial number attribute as long as the same encoding method is used for all certificates issued by a CA. Acceptable methods for encoding the smart card number within the serial number attribute include encoding the 25-byte binary value as 50 bytes of ASCII HEX or encoding the 40 decimal digits as 40 bytes of ASCII decimal. When included in the subject field the unique smart card number must be encoded as a PrintableString that is at most 64 characters long.

Certificates issued to subscribers under id-XTec-nfissp-contentsigning will take one of the following name forms:

- [DirAddressPrefix], ou=[shared CA], ou=[state/local government or company name], <ou=department>, <ou=agency>, <ou=structuralcontainer>, cn=CMS_content_signing_device
- dc=org0, [dc=org1],.., [dc=orgN], [ou=structural_container], cn=CMS_content_signing_device

where the Fully Qualified Distinguished Name (FQDN) will fully and uniquely identify the organization operating the card management system, CMS, which is issuing the PIV-I devices whose content is signed using the associated private key.

3.1.1.2 Subject Alternative Names

Values that are asserted in the subjectAltName extension within a certificate MUST asdhere to the following:

- Subscriber certificates that contain id-kp-emailProtection in the EKU must include a subject alternative name extension that includes a rfc822Name.
- 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 service, or system boundary within the scope of the sponsoring organization.

3.1.2. Need for Names to Be Meaningful

The subscriber certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates can be understood and used by relying parties. Names used in the certificates must identify in a meaningful way the subscriber to which they are assigned.

The common name in the DN shall represent the subscriber in a way that is easily understandable for humans. For people, this will typically be a legal name, so the preferred common name form is

cn=firstname initial. lastname

When User Principal Name (UPN) is used in the subjectAlternativeName then the structure of the UPN will reflect the organizations UPN structure for affiliated subjects.

While the issuer name in CA certificates is not generally interpreted by relying parties, this CP still requires use of meaningful names by CAs issuing under this policy. If included, the common name should describe the issuer, such as:

cn=AgencyX CA

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

3.1.3. Anonymity or Pseudonymity of Subscribers

The CA shall not issue anonymous certificates.

Pseudonymous certificates may be issued by the CA to support internal operations.

CAs may also issue pseudonymous certificates that identify subjects by their organizational roles, as described in section 3.1.1.

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

3.1.4. Rules for Interpreting Various Name Forms

Rules for interpreting distinguished name forms are specified in X.501. Rules for interpreting e-mail addresses are specified in [RFC 2822].

3.1.5. Uniqueness of Names

Name uniqueness for certificates issued by each CA must be enforced. Each CA and its associated RAs shall enforce name uniqueness within the X.500 name space. When other name forms are used, they too must be allocated such that name uniqueness is ensured for certificates issued by that CA.

Practice Note: For distinguished names, name uniqueness is enforced for the entire name rather than a particular attribute, such as common name.

The CPS shall identify the method for the assignment of subject names. Directory information trees may be assigned to a single CA, or shared between CAs. Where multiple CAs share a single directory information tree, the XTecPA shall review and approve the method for assignment of subject names.

3.1.6. Recognition, Authentication, and Role of Trademarks

CAs operating under this policy shall not issue a certificate knowing that it infringes the trademark of another. The XTecPA shall resolve disputes involving names and trademarks.

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

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

In the case where key generation is performed under the CA or RA's direct control, proof of possession is not required.

3.2.2. Authentication of Organization Identity

Requests for CA certificates shall include the requesting organization's name, address, and documentation of the existence of the specified CA. Before issuing CA certificates, an authority for the issuing CA (e.g., XTecPA or OA) shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the CA organization.

Requests for role or group certificates, in the name of an organization, shall include the requesting organization's name, address, and documentation of the existence of the specified organization. Before issuing the certificates, an authority for the issuing organization shall verify the information, in addition to 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

This policy allows a certificate to be issued only to a single entity. Certificates shall not be issued that contain a public key whose associated private key is shared.

3.2.3.1 Authentication of Human Subscribers

Procedures used by agencies and/or by subscribers' organizations to issue identification to their own personnel and affiliates may be more stringent than that set forth below. When this is the case, the agency procedures for authentication of personnel shall apply in addition to the guidance in this section.

The RA shall ensure that the applicant's identity information is verified. Identity shall be verified no more than 30 days before initial certificate issuance. For all policies, RAs may accept authentication of an applicant's identity attested to and documented by a trusted agent to support identity proofing of remote applicants, assuming agency or organizational identity badging requirements are otherwise satisfied. For all policies, except PIV-I policies, supervised remote identity proofing is valid.

3.2.3.1.1 Basic Policies

An entity certified by a State or Federal Entity as being authorized to confirm identities may perform in-person authentication on behalf of the RA. The certified entity forwards the information collected from the applicant directly to the RA in a secure manner. Packages secured in a tamper-evident manner by the certified entity satisfy this requirement; other secure methods are also acceptable. Such authentication does not relieve the RA of its responsibility to verify the presented data.

Identity may be established by in-person proofing or supervised remote identity proofing before a Registration Authority or Trusted Agent; or by remotely 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 confirming that name, DoB, address and other personal information in records are consistent with the application and sufficient to identify a unique individual.

Address confirmation of applicant:

- Issue credentials in a manner that confirms the address of record supplied by the applicant; or
- Issue 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.

The RA shall record the process that was followed for issuance of each certificate. The process documentation and authentication requirements shall include the following:

- 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 by the CPS using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury);
- Unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- The date and time of the verification; and
- For in-person or supervised remote identity proofing, a declaration of identity signed by the applicant using a handwritten signature and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury). For supervised remote identity proofing the signed declaration must be securely sent to the RA or Trusted Agent.

3.2.3.1.2 PIV-I Policies

Authentication procedures for subscribers issued under a PIV-I policy must include the steps listed below. Authentication by a trusted agent does not relieve the RA of its responsibility to perform steps 1), 2), the verification of identifying information (e.g., by checking official records) in step 3), and the maintenance of biometrics in step 4), below.

1) Verify that a request for certificate issuance to the applicant was submitted by an authorized agent of the sponsoring organization
2) Verify sponsoring agency employee's identity and employment through either of the following methods:
    a) A digital signature verified by a currently valid employee signature certificate issued by the CA may be accepted as proof of both employment and identity, or
    b) Employee's identity shall be established by in-person proofing before the registration authority as in employee authentication above and employment validated through use of the official agency records.
3) Establish applicant's identity by in-person proofing before the registration authority, based on the following process:
        i) The applicant presents the required credentials which are two identity source documents in original form. The 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).

ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and

iii) The credential presented in step 3) a) i) above shall be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid). Typically this is accomplished by querying a database maintained by the organization that issued the credential, but other equivalent methods may be used.

Practice note: This may be accomplished by querying a database maintained by the organization that issued the financial instrument or through use of a commercial credit database. In some instances, commercial credit card databases will validate name and address of current cardholders on-line; this validation is acceptable if the card is presented to the RA. Other methods may be accepted.

1) Record and maintain two biometrics of the applicant during the identity proofing and registration process These biometrics shall be formatted in accordance with [NIST SP 800-76] (see Appendix A):

   a) An electronic facial image used for printing facial image on the card, as well as for performing visual authentication during card usage. A new facial image shall be collected each time a card is issued; and

   b) Two electronic fingerprints to be stored on the card for automated authentication during card usage.

Additionally, the RA shall record the process that was followed for issuance of each certificate. The process documentation and authentication requirements shall include the following:

- 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 by the CPS using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury);
- Unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- The biometric of the applicant;
- The date and time of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury).

3.2.3.1.3 Derived Policies

Derived issuance will be dependent upon authentication of the individual requesting the derived policy OID through the use of a credential asserting a medium hardware or PIV-I hardware policy OID.

3.2.3.1.4 PIV-C Policies

Authentication procedures for subscribers issued under a PIV-C policy must include the steps listed below. Authentication by a trusted agent does not relieve the RA of its responsibility to perform steps 1), 2) and the verification of identifying information in step 3.

1) Verify that a request for certificate issuance to the applicant was submitted by an authorized agent of the sponsoring organization.
2) Verify sponsoring organization's employee's identity and employment through either of the following methods:
   a) A digital signature verified by a currently valid employee signature certificate issued by the CA may be accepted as proof of both employment and identity, or
   b) Employee's identity shall be established by in-person or video proofing before the registration authority or a trusted agent as in employee authentication above and employment validated through use of the official agency records.
3) Establish applicant's identity by in-person or video proofing before a Trusted Agent (TA), based on the following process:
   a) The applicant presents the required credentials which are two identity source documents in original form. The 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). If video proofing is to be used the applicant must send to the TA high quality photographs of both sides of all identity source documents and must present those documents during the video proofing session;
   b) The TA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and;
   c) The credential presented in step 3) a) above shall be verified by the TA for currency and legitimacy. Typically, this is accomplished by querying a database maintained by the organization that issued the credential, but other equivalent methods may be used.

Practice note: This may be accomplished by querying a database maintained by the organization that issued the financial instrument or through use of a commercial credit database. In some instances, commercial credit card databases will validate name and address of current cardholders on-line; this validation is acceptable if the card is presented to the RA. Other methods may be accepted but must be noted.

4) Optionally, record and maintain two biometrics of the applicant during the identity proofing and registration process These biometrics, if collected, shall be formatted in accordance with [NIST SP 800-76] (see Appendix A):
   a) An electronic facial image used for printing facial image on the card, as well as for performing visual authentication during card usage. A new facial image shall be collected each time a card is issued; and
   b) Two electronic fingerprints to be stored on the card for automated authentication during card usage.

Additionally, the RA shall record the process that was followed for issuance of each certificate. The process documentation and authentication requirements shall include the following:

- 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 by the CPS using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury);
- Unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- The biometric of the applicant;
- The date and time of the verification; and

A declaration of identity signed by the applicant using a handwritten signature and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury).

3.2.3.1.5 AATL Policies

Authentication procedures for subscribers issued under an AATL policy must include the steps listed below. Authentication by a trusted agent does not relieve the RA of its responsibility to perform steps 1), 2) and the verification of identifying information in step 3.

1) Verify that a request for certificate issuance to the applicant was submitted by an authorized agent of the sponsoring organization.
2) Verify sponsoring organization's employee's identity and employment through either of the following methods:
   a) A digital signature verified by a currently valid employee signature certificate issued by the CA may be accepted as proof of both employment and identity, or
   b) Employee's identity shall be established by in-person or video proofing before the registration authority or a trusted agent as in employee authentication above and employment validated through use of the official agency records.
3) Establish applicant's identity by in-person or video proofing before a Registration Authority RA) or Trusted Agent (TA), based on the following process:
   a) The applicant presents the required credentials which are two identity source documents in original form. The 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). If video proofing is to be used the applicant must send to the RA or TA high quality photographs of both sides of all identity source documents and must present those documents during the video proofing session;
   b) The RA or TA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and;
   c) The credential presented in step 3) a) above shall be verified by the RA or TA for currency and legitimacy. Typically, this is accomplished by querying a database maintained by the organization that issued the credential, but other equivalent methods may be used.

Practice note: This may be accomplished by querying a database maintained by the organization that issued the financial instrument or through use of a commercial credit database. In some instances, commercial credit card databases will validate name and

address of current cardholders on-line; this validation is acceptable if the card is presented to the RA or TA. Other methods may be accepted but must be noted.

4) Optionally, record and maintain two biometrics of the applicant during the identity proofing and registration process These biometrics, if collected, shall be formatted in accordance with [NIST SP 800-76] (see Appendix A):
   a) An electronic facial image used for printing facial image on the card, as well as for performing visual authentication during card usage. A new facial image shall be collected each time a card is issued; and
   b) Two electronic fingerprints to be stored on the card for automated authentication during card usage.

Additionally, the RA or TA shall record the process that was followed for issuance of each certificate. The process documentation and authentication requirements shall include the following:

- 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 by the CPS using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury);
- Unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- The biometric of the applicant;
- The date and time of the verification; and

A declaration of identity signed by the applicant using a handwritten signature and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury).

3.2.3.1.6 All Other Policies

With the exception of policies noted above, authentication procedures for employees or contractors must include the steps listed below. Authentication by a trusted agent does not relieve the RA of its responsibility to perform steps 1), 2), the verification of identifying information (e.g., by checking official records) in step 3), and the maintenance of biometrics in step 4), below.

1) Verify that a request for certificate issuance to the applicant was submitted by agency or organizational management.
2) Verify Applicant's employment through use of official records.
3) Establish applicant's identity by in-person or supervised remote identity proofing before the registration authority, based on either of the following processes:
   a) Process #1:
      i) The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and
      ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and

iii) The credential presented in step 3) a) i) above shall be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid). Typically, this is accomplished by querying a database maintained by the organization that issued the credential, but other equivalent methods may be used.

b) Process #2:

i) The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and

ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and

iii) The applicant presents current corroborating information (e.g., current credit card bill or recent utility bill) to the RA. The identifying information (e.g., name and address) on the credential presented in step 3) b) i) above shall be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid).

For contractors and other affiliated personnel, the authentication procedures must include the following steps:

1) Verify that a request for certificate issuance to the applicant was submitted by an authorized sponsoring agency employee (e.g., contracting officer or contracting officer's technical representative).

2) Verify sponsoring agency employee's identity and employment through either of the following methods:

a) A digital signature verified by a currently valid employee signature certificate issued by the CA may be accepted as proof of both employment and identity, or

b) Employee's identity shall be established by in-person or video proofing before the registration authority as in employee authentication above and employment validated through use of the official agency records.

3) Establish applicant's identity by in-person proofing before the registration authority, based on either of the following processes:

a) Process #1:

i) The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and

ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and

iii) The credential presented in step 3) a) i) above shall be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid). Typically this is accomplished by querying official records maintained by the organization that issued the credential.

b) Process #2:

i) The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and

ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and

iii) The applicant presents current corroborating information (e.g., current credit card bill or recent utility bill) to the RA. The identifying information (e.g., name and address) on the credential presented in step 3) b) i) above shall be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid).

Additionally, the RA shall record the process that was followed for issuance of each certificate. The process documentation and authentication requirements shall include the following:

- 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 by the CPS using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury);
- Unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- The biometric of the applicant, if captured;
- The date and time of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury).

FIPS 201 imposes the strict requirement of in-person registration. The following text only applies to the issuance of non-FIPS 201 credentials:

For all certificate policies where it is not possible for applicants to appear in person before the RA, a trusted agent may serve as proxy for the RA. The trusted agent forwards the information collected from the applicant directly to the RA in a secure manner. The requirement for recording a biometric of the applicant may be satisfied by providing passport-style photographs to the trusted agent. The trusted agent shall verify the photographs against the appearance of the applicant and the biometrics on the presented credentials and securely incorporate the biometric as a component in the notarized package. Packages secured in a tamper-evident manner by the trusted agent satisfy this requirement; other secure methods are also acceptable.

3.2.3.2 **Authentication of Devices**

Some computing and communications devices (routers, firewalls, servers, etc.) will be named as certificate subjects. In such cases, the device must have a human sponsor. The sponsor is responsible 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)
- Contact information to enable the CA or RA to communicate with the sponsor when required.

These certificates must be issued only to authorized devices under the subscribing organization’s control. In the case a human sponsor is changed, the new sponsor must review

the status of each device under his/her sponsorship to ensure it is still authorized to receive certificates. The CPS must describe procedures to ensure that certificate accountability is maintained. See Section 9.6.3 for Subscriber responsibilities.

Before issuing a certificate with a wildcard character (*) in a common name or subject alternative name of type dNSName, the CA must establish and follow a documented procedure to ensure that the wildcard does not fall immediately to the left of an agency or organization name, but is qualified down to a unique application, server, or server farm under control of the sponsor's organization. The device sponsor must demonstrate that the domain name requested is entirely within the namespace to be covered by the wildcard certificate.

The identity of the sponsor shall be authenticated by:

- Verification of digitally signed messages sent from the sponsor using a certificate issued under this policy; or
- In-person registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of section 3.2.3.1.

3.2.3.3 Authentication of Human Subscribers For Role-based Certificates

There is a subset of human subscribers who will 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 and are issued in the interest of supporting accepted business practices. The role-based certificate can be used in situations where non-repudiation is desired. Normally, it will be issued in addition to an individual subscriber certificate. A specific role may be identified in certificates issued to multiple subscribers, however, the key pair will be unique to each individual role-based certificate (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). Roles for which role-based certificates may be issued are limited to those that uniquely identify a specific individual within an organization (e.g., *Chief Information Officer* is a unique individual whereas *Program Analyst* is not). Role-based certificates shall not be shared, but shall be issued to individual subscribers and protected in the same manner as individual certificates.

The XTec Management Authority 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 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 pseudonymous certificates that identify subjects by their organizational roles, the CA shall validate that the individual either holds that role or has been delegated the authority to sign on behalf of the role.

Practice Note: When determining whether a role-based certificate is authorized, 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*".

3.2.3.4 Authentication of Human Subscribers For Group Certificates

Normally, a certificate shall be issued to a single Subscriber. For cases where there are several entities acting in one capacity, and where non-repudiation for transactions is not desired, a certificate MAY be issued that corresponds to a private key that is shared by multiple Subscribers. The XTec Management Authority, Entities and/or RAs shall record the information identified in Section 3.2.3.1 for a sponsor from the Information Systems Security Office or equivalent before issuing a group certificate.

In addition to the authentication of the sponsor, the following procedures shall be performed for members of the group:

- The Information Systems Security Office or equivalent shall be responsible for ensuring control of the private key, including maintaining a list of Subscribers who have access to use of the private key, and accounting for which Subscriber had control of the key at what time.
- The subjectName DN must not imply that the subject is a single individual, e.g. by inclusion of a human name form;
- The list of those holding the shared private key must be provided to, and retained by, the applicable CA or its designated representative; and
- The procedures for issuing tokens for use in shared key applications must comply with all other stipulations of this CP (e.g., key generation, private key protection, and Subscriber obligations).

3.2.4. Non-verified Subscriber Information

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

3.2.5. Validation of Authority

Before issuing CA certificates or signature certificates that assert organizational authority, the CA shall validate the individual's authority to act in the name of the organization. For pseudonymous certificates that identify subjects by their organizational roles, the CA shall validate that the individual either holds that role or has been delegated the authority to sign on behalf of the role.

In accordance with Section 3.2.3.2, all requests for device certificates in the name of an organization, must be digitally signed by the sponsor. In addition, the CPS must specify a process by which an organization identifies the individuals who may request certificates that assert organizational authority. If an organization specifies, in writing, the individuals who may request a certificate, then the CA must not accept any certificate requests that are outside this specification. The CA must provide an Applicant with a list of the organization's authorized certificate requestors upon the Applicant's verified written request.

Practice Note: Examples of signature certificates that assert organizational authority are code signing certificates and FIPS 201 id-XTec-nfissp-contentSigning certificates.

3.2.6. Criteria for Interoperation

The XTecPA shall determine the interoperability criteria for CAs operating under this policy. The MOA(s) with other entities, listed in Appendix B, ensure interaction and interoperability with other CAs, and authorized Federal, State and Local Government agencies.

3.3. Identification and Authentication for Re-key Requests

3.3.1. Identification and Authentication for Routine Re-key

CA certificate re-key shall follow the same procedures as initial certificate issuance. When a XTec PKI PKI CA updates its private signature key and thus generates a new public key and certificate, the XTec PKI PKI CA shall notify the XTecPA, RAs, and Subscribers, indicating that the CA's public certificate has been changed, in addition to publishing the certificate in the repository and making it publicly available.

A subscriber's identity may be established through use of current signature key, except that identity shall be re-established through an in-person registration process at least once every nine years from the time of initial registration.

Table 2: Re-Key Identity Requirements

Assurance Level	Routine Re-key Identity Requirements for Subscriber Signature, Authentication and Encryption Certificates
Medium (all policies)	Identity may be established through use of current signature key, except that identity shall be established through initial registration process at least once every nine years from the time of initial registration. For mediumDevice certificates, identity may be established through the use of current signature key or using means commensurate with the strength of the certificate being requested, except that identity shall be established through initial registration process at least once every nine years from the time of initial registration.
PIV-I Card Authentication	Identity may be established through use of the current signature key certificate, except that identity shall be established through initial registration process at least once every nine years from the time of initial registration.

Subscribers' signature private keys and certificates have a maximum lifetime of three years. Subscriber encryption certificates have a maximum lifetime of three years; use of subscriber decryption private keys is unrestricted.

For Device Subscribers, identity may be established through the use of the device's current signature key or the signature key of the device's human sponsor.

3.3.2. Identification and Authentication for Re-key after Revocation

In the event of certificate revocation, issuance of a new certificate shall always require that the party go through the initial registration process per section 3.2 above.

3.4. Identification and Authentication for Revocation Request

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

3.5. Identification and Authentication for Key Recovery Requests

This section addresses the requirements for authentication to a Key Recovery Authority. These requirements are not applicable for systems that implement automated implementation of key history for a subscriber during issuance of the subscriber's credential/

3.5.1. KRA Authentication

The KRA must authenticate to the KED or DDS directly or using a public key certificate issued by the associated PKI. The assurance level of the certificate must be the same as or greater than that of the certificate whose corresponding private key is being recovered and must meet the requirements of an RA credential.

3.5.2. KRO Authentication

The KRO must authenticate to the KRA using a public key certificate issued by the associated PKI. The assurance level of the certificate must be the same as or greater than that of the certificate whose corresponding private key is being recovered and must meet the requirements of an RA credential.

3.5.3. Subscriber Authentication

The Subscriber identity must 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 must be authenticated to the KED using a valid public key certificate. The assurance level of the Subscriber certificate must be equal to or greater than that of the certificate whose corresponding private key is being recovered.

3.5.4. Third-Party Requestor Authentication

This section addresses the requirements for authentication of a Third-Party Requestor, i.e., a Requestor other than the Subscriber themself.

Identity authentication must be commensurate with the assurance level of the certificate associated with the key being recovered. Identity must 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).

- Certificate-based authentication (e.g., digitally signed e-mail or client-authenticated 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).

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

3.5.5. Data Decryption Server Authentication

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

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

The Certificate application process must provide sufficient information to:

- Establish the applicant's authorization (by the employing or sponsoring agency) to obtain a certificate. (per section 3.2.3)
- Establish and record identity of the applicant. (per section 3.2.3)
- Obtain the applicant's public key and verify the applicant's possession of the private key for each certificate required. (per section 3.2.1)
- Verify any role or authorization information requested for inclusion in the certificate.

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

4.1.1. Who Can Submit a Certificate Application

4.1.1.1 CA Certificates

An application for a CA certificate shall be submitted by an authorized representative of the Applicant CA.

4.1.1.2 User Certificates

An application for a user (subscriber) certificate shall be submitted by either the Applicant or a trusted agent on behalf of the Applicant.

4.1.1.3 Device Certificates

An application for a device certificate shall be submitted by the human sponsor of the device.

4.1.2. Enrollment Process and Responsibilities

All communications among PKI Authorities supporting the certificate application and issuance process shall be authenticated and protected from modification; any electronic transmission of shared secrets shall be protected. Communications may be electronic or out-of-band. Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair shall be used. Out-of-band communications shall protect the confidentiality and integrity of the data.

Subscribers are responsible for providing accurate information on their certificate applications.

During the issuance of cross-certificates with an external CA, the XTec PKI CA shall manually check the external CA certificate to be cross-certified for accuracy prior to its delivery and publication.

4.2. Certificate Application Processing

Information in certificate applications shall be verified by the RA, or its delegate, as accurate before certificates are issued. Procedures to verify information in certificate applications shall be specified in the CPS.

4.2.1. Performing Identification and Authentication Functions

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

4.2.2. Approval or Rejection of Certificate Applications

For cross-certificates with an external CA, approval or rejection of certificate applications is at the discretion of the XTecPA or its designee.

For all other certificates, approval or rejection of certificate applications is at the discretion of the RA or its delegate.

4.2.3. Time to Process Certificate Applications

Certificate applications must be processed, and a certificate issued within 90 days of identity verification.

4.3. Certificate Issuance

4.3.1. CA Actions During Certificate Issuance

Upon receiving the request, the CAs/RAs will:

- Verify the identity of the requester.
- Verify the authority of the requester and the integrity of the information in the certificate request.
- Build and sign a certificate if all certificate requirements have been met (in the case of an RA, have the CA sign the certificate).
- Make the certificate available to the subscriber after confirming that the subscriber has formally acknowledged their obligations as described in section 9.6.3.

The certificate request may already contain a certificate built by either the RA or the subscriber. This certificate will not be signed until all verifications and modifications, if any, have been completed to the CA's satisfaction.

All authorization and other attribute information received from a prospective subscriber shall be verified before inclusion in a certificate. The responsibility for verifying prospective subscriber data shall be described in a CA's CPS.

4.3.2. Notification to Subscriber by the CA of Issuance of Certificate

CAs operating under this policy shall inform the subscriber (or other certificate subject) of the creation of a certificate and make the certificate available to the subscriber. For device certificates, the CA shall inform the human sponsor.

4.4. Certificate Acceptance

Before a subscriber can make effective use of its private key, a PKI Authority shall explain to the subscriber its responsibilities as defined in section 9.6.3.

4.4.1. Conduct Constituting Certificate Acceptance

Acceptance is the action taken by a subscriber that triggers the subscriber's duties and potential liability following the issuance of a certificate. It is the responsibility of the RA through the delivery process to:

- Explain to the subscriber their responsibilities;
- Inform the subscriber of the creation of a certificate and to the contents and purpose of the certificate; and
- Require the Subscriber to indicate acceptance of their responsibilities.

The certificate acceptance process is complete when the subscriber brings the certificate into their local certificate store for use.

4.4.2. Publication of the Certificate by the CA

As specified in 2.1, all CA certificates shall be published in repositories.

Certificates that contain the FASC-N and/or UUID in the subject alternative name extension, such as PIV-I Authentication Certificates, must not be distributed via public repositories (e.g., via LDAP or HTTP). This policy makes no other stipulation regarding publication of Subscriber certificates, except as noted in section 9.4.3.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

The XTec PKI Policy Authority must be notified whenever a CA operating under this policy issues a CA certificate.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

The intended scope of usage for a private key is specified through certificate extensions, including the key usage and extended key usage extensions, in the associated certificate.

4.5.2. Relying Party Public key and Certificate Usage

Certificates issued from CAs under this policy specify restrictions on use through critical certificate extensions, including the basic constraints and key usage extensions. All CAs operating under this policy shall issue CRLs specifying the current status of all unexpired certificates (except for OCSP responder certificates that include the id-pkix-ocsp-nocheck extension). It is recommended that relying parties process and comply with this information whenever using certificates in a transaction.

4.6. Certificate Renewal

Renewing a certificate means creating a new certificate with the same name, key, and other information as the old one, but with a new, extended validity period and a new serial number. The old certificate may or may not be revoked, but must not be used for requesting further re-key, renewal, or modification.

4.6.1. Circumstance for Certificate Renewal

Subscriber certificates issued under this policy shall not be renewed, except during recovery from CA key compromise (see 5.7.3). In such cases, the renewed certificate shall expire as specified in the original subscriber certificate. Additionally, a certificate shall be renewed only if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the Subscriber name and attributes are unchanged.

CA Certificates and OCSP responder certificates may be renewed so long as the aggregated lifetime of the public key does not exceed the certificate lifetime specified in section 6.3.2.

The CA may automatically renew certificates during recovery from key compromise.

4.6.2. Who May Request Renewal

For all CAs and OCSP responders operating under this policy, the corresponding operating authority may request renewal of its own certificate. For the Root CA, the XTecPA may also request renewal of CA certificates.

The CA shall determine if subscriber certificates are to be renewed during recovery from CA key compromise.

4.6.3. Processing Certificate Renewal Requests

For the Root CA, CA certificate renewal for reasons other than re-key shall be approved by the XTecPA.

In all cases, the certificate renewal identity-proofing shall be achieved using one of the following processes:

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

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 different public key (and serial number) while retaining the remaining contents of the old certificate that describe 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. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, modified or used for requesting such renewals, re-keys or modifications.

Subscribers shall identify themselves for the purpose of re-keying as required in section 3.3.2.

4.7.1. Circumstance for Certificate Re-key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a subscriber periodically obtain new keys. (Section 6.3.2 establishes usage periods for private keys for both CAs and subscribers.) Examples of circumstances requiring certificate re-key include: expiration, loss or compromise, issuance of a new hardware token, and hardware token failure.

4.7.2. Who May Request Certification of a New Public Key

Requests for certification of a new public key shall be considered as follows:

Subscribers with a currently valid certificate may request certification of a new public key. CAs and RAs may request certification of a new public key on behalf of a subscriber. For device certificates, the human sponsor of the device may request certification of a new public key.

The operating authority for a CA may request re-key of its own CA certificate.

4.7.3. Processing Certificate Re-keying Requests

If a subscriber has been identity proofed in accordance with Section 3.2 or 3.3 within the last 6 years then a digitally signed subscriber re-key requests shall be validated by validating the signature on that request before the electronic re-key is processed.

Alternatively, before processing certificate re-key requests, the XTec PKI PKI CA shall identify and authenticate the subscriber in accordance with Section 3.3., Identification & Authentication for Re-Key and Renewal.

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

All CA certificates must be published as specified in section 2.1.

See section 4.4.2.

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

See section 4.4.3.

4.8. Certificate Modification

Modifying a certificate means creating a new certificate that has the same or a different key and a different serial number, and that differs in one or more other fields from the old certificate. The

old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified or used for requesting such renewals, re-keys or modifications.

4.8.1. Circumstance for Certificate Modification

A CA operating under this policy may modify a CA or OCSP responder certificate whose characteristics have changed (e.g. assert new policy OID). The new certificate may have the same or a different subject public key.

A CA may perform certificate modification for a subscriber whose characteristics have changed (e.g., name change due to marriage). The new certificate shall have a different subject public key.

4.8.2. Who May Request Certificate Modification

Requests for certification of a new public key shall be considered as follows:

Subscribers with a currently valid certificate may request certificate modification. CAs and RAs may request certificate modification on behalf of a subscriber. For device certificates, the human sponsor of the device may request certificate modification.

4.8.3. Processing Certificate Modification Requests

If an individual's name changes (e.g., due to marriage), then proof of the name change must be provided to the RA or other designated agent in order for a certificate with the new name to be issued. If an individual's authorizations or privileges change, the RA will verify those authorizations. If authorizations have reduced, the old certificate must be revoked.

Proof of all subject information changes must be provided to the RA or other designated agent and verified in accordance with the initial identity-proofing process as described in Section 3.2 before the modified certificate is issued.

A certificate modification request identity-proofing shall be achieved using one of the following processes:

- Initial identity-proofing process as described in Section 3.2; or
- Identity-proofing for Re-key as described in Section 3.3.

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

All CA certificates must be published as specified in section 2.1.

See Section 4.4.2.

4.8.7. Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.9. Certificate Revocation and Suspension

CAs operating under this policy shall issue CRLs covering all unexpired certificates issued under this policy except for OCSP responder certificates that include the id-pkix-ocsp-nocheck extension.

CAs operating under this policy shall make public a description of how to obtain revocation information for the certificates they publish, and an explanation of the consequences of using dated revocation information. This information shall be given to subscribers during certificate request or issuance, and shall be readily available to any potential relying party.

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*.*

Certificate suspension for CA certificates is not allowed by this policy. However, the use of certificate suspension for end entity certificates is allowed.

For CAs operating under this policy, the XTecPA must be notified at least two weeks prior to the revocation of a CA certificate, whenever possible. For emergency revocation, CAs must follow the notification procedures in Section 5.7.

4.9.1. Circumstances for Revocation

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

- Identifying information or affiliation components of any names in the certificate becomes invalid.
- Privilege attributes asserted in the subscriber's certificate are reduced.
- The subscriber can be shown to have violated the stipulations of its subscriber agreement.
- There is reason to believe the private key has been compromised.
- Certification of the Subject is no longer in the interest of the CA.
- The subscriber or other authorized party (as defined in the CPS) asks for his/her certificate to be revoked.

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

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 actual or suspected compromise must be revoked or must be verified as appropriately issued.

4.9.2. Who Can Request Revocation

Within the PKI, a CA may summarily revoke certificates within its domain. A written notice and brief explanation for the revocation shall subsequently be provided to the subscriber. The RA

can request the revocation of a subscriber's certificate on behalf of any authorized party as specified in the CPS. A subscriber may request that its own certificate be revoked. Other authorized agency officials may request revocation of a subscriber certificate within its domain as described in the CPS.

The CA must provide Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for reporting suspected private key compromise, certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to certificates. The CA must publicly disclose the instructions through a readily accessible online means.

The XTecPA can request revocation of any CA certificate issued under this CP.

4.9.3. **Procedure for Revocation Request**

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). The CA or RA shall authenticate the request as well as the authorization of the requester per Section 4.9.2.

If an RA performs this function on behalf of the CA, the RA shall send a message to the CA requesting revocation of the certificate. The RA shall digitally or manually sign the message. The message shall be in a format known to the CA.

The steps involved in the process of requesting a certification revocation are detailed in the CPS.

Where subscribers use hardware tokens, they shall be required, prior to departure, to surrender to the RA or its delegate (through any accountable mechanism) all cryptographic hardware tokens that were issued to the Subscriber. For end entities with certificates asserting id-XTec-nfissp-medium-cardAuth or id-XTec-nfissp-pivi-hardware all certificates must be revoked in all cases. Certificate revocation is optional, for all other certificates, 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 RA, or its delegate;
- the token was zeroized or destroyed promptly upon surrender;
- the token has been protected from malicious use between surrender and zeroization or destruction.

In all other cases, revocation of the certificates is mandatory. If the hardware tokens cannot be obtained from the subscriber, then all subscribers' certificates associated with the un-retrieved tokens shall be immediately revoked, expressing reason code "key compromise." Even where all the above conditions have been met, revocation of the associated certificates is recommended.

For certificates issued under a PIV-I policy entity CAs (or delegate) shall whenever possible, collect and destroy PIV-I Cards from Subscribers whenever the cards are no longer valid. Entity CAs (or delegate) shall record the destruction of PIV-I Cards.

4.9.4. Revocation Request Grace Period

There is no grace period for revocation under this policy. Authorized parties, including subscribers, are required to request the revocation of a certificate immediately after the need for revocation comes to their attention.

4.9.5. Time within which CA must Process the Revocation Request

CAs will revoke certificates as quickly as practical upon receipt of a proper revocation request. Revocation requests shall be processed before the next CRL is published, excepting those requests received within two hours of CRL issuance. Revocation requests received within two hours of CRL issuance shall be processed before the following CRL is published, or within 24 hours.

The CA must maintain a continuous 24x7 ability to respond internally to high-priority problem reports, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a certificate that is the subject of such a complaint.

4.9.6. Revocation Checking Requirements for Relying Parties

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

Practice Note: Use of revoked certificates could have damaging or catastrophic consequences. The matter of how often new revocation data should be obtained 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

CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below.

Certificate status information shall be published not later than the next scheduled update. This will facilitate the local caching of certificate status information for off-line or remote (laptop) operation.

A self-signed Root CA, that only issues certificates to CAs and operates off-line, must issue CRLs at least once every 31 days, and the *nextUpdate* time in the CRL may be no later than 32 days after issuance time (i.e., the *thisUpdate* time).

CAs that issue certificates to subscribers or operate on-line must issue CRLs at least once every 18 hours, and the *nextUpdate* time in the CRL may be no later than 48 hours after issuance time (i.e., the *thisUpdate* time).

Circumstances related to emergency CRL issuance are specified in section 4.9.12.

Practice Note: Since many applications only check for a new CRL at nextUpdate, a longer nextUpdate time may result in applications continuing to rely on older CRLs even when a newer CRL is available. A longer nextUpdate time also increases the potential of a replay attack to validate a newly revoked certificate. Where the CRL nextUpdate exceeds 48 hours, relying parties should consider these risks and take appropriate measures to mitigate the risk. For high-risk, sensitive Relying Party applications suggested measures include configuring a preference

for OCSP by applications, pre-fetching CRLs at least every 18 hours, and use of other compensating controls.

4.9.8. Maximum Latency for CRLs

The maximum delay between the time that a subscriber's certificate is revoked by the CA and the time that this revocation information is available to Relying Parties shall be no greater than 24 hours. 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.

4.9.9. On-line Revocation/Status Checking Availability

CAs shall support on-line status checking via OCSP [RFC 6960] at the request of an agency for certificates issued within its domain. OCSP shall be provided for certificates asserting the id-XTec-nfissp-medium-cardAuth, id-XTec-nfissp-pivi-hardware, and id-XTec-nfissp-contentsigning OIDs.

Where on-line status checking is supported, status information must be updated and available to relying parties within 24 hours of certificate revocation.

Since some relying parties cannot accommodate on-line communications, all CAs will be required to support CRLs.

The CA must operate and maintain its CRL capability with resources sufficient to provide a response time of ten (10) seconds or less under normal operating conditions.

4.9.10. On-line Revocation Checking Requirements

The CA does not impose a mandatory requirement on relying party client software to support on-line status checking, however, an agency may make such a requirement mandatory through its own policies. Client software using on-line status checking need not obtain or process CRLs.

The timeliness of certificate status information supplied by the OCSP Responder shall be as specified in Section 4.9.8 of this CP. OCSP requests and responses shall comply with the profiles specified later in this CP.

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.
- The alternative method must meet the issuance and latency requirements for CRLs stated in sections 4.9.7 and 4.9.8.

4.9.12. Special Requirements Related To Key Compromise

In the event of a Root CA private key compromise or loss, the cross-certificate shall be revoked and a CRL shall be published within 18 hours of notification. The XTecPA will

also notify any organization that the XTecPA has a Memorandum of Agreement or Memorandum of Understanding with.

For Subordinate CAs, when a CA certificate is revoked or subscriber certificate is revoked because of compromise, or suspected compromise, of a private key, a CRL must be issued as specified below:

Policy Type	Maximum Latency for Emergency CRL Issuance
Basic	24 hours after notification
Medium (all policies) and PIV-I policies	18 hours after notification

4.9.13. Circumstances for Suspension

For CA certificates, suspension is not permitted.

CAs may support certificate suspension and restoration for Subscriber certificates. If suspension and restoration are supported by the CA, the CPS must describe under what circumstances and details for the corresponding sections below.

4.9.14. Who Can Request Suspension

For CAs that support suspension, those authorized to request suspension of a certificate must be identified.

4.9.15. Procedure for Suspension Request

For CAs that support suspension, all suspended certificate serial numbers must be populated on a full CRL within a timeframe specified in Section 4.9.7. The reason code CRL entry extension shall be populated with “certificateHold.”

For CAs that support suspension, a request to suspend a certificate must include:

- authentication of the requestor,
- identification of the certificate to be suspended, and
- explanation of the reason for suspension.

4.9.16. Limits on Suspension Period

For CAs that support suspension, the maximum time period a certificate may be suspended must be specified. The CPS must describe in detail how this maximum suspension period is enforced. If the subscriber has not removed the certificate from hold (suspension) within that period, the certificate must be revoked. Certificates must not be published on a CRL with a reason code of “certificateHold” beyond the expiration date of the certificate.

Practice Note: In order to mitigate the threat of unauthorized person removing the certificate from hold, the identity of the RA or authorized individual removing the suspension should be authenticated using a mechanism equivalent or higher than the assurance level of the certificate being unsuspended.

4.10. Certificate Status Services

See Section 4.9.9 for OCSP.

4.10.1. Operational Characteristics

Where an agency has made online certificate status checking mandatory upon relying parties, the relying parties shall be bound to their obligations and the stipulations of this CP irrespective of the operational characteristics of the certificate status service. Where applicable this shall be described in the corresponding CPS.

4.10.2. Service Availability

Where an agency has made online certificate status checking mandatory upon relying parties, the relying parties shall be bound to their obligations and the stipulations of this CP irrespective of the availability of the certificate status service. Where applicable this shall be described in the corresponding CPS.

4.10.3. Optional Features

Where applicable this shall be described in the corresponding CPS.

4.11. End Of Subscription

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

4.12. Key Escrow and Recovery

4.12.1. Key Escrow and Recovery Policy and Practices

CA private keys are never escrowed.

Subscriber key management keys may be escrowed to provide key history for use with a subscriber's physical token.

CAs that support private key escrow for key management keys other than for key history shall describe the practices in the applicable CPS or Key Recovery Practices Statement (KRPS). Escrowed keys shall be protected at no less than the level of security in which they are generated, delivered, and protected by the subscriber.

Unless held by an approved RSSP, a subscriber signature key may not be held in trust by a third party.

4.12.1.1 Key Escrow Processes and Responsibilities

Human subscriber private keys (i.e., decryption private keys) associated with a key management certificate must be securely escrowed by the KED. The CA must ensure that the keys are escrowed successfully prior to issuance of the key management certificates.

Subscriber private keys must be protected during transit and storage using cryptography at least as strong as 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 Processes 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 KRS. The Subscriber may submit the request to the KED, KRA or KRO. If the request is made electronically, the subscriber must 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 must be made in person, and 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 a trusted authentication or signature certificate, as determined by the recovering organization, with an assurance level equal to or greater than that of the escrowed key. Manual requests must include proper identity verification by the KRA in accordance with Section 3.2.3.1.

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

Third party key recovery in and of itself does not require revocation of a subscriber certificate. This does not prohibit Subscribers from revoking 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 is not required to notify subscribers of a third-party key recovery.

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
- 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.

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

4.12.1.2.3 Key Recovery During Token Issuance

When a Subscriber (individual and/or group/role sponsor or member) 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 as long as the KED uses secure means, such as Global Platform Secure Channel Protocol, to inject the key history onto the hardware token directly.

The hardware token must meet FIPS 140 Level 2 hardware requirements and the key must be injected into the token such that it is not thereafter exportable.

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;
- 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 another 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 DDSs. The DDSs must be designed to maximize the ability to enforce two-person control technically.

4.12.1.3 Who Can Submit a Key Recovery Application

Subscribers 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, as verified by the KRO, and by authorized external Third-Party Requestors (e.g., law enforcement personnel with a court order from a competent court).

4.12.1.4 Requestor Authorization Validation

The KRA or the KRO, as an intermediary for the KRA, must validate the authorization of the Requestor in consultation 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.

4.12.1.5 Subscriber Authorization Validation

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

4.12.1.6 KRA Authorization Validation

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

4.12.1.7 KRO Authorization Validation

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

4.12.1.8 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

CAs that support session key encapsulation and recovery must identify the document describing the practices in the applicable CPS.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. Physical Controls

CA, CMS, RSSP and CSS equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. The CA, CMS, RSSP and CSS shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. CA, CMS, RSSP and CSS cryptographic tokens shall be protected against theft, loss, and unauthorized use.

5.1.1. Site Location and Construction

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

5.1.2. Physical Access

5.1.2.1 Physical Access for CA Equipment

At a minimum, the physical access controls shall—

- Ensure that no unauthorized access to the hardware is permitted.
- Ensure that all removable media and paper containing sensitive plain-text information is stored in secure containers.
- Be manually or electronically monitored 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 system.

When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules, and CA equipment shall be placed in secure containers. Activation data shall be either memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module and shall not be stored with the cryptographic module.

A security check of the facility housing the CA equipment 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,” and for the CA, that all equipment other than the repository is in a mode appropriate to its required operational state).
- Any security containers are properly secured.
- Physical security systems (e.g., door locks, vent covers) are functioning properly.
- The area is secured against unauthorized access.

Notice of this requirement is to be clearly posted at the facility exit.

A person or group of persons shall be made explicitly responsible for making such checks. All personnel that have authorized access to the facility must sign a responsibility agreement that clearly states that these requirements will be met and that they will perform the security check at each exit of the facility. When a group of persons is responsible, a log identifying the person performing the check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall ensure that the checks are made. Failure to do so will result in remedial action.

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) must meet the CA physical access requirements specified in 5.1.2.1.

5.1.2.4 Physical Access for CMS Equipment

Physical access control requirements for CMS equipment must meet the CA physical access requirements specified in 5.1.2.1.

5.1.2.5 Physical Access for KED Equipment

Physical access control requirements for KED equipment that store private keys must meet the CA physical access requirements specified in 5.1.2.1.

5.1.2.6 Physical Access for DDS Equipment

Physical access control requirements for DDS equipment that store or use private keys must meet the CA physical access requirements specified in 5.1.2.1.

5.1.2.7 Physical Access for KRA and KRO Equipment

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

5.1.2.8 Physical Access for RSSP Equipment

Physical access control requirements for RSSP equipment must meet the CA physical access requirements specified in 5.1.2.1.

5.1.3. Power and Air Conditioning

The CA shall have backup capability sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown. The directories (containing CA certificates and CRLs) shall be provided with

uninterrupted power sufficient for a minimum of 6 hours operation in the absence of commercial power, to maintain availability and avoid denial of service.

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).

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

5.1.5. Fire Prevention and Protection

The CA must comply with local commercial building codes for fire prevention and protection.

5.1.6. Media Storage

Media shall be stored so as to protect them from accidental damage (e.g., water, fire, or 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

Full system backups sufficient to recover from system failure shall be made on a periodic schedule and described in a CA's CPS. Backups are to be performed and stored off-site not less than once per week. At least one full backup copy of all CA data shall be stored at an off-site location (separate from primary CA equipment). Only the latest full backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA.

Requirements for CA private key backup are specified in section 6.2.4.1.

5.2. Procedural Controls

5.2.1. Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible, or the integrity of the CA will be weakened. The functions performed in these roles form the basis of trust for the entire 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.

The primary trusted roles defined in this policy are Administrator, Officer, Auditor, and Operator. Individual personnel shall be specifically designated to the four roles defined below. These four roles are employed at the CA, RA, CMS, KED, DDS, and CSS locations as appropriate.

5.2.1.1 Administrator

The administrator role shall be responsible for:

- Installation, configuration, and maintenance of the CA, CMS, and CSS (where applicable);
- Establishing and maintaining CA, CMS, and CSS system accounts;
- Configuring certificate profiles or templates;
- Configuring CA, RA, and CSS audit parameters;
- Configuring CSS response profiles; and
- Generating and backing up CA, CMS, and CSS keys.

Administrators do not issue certificates to subscribers.

5.2.1.2 Officer

The officer role 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.

The Officer role encompasses RAs, and LRAs.

5.2.1.3 Auditor

The auditor role shall be responsible for:

- Reviewing, maintaining, and archiving audit logs; and
- Performing or overseeing internal compliance audits to ensure that the CA, associated RAs, and CSS (where applicable) are operating in accordance with its CPS.

5.2.1.4 Operator

The operator role shall be 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 RSSP Roles

The RSSP requires the following roles:

- The RSSP Administrator is responsible for:
    - Installation, configuration, and maintenance of the RSSP;
    - Establishing and maintaining any RSSP system accounts;
    - Configuring audit parameters, and;
    - Generating and backing up RSSP keys.
- The RSSP Audit Administrator is responsible for:
    - Reviewing, maintaining, and archiving RSSP audit logs; and

    - Performing or overseeing internal compliance audits to ensure that the RSSP is operating in accordance with its CPS.
- The RSSP Operator is responsible for
    - The routine operation of the RSSP equipment; and
    - Operations such as system backups and recovery.

5.2.1.6 Registration Authority (RA)

The RA responsibilities are:

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

5.2.1.7 Local Registration Authority (LRA)

The LRA 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 RA; and
- Receiving and distributing Subscriber certificates.

While the LRA performs functions similar to RA, an LRA generally is authorized to serve a limited population of Subscribers, based on logical or geographical organization.

5.2.1.8 CMS Roles

A CMS shall have at least the following roles which correspond to those listed in section 4.2.1 and are submitted to the same requirements:

- The CMS Administrators shall be responsible for:
    - Installation, configuration, and maintenance of the CMS;
    - Establishing and maintaining CMS system accounts;
    - Configuring CMS application and audit parameters; and
    - Generating and backing up CMS keys.
- The CMS Audit Administrators 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 the applicable CPSs.
- The CMS Operators shall be responsible for:
    - The routine operation of the CMS equipment; and

Operations such as system backups and recovery or changing recording media.

5.2.2. Number of Persons Required per Task

Two or more persons are required for the following tasks:

- CA, KED or DDS key generation;
- CA signing key activation;
- CA, KED or DDS private key backup.

Where multiparty control 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 shall not be achieved using personnel that serve in the Auditor trusted role.

5.2.3. Identification and Authentication for Each Role

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

5.2.4. Roles Requiring Separation of Duties

With respect to the CA, RSSP and CSS, individuals shall only assume one of the Officer, Administrator, and Auditor roles. Any individual, except one who has been assigned to the Auditor role, may assume the Operator role.

The CA, RSSP, RA and KRS software and hardware shall identify and authenticate its users and shall ensure that no user identity can assume both the Administrator and Officer roles, assume both the Administrator and Auditor roles, or assume both the Auditor and Officer roles.

No individual shall have more than one identity.

A Trusted Role may perform the same role on the CA, KED, and DDS.

Under no circumstances will a KRA or KRO be an Administrator or Auditor for a KED or DDS.

A Registration Authority (RA) may fill the role of a KRA or KRO.

A Trusted Agent (TA) may fill the role of a KRO.

5.3. Personnel Controls

5.3.1. Qualifications, Experience, and Clearance Requirements

Each Entity shall identify at least one individual or group responsible and accountable for the operation of each CA in that Entity.

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity. Each person filling a trusted role must 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 personnel only, in addition to the above, the person may be a citizen of the country where the RA is located.

For PKIs operated at policy levels of Medium Hardware-CBP and below, there is no citizenship requirement or security clearance specified.

5.3.2. Background Check Procedures

CA personnel shall, at a minimum, pass a background investigation covering the following areas:

- Employment;
- Education;
- Place of residence;
- Law Enforcement; and
- References.

The 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. Regardless of the date of award, the highest educational degree shall be verified.

Adjudication of the background investigation shall be performed by a competent adjudication authority using a process equivalent to Executive Order 12968 August 1995.

All cleared personnel must maintain their clearance per the requirements of the Defense Counterintelligence and Security Agency's requirement for periodic re-investigation.

5.3.3. Training Requirements

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

- CA (or RA) security principles and mechanisms;
- All PKI software versions in use on the CA (or RA) system;
- All RSSP and CSS software versions in use;
- Key Recovery System Principles and processes;
- All PKI duties they are expected to perform;
- Disaster recovery and business continuity procedures; and
- Stipulations of this policy and any associated practices statement.

5.3.4. Retraining Frequency and Requirements

All individuals responsible for PKI roles shall be made aware of changes in the CA 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 and Sequence

Job rotation must not violate role separation. All access rights associated with a previous role must be terminated.

All job rotations must be documented. Individuals assuming an auditor role must not audit their own work from a previous role.

5.3.6. Sanctions for Unauthorized Actions

The CA shall take appropriate and timely administrative and disciplinary actions against personnel who have performed actions involving the CA or its RAs that are not authorized in this CP, CPSs, or other published procedures.

5.3.7. Independent Contractor Requirements

Contractors fulfilling trusted roles are subject to all personnel requirements stipulated in this policy.

PKI vendors who provide any services shall establish procedures to ensure that any subcontractors perform in accordance with this policy and the CPS.

5.3.8. Documentation Supplied to Personnel

Documentation sufficient to define duties and procedures for each role shall be provided to the personnel filling that role.

5.4. Audit Logging Procedures

Audit log files shall be generated for all events relating to the security of the CA, CSS, RSSP and RA. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with section 5.5.2, *Retention Period for Archive*.

Audit record reviews should be performed using an automated process, and must include verification that the logs have not been tampered with, an inspection of log entries, and a root cause analysis for any alerts or irregularities. Implementation and documentation of automated tools must meet the requirements of the CP such that relevant events and anomalies are identified.

Reviews may be performed manually for physical or non-electronic records and logs, or when the audit log is small enough to allow for a thorough manual review.

All KED audit records of unsuccessful key recoveries must be analyzed to determine the cause and to ensure that the KRS is operating correctly and securely, and is not vulnerable to unauthorized use.

5.4.1. Types of Events Recorded

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

- The type of event;
- The date and time the event occurred;
- Where the event occurred (e.g., system or physical location)
- Source of the event;
- Outcome of the event to include a success or failure indicator;
- The identity of the entity and/or operator associated with the event.

A message from any source requesting an action by the CA, CSS, or RA is an auditable event; the corresponding audit record must also include message date and time, source, destination, and contents.

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

- SECURITY AUDIT:
  - Any changes to the Audit parameters, e.g., audit frequency, type of event audited
  - Any attempt to delete or modify the Audit logs
- IDENTIFICATION AND AUTHENTICATION:
  - Platform or CA application level authentication attempts
  - The value of maximum authentication attempts is changed
  - Maximum authentication attempts unsuccessful authentication attempts occur during user login
  - An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
  - An Administrator changes the type of authenticator, e.g., from password to biometrics
- DATA ENTRY AND OUTPUT:
  - Any additional event that is relevant to the security of the CA (such as remote or local data entry or data export); must be documented
- KEY GENERATION:
  - Whenever the CA, CSS, RSSP, RA and KRS generates a key. (Not mandatory for single session or one-time use symmetric keys)
- PRIVATE KEY LOAD AND STORAGE:

  - The loading of Component private keys or other keys used by the CA in the lifecycle management of certificates
  - All access to certificate subject private keys retained within the CA for key recovery purposes
- TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE:
  - All changes to the trusted public keys, including additions and deletions
- SECRET KEY STORAGE:
  - The manual entry of secret keys used for authentication
- PRIVATE AND SECRET KEY EXPORT:
  - The export of private and secret keys (keys used for a single session or message are excluded)
- 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
- CERTIFICATE REVOCATION:
  - All certificate revocation requests
- CERTIFICATE STATUS CHANGES:
  - All records including request authorization, approval and execution related to certificate status changes (e.g., revocation, suspension or restoration) whether generated directly on the CA or generated by a related external system or process
- CA, CSS, RSSP, RA and KRS CONFIGURATION:
  - Any security-relevant changes to the configuration of the CA, CSS, RSSP, RA and KRS
- ACCOUNT ADMINISTRATION:
  - Roles and users are added or deleted
  - The access control privileges of a user account or a role are modified
- CERTIFICATE PROFILE MANAGEMENT:
  - All changes to the certificate profile
- CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT:
  - All changes to the certificate revocation list profile
- MISCELLANEOUS:
  - Appointment or removal of an individual to a trusted role and who appointed or removed them from that role

  - Designation of personnel for multiparty control and who performed the designation
  - Installation of the operating system
  - Installation of the CA, CSS, RSSP, RA and KRS
  - Installing hardware cryptographic modules
  - Removing hardware cryptographic modules
  - Destruction of cryptographic modules
  - System startup
  - Logon attempts to CA, CSS, RSSP, RA and KRS applications
  - Receipt of hardware / software
  - Attempts to set passwords
  - Attempts to modify passwords
  - Backing up CA, CSS, RSSP, RA and KRS internal database
  - Restoring CA internal database
  - File manipulation of critical files (e.g., creation, renaming, moving)
  - Posting of any material to a repository
  - Access to CA internal database
  - All certificate compromise notification requests
  - Loading tokens with certificates
  - Shipment and receipt of tokens containing key material, or tokens that allow access to key material
  - Zeroizing tokens
  - Re-key of the CA
  - Configuration changes to the CA, CSS, RSSP, RA and KRS server involving:
    - Hardware
    - Software
    - Operating system
    - Patches
    - Security profiles
- PHYSICAL ACCESS / SITE SECURITY:
  - Personnel access to room housing CA, CSS, RSSP, RA and KRS
  - Access to the CA, CSS, RSSP, RA and KRS server
  - Known or suspected violations of physical security
- ANOMALIES:

- Software error conditions
- Software check integrity failures
- Receipt of improper messages
- Misrouted messages
- Network attacks (suspected or confirmed)
- Equipment failure
- Electrical power outages
- Uninterruptible power supply (UPS) failure
- Obvious and significant network service or access failures
- Violations of certificate policy
- Violations of certification practice statement
- Resetting operating system clock

5.4.2. Frequency of Processing Log

Review of the audit log shall be required at least every month.

Such reviews involve verifying that the log has not been tampered with and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. A statistically significant portion of the security audit data generated by the CA, CSS, RSSP, RA and KRS since the last review shall be examined. This amount will be described in the CPS.

All significant events shall be explained in an audit log summary. Actions taken as a result of these reviews shall be documented. This review summary must be retained as part of the long-term archive.

5.4.3. Retention Period for Audit Log

Audit logs must be accessible until reviewed in addition to being archived as described in section 5.5.

5.4.4. Protection of Audit Log

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

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.

CA, CSS, RSSP, RA and KRS system configuration and procedures must be implemented together to ensure that only authorized people archive or delete security audit data. Procedures must be implemented to protect archived data from deletion or destruction before the end of the security audit data retention period (note that deletion requires modification access).

Security audit data shall be maintained in a safe, secure storage location that ensures continuous availability and viability of the audit data.

5.4.5. Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up at least monthly to a site that is geographically separate from the source of the log data.

The process for backing up the audit records must 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, CSS, RSSP, RA and KRS system. Automated audit processes shall be invoked at system or application startup and cease only at system or application shutdown. Audit collection systems shall be configured such that security audit data is protected against loss (e.g., overwriting or overflow of automated log files). Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, operations shall be suspended until the problem has been remedied.

5.4.7. Notification to Event-Causing Subject

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

5.4.8. Vulnerability Assessments

The CA, CSS, RSSP, RA and KRS will perform routine self-assessments of security controls.

Self-assessment of controls and control effectiveness (e.g., FISMA) must be performed in accordance with the frequency determined by the risk rating of the CA.

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 the vulnerability assessment must be documented.

Practice Note: The security audit data should be reviewed by the security auditor for events such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. Security auditors should check for continuity of the security audit data.

5.5. Records Archival

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

CA, CSS, RSSP, RA and KRS archive records shall be sufficiently detailed to determine the proper operation of the CA, CSS, RSSP, RA and KRS.

At a minimum, the following data shall be recorded for archive, for each system, as applicable:

Data To Be Archived	All Policies
CA accreditation (if applicable)	X
Certificate Policy	X
Certification Practice Statement/Key Recovery Practices Statement	X
Contractual obligations	X
Other agreements concerning operations of the CA, CSS, RSSP, RA and KRS	X
System and equipment configuration	X
Modifications and updates to system or configuration	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
All records related to certificate status changes (e.g., revocation, suspension, or restoration) whether generated directly on the CA or generated as part of a related external system or process	X
The approval or rejection of a certificate status change request	X
Subscriber identity Authentication data as per Section 3.2.3	X
Documentation of receipt and acceptance of certificates	X
Subscriber Agreements	X
Documentation of receipt of tokens	X
All certificates issued or published	X
Record of re-key	X
All CRLs issued and/or published	X
Other data or applications to verify archive contents	X

Data To Be Archived	All Policies
Audit summary reports generated by internal reviews, documentation generated during third party audits and Compliance Auditor reports	X
Whenever a CA generates a key (not mandatory for one-time use symmetric keys or single session keys)	X
All access to certificate subject private keys retained within the CA for key recovery purposes	X
Changes to trusted public keys used or published by the CA including certificates used for trust between the CA and other components	X
The export of private and secret keys (keys used for a single session or message are excluded)	X
Record of an individual being added or removed from a trusted role, and who added or removed them from the role	X
Evidence of qualifications for Trusted Agents and the associated period(s) for which they are authorized to act as Trusted Agents	X
Destruction of cryptographic modules	X
All certificate compromise notifications	X
Remedial action taken as a result of violations of physical security	X
Violations of this Certificate Policy	X
Violations of Certification Practice Statement/Key Recovery Practices Statement	X
All Audit logs	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.

Archive records must be kept for a minimum of 10 years and 6 months, from date of creation, without any loss of data. If a record is related to record that is updated than the original record information must be kept for the same period beginning at the update of the record.

5.5.3. **Protection of Archive**

No unauthorized user shall be permitted to write to, modify, or delete the archive. Archived records may be moved to another medium. The contents of the archive shall not be released except in accordance with sections 9.3 and 9.4, or under circumstances described in the

approved CPS. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents.

Archive media shall be stored in a safe, secure storage facility such that is available and protected as indicated in 5.5.2.

If the original media cannot retain the data for the required period, or the associated hardware and applications to read the archives for the required period cannot be maintained, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site to ensure that the records may be refenced, as required, for the retention period.

5.5.4. Archive Backup Procedures

XTec PKI archives critical data. Archived information is stored in a GSA approved safe in a Top Secret cleared facility or, in the case of contractual obligations, may be stored in the XTec Legal department. Data, such as the CA database and audit logs are also maintained on the CA, CSS, RSSP, RA and KRS in the production facility and are transferred electronically to the XTec PKI Disaster Recovery facility. The archived information is not otherwise backed up.

5.5.5. Requirements for Time-Stamping of Records

CA, CSS, RSSP, RA and KRS archive records shall be automatically time-stamped as they are created. The CPS and KRPS shall describe how system clocks used for time-stamping 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 must be documented in the CPS/KRPS.

5.5.7. Procedures to Obtain and Verify Archive Information

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

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

5.6. Key Changeover

To minimize risk from compromise of a CA's private signing key, that key may be changed often. From that time on, only the new key will be used to sign CA and subscriber certificates. The older, but still valid, public key will be available to verify old signatures until all of the certificates signed using the associated private key have also expired. If the old private key is used to sign OCSP responder certificates or CRLs that cover certificates signed with that key, the old key must be retained and protected.

After all certificates signed with the old key have expired or been revoked, the CA may issue a final long-term CRL using the old key, with a nextUpdate time past the validity period of all issued certificates. This final CRL must 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.

The CA's signing key shall have a validity period as described in section 6.3.2.

When a CA updates its private signature key and thus generates a new public key, the CA shall notify all CAs, RAs, and subscribers that rely on the CA's certificate that it has been changed. When a CA that distributes self-signed certificates updates its private signature key, the CA may generate key rollover certificates, where the new public key is signed by the old private key, and vice versa. This permits validation of newly issued certificates and CRLs without distribution of the new self-signed certificate to current users. Key rollover certificates are optional for CAs that do not distribute self-signed certificates.

5.7. Compromise and Disaster Recovery

CAs under this policy must have an incident handling process, which documents any security incidents. Security incidents may include violation or threat of violation to the system, improper usage, malicious or anomalous activity and violations of the CPS or CP.

5.7.1. Incident and Compromise Handling Procedures

The XTec PKI Policy Authority (XTecPA) shall be notified if any CAs operating under this policy experience the following:

- suspected or detected compromise of the CA systems;
- suspected or detected compromise of a certificate status server (CSS) if (1) the CSS certificate has a lifetime of more than 72 hours and (2) the CSS certificate cannot be revoked (e.g., an OCSP responder certificate with the id-pkix-ocsp-nocheck extension);
- physical or electronic penetration of CA systems;
- successful denial of service attacks on CA components; or
- any incident preventing the CA from issuing a CRL within 48 hours of the issuance of the previous CRL.

The XTecPA will take appropriate steps to protect the integrity of the PKI.

The CA's PA shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the CA's CPS.

If the RSSP is compromised or suspected of being compromised, the incident must be investigated.All certificates associated with the subscriber private keys held in the RSSP must be revoked unlessa definitive determination is made that the RSSP is not compromised.

Once the incident has been resolved, the organization operating the CA or RSSP must provide notification directly to the XTecPA which includes detailed measures taken to remediate the incident. The notice must include the following:

- Which components were affected by the incident
- The CA or RRSP Operations Team's interpretation of the incident
- Who was/is impacted by the incident
- When the incident was discovered
- A complete list of all certificates that may have been issued erroneously, are not compliant with the CP/CPS or were misused as a result of the incident
- A signed statement that the incident has been fully remediated.

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

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

- 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 CRL issuance schedule specified in section 4.9.7.
- 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 organization operating the CA must provide notification to the XTecPA. See Section 5.7.1 for contents of the notice.

5.7.3. Entity Private Key Compromise Procedures

5.7.3.1 CA Private Key Compromise Procedures

In the event of a CA private key compromise, the following operations must be performed.

- The XTecPA shall be immediately informed, as well as any superior or cross-certified CAs and any entities known to be distributing the CA certificate (e.g., in a root store).
- The CA must generate new keys in accordance with section 6.1.1.1.

If the CA distributed the private key in a Trusted Certificate, the CA shall perform the following operations:

- Generate a new Trusted Certificate.
- Securely distribute the new Trusted Certificate as specified in section 6.1.4.
- Initiate procedures to notify subscribers of the compromise.

Subscriber certificates may be renewed automatically by the CA under the new key pair (see section 4.6), or the CA may require subscribers to repeat the initial certificate application process.

The XTec PKI Operational Authority shall also investigate and report to affected parties the cause of the compromise or loss, and what measures have been taken to preclude recurrence.

5.7.3.2 KRS Private Key Compromise Procedures

In the event that the KED or DDS is compromised or is suspected to be compromised, the following operations must be performed:

- Notify the XTecPA of the compromise
- Provide detail concerning the root cause, operational impact and initial remediation actions
- Determine the extent of the compromise
- Gain concurrence from the XTecPA 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, the following operations must be performed:

- Audit record review by the audit administrator to identify all potentially exposed escrowed keys
- Revocation of each of the certificates associated eith the potentially exposed escrowed keys, according to procedures specified in Section 4.9.3, to include Subscriber notification of the revocation
- Reissuance of the KRA or KRO authentication certificate

5.7.4. Business Continuity Capabilities after a Disaster

All CAs operating under this policy shall have recovery procedures in place to reconstitute the CA within 72 hours of failure.

In the case of a disaster whereby the CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, the XTecPA shall be notified at the earliest feasible time, and the XTecPA shall take whatever action it deems appropriate.

Relying parties may decide of their own volition whether to continue to use certificates signed with the destroyed private key pending reestablishment of CA operation with new certificates.

The directories containing certificates and certificate status information and the CSS shall be deployed so as to provide 24 hour per day/365 day per year availability.

5.8. CA or RA Termination

Whenever possible, a CA operator must provide notification of a CA termination to the XTecPA at least two weeks prior to the termination. For emergency termination, CAs must follow the notification procedures in Section 5.7.

When a CA operating under this policy terminates operations before all certificates have expired, the CA signing keys shall be surrendered to the XTec PKI Policy Authority. Prior to CA or KRS termination, the CA or KRS shall provide archived data to an archive facility as specified in the CPS. As soon as possible, the CA or KRS will advise all other organizations to which it has issued certificates of its termination, using an agreed-upon method of communication specified in the CPS.

Practice Note: This section does not apply to CAs that have ceased issuing new certificates but are continuing to issue CRLs until all certificates have expired. Such CAs are required to continue to conform with all relevant aspects of this policy (e.g., audit logging and archives).

Any issued certificates that have not expired, must be revoked and a final long term CRL with a nextUpdate time past the validity period of all issued certificates must be generated. This final CRL must 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 CA to be terminated will be destroyed or taken offline, designated as "not in use", and protected as stipulated in Section 5.1.2.1.

For RA termination, the RA certificate shall be revoked, RA Private keys destroyed, and the RA shall provide archived data to the archival facility approved by the XTecPA.

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

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

6.1.1.1 CA Key Pair Generation

Cryptographic keying material used by CAs to sign certificates, CRLs or status information shall be generated in FIPS 140 validated cryptographic modules. The module(s) must meet or exceed the requirements stipulated in section 6.2.1. Multiparty control is required for CA key pair generation, as specified in section 6.2.2.

CA, CMS, RSSP and CSS key pair generation must create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure must be detailed enough to show that appropriate role separation was used. An independent third party shall validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation.

Practice Note: If the audit trail identifies and documents any failures or anomalies in the key generation process, along with the corrective action taken, the key generation process need not be restarted but may continue.

6.1.1.2 Subscriber Key Pair Generation

Subscriber key pair generation may be performed by the subscriber, CA, or RA. If the CA or RA generates subscriber key pairs, the requirements for key pair delivery specified in Section 6.1.2 must also be met.

Key generation shall be performed using a FIPS 140 validated cryptographic module. The module(s) must meet or exceed the requirements stipulated in section 6.2.1.

For PIV-I, all keys, with the exception of key management, must be generated on the card.

6.1.1.3 CSS Key Pair Generation

Cryptographic keying material used by CSSs to sign status information shall be generated in FIPS 140 validated cryptographic modules. The module(s) must meet or exceed the requirements stipulated in section 6.2.1.

6.1.1.4 PIV-I Content Signing Key Pair Generation

Cryptographic keying material used by PIV-I issuing systems or devices for PIV-I Content Signing must be generated in [FIPS 140] validated cryptographic modules as specified in Section 6.2.1.

6.1.1.5 RSSP Key Pair Generation

Cryptographic keying material used by RSSPs shall be generated in FIPS 140 validated cryptographic modules. The module(s) must meet or exceed the requirements stipulated in section 6.2.1.

6.1.1.6 RA Key Pair Generation

Cryptographic keying material for RA keys shall be generated in FIPS 140 validated cryptographic modules. The module(s) must meet or exceed the requirements stipulated in section 6.2.1.

6.1.2. Private Key Delivery to Subscriber

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

When CAs or RAs generate keys on behalf of the subscriber, then the private key must be delivered securely to the subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases, the following requirements 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(s) must be protected from activation, compromise, or modification during the delivery process.
- The subscriber shall acknowledge receipt of the private key(s).
- Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct subscribers.
    - For hardware modules, accountability for the location and state of the module 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.

The CA must maintain a record of the subscriber acknowledgment of receipt of the token.

6.1.3. Public Key Delivery to Certificate Issuer

Where key pairs are generated by the subscriber or RA, the public key and the subscriber's identity 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 CA keys used to sign the certificate.

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 cross-certificates.

Self-signed certificates shall be conveyed to relying parties in a secure fashion to preclude substitution attacks. Acceptable methods for self-signed certificate delivery are:

- Loading a self-signed certificate onto tokens delivered to relying parties via secure mechanisms, such as:
    - The Trusted Certificate is loaded onto the token during the subscriber's appearance at the RA.
    - The Trusted Certificate is loaded onto the token when the RA generates the subscriber's key pair and loads the private key onto the token, which is then delivered to the subscriber in accordance with section 6.1.2.
- 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.

Practice Note: Other methods that preclude substitution attacks may be considered acceptable.

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 must be distributed using directories and other repositories.

6.1.5. **Key Sizes**

All FIPS-approved signature algorithms shall be considered acceptable; additional restrictions on key sizes are detailed below.

This CP requires use of RSA PKCS #1, RSASSA-PSS.

For CAs that distribute self-signed certificates to relying parties, the CA's subject public keys in such certificates shall be at least 2048 bits for RSA.

CAs that generate certificates and CRLs under this policy shall use signature keys of at least 2048 bits for RSA, if they expire prior to 12/31/2030. For CA certificates that expire beyond 12/31/2030 the CA certificates and CRLs shall use signature keys of at least 3072 bits for RSA.

CAs that generate certificates and CRLs under this policy shall use SHA-256, SHA-384, or SHA-512 hash algorithm when generating digital signatures.

Where implemented, CSSs shall sign responses using the same signature algorithm, key size, and hash algorithm used by the CA to sign CRLs.

End-entity certificates shall contain public keys that are at least 2048 bit for RSA, DSA, or Diffie-Hellman, or 256 bits for elliptic curve algorithms. The following special conditions also apply:

- End-entity certificates issued for PIV-I, those that assert id-XTec-nfissp-medium-cardAuth, id-XTec-nfissp-pivi-hardware or id-XTec-nfissp-contentsigning, shall contain public keys and algorithms that conform to [NIST SP 800-78].

CAs operating under this policy must meet the following conditions:

- Certificates are signed with keys of at least 2048 bits for RSA.
- End-entity certificates that include a keyUsage extension that asserts the *nonRepudiation*, *keyEncipherment*, *dataEncipherment*, or *keyAgreement* bit contain public keys that are at least 2048 bits for RSA, DSA, or Diffie-Hellman, or 256 bits for elliptic curve algorithms.
- End-entity certificates that do not include a keyUsage extension contain public keys that are at least 2048 bits for RSA, DSA, or Diffie-Hellman, or 256 bits for elliptic curve algorithms.

Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum AES (128 bits) or equivalent for the symmetric key, and at least 2048 bit RSA or equivalent for the asymmetric keys.

6.1.6. Public Key Parameters Generation and Quality Checking

Public key parameters for signature algorithms defined in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186. For RSA, the CA shall perform partial public key validation as specified in NIST SP 800-89 (Section 5.3.3).

Parameter quality checking (including primality testing for prime numbers) shall be performed in accordance with FIPS 186.

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

The use of a specific key is constrained by the key usage extension in the X.509 certificate. All certificates shall include a critical key usage extension.

Public keys that are bound into subscriber user certificates shall be used only for signing or encrypting, but not both, therefore certificates that have the nonrepudiation bit set shall not have the keyEncipherment bit set. User certificates to be used for authentication shall assert only the *digitalSignature* bit. Other user certificates to be used for digital signatures shall assert both the *digitalSignature* and *nonRepudiation* bits. User certificates that contain RSA public keys that are to be used for key transport shall assert the *keyEncipherment* bit.

Public keys that are bound into CA certificates shall be used only for signing certificates and status information (e.g., CRLs). CA certificates whose subject public key is to be used to verify other certificates shall assert the *keyCertSign* bit. CA certificates whose subject public key is to be used to verify CRLs shall assert the *cRLSign* bit. CA certificates whose subject public key is to be used to verify Online Certificate Status Protocol (OCSP) responses shall assert the *digitalSignature* and/or *nonRepudiation* bits.

Public keys that are bound into device certificates may be used for digital signature (including authentication), key management, or both. Device certificates to be used for digital signatures shall assert the *digitalSignature* bit. Device certificates that contain RSA public keys that are to be used for key transport shall assert the *keyEncipherment* bit. Device certificates to be used for both digital signatures and key management shall assert the *digitalSignature* bit and either the *keyEncipherment* (for RSA). Device certificates shall not assert the *nonRepudiation* bit.

For all Subscriber certificates, Extended Key Usage OIDs shall be consistent with key usage bits asserted. The Extended Key Usage extension must not contain anyExtendedKeyUsage {2.5.29.37.0} or id-kpcodeSigning {1.3.6.1.5.5.7.3.3}.

Public keys that are bound into device certificates that are issued under id-XTec-nfissp-contentsigning shall include a critical extended key usage of *id-fpki-pivi-content-signing.*

The *dataEncipherment*, *encipherOnly*, and *decipherOnly* bits shall not be asserted in certificates issued under this policy.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is *Security Requirements for Cryptographic Modules* [FIPS 140-2]. Cryptographic modules shall be validated to a FIPS 140 level identified in this section.

The table, following, summarizes the minimum requirements for cryptographic modules; higher levels may be used.

Policy Type	CA, RSSP, CSS, KED and DDS	Subscriber	RA
Basic	Level 3 (Hardware)	Level 1 (HW or SW) See Note 1	Level 1 (HW or SW) See Note 2
Medium Software	Level 3 (Hardware)	Level 1 (HW or SW) See Note 1	Level 2 (HW)
Medium Hardware and PIV-I	Level 3 (Hardware)	Level 2 (HW)	Level 2 (HW)

NOTE: Certificates issued under id-XTec-nfissp-contentsigning or id-XTec-PIVC-contentSigning will only be issued to devices that meet a minimum requirement of current FIPS 140 level 2 (or higher).

PIV-I cards must only be issued using card stock that has been tested and approved by the FIPS 201 Evaluation Program and listed on the GSA Approved Products List (APL). 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 XTecPA.

Any pseudo-random numbers used for key generation material must be generated using a FIPS-validated cryptographic module.

6.2.1.1 Remote Signing Service Provider Key Stores

Remote Signing Service Provider (RSSP) Key Stores hold keys for a number of Subscriber certificates in one location. When a collection of private keys for Subscriber certificates are held in a single location, there is a higher risk associated with compromise of that cryptographic module than that of a single Subscriber; therefore, RSSP Key Stores must utilize a minimum FIPS 140 Level 3 or equivalent cryptographic module for key storage.

The RSSP must be deployed to provide 24 hour per day/365 day per year availability. RSSP providers should implement features to provide high levels of RSSP reliability (99% availability or better).

Authentication to the RSSP to activate the private key associated with a given certificate requires multi-factor authentication commensurate with the assurance level of the certificate.

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

A single person shall not be permitted to activate or access any cryptographic module that contains the complete CA private signing key. CA signature keys may be backed up only under two-person control. Access to CA signing keys backed up for disaster recovery shall be under at least two-person control. The names of the parties used for two-person control shall be maintained on a list that shall be made available for inspection during compliance audits.

6.2.3. Private Key Escrow

CA private keys shall not be escrowed.

Under no circumstances shall a third party escrow any Signing Keys used to support non-repudiation services. Subscriber private dual-use keys shall not be escrowed.

Subscriber key management keys may be escrowed to provide key recovery as described in section 4.12.1.

6.2.4. Private Key Backup

6.2.4.1 Backup of CA Private Signature Key

The CA private signature keys shall be backed up under the same multi-person control as the original signature key. At least one copy of the private signature key shall be stored off-site. All copies of the CA private signature key shall be accounted for and protected in the same manner as the original. Backup procedures shall be included in the CA's CPS.

6.2.4.2 Backup of Subscriber Private Signature Key

Subscriber and RA private signature keys whose corresponding public key is contained in a certificate asserting a medium hardware or FIPS 201 PIV policy shall not be backed up or copied.

Subscriber private signature keys whose corresponding public key is contained in a certificate asserting a basic or medium software policy 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 plaintext form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module.

Subscriber private keys held in a RSSP may be backed up to a device providing comparable protection levels and approved for RSSP use. The RSSP backup must be performed under two-person control.

6.2.4.3 Backup of Subscriber Private Key Management Key

Backed up subscriber private key management keys shall not be stored in plaintext 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 Content Signing Private Key

The private keys associated with the public certificate issued under id-XTec-nfissp-contentsigning or id-XTec-PIVC-contentSigning may be backed up. If backed up, all copies shall be accounted for and protected in the same manner as the original.

6.2.4.6 Backup of RSSP Private Keys

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

6.2.5. Private Key Archival

CA private signature keys and subscriber private signatures keys shall not be archived. CAs that retain subscriber private encryption keys for business continuity purposes shall archive such subscriber private keys, in accordance with section 5.5.

6.2.6. Private Key Transfer into or from a Cryptographic Module

CA private keys may be exported from the cryptographic module only to perform CA key backup procedures as described in section 6.2.4.1. At no time shall the CA private key exist in plaintext outside the cryptographic module.

All other keys shall be generated by and in a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport; private keys must never exist in plaintext form outside the cryptographic module boundary.

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

6.2.7. Private Key Storage on Cryptographic Module

No stipulation beyond that specified in FIPS 140.

6.2.8. Method of Activating Private Key

Cryptographic modules shall be protected from unauthorized access.

For certificates issued under all policies except id-XTec-nfissp-pivi-cardAuth, id-XTec-nfissp-medium-cardAuth and id-XTec-PIVC-cardAuth, the subscriber must be authenticated to the cryptographic token before the activation of the associated private key(s). Acceptable means of authentication include but are not limited to passphrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered). Activation of private keys stored on an RSSP requires multi-factor authentication.

For certificates issued under id-XTec-nfissp-contentsigning or id-XTec-PIVC-contentSigning, key activation requires the same multiparty control as described in 6.2.2.

Activation requirements for all policies are described in the table below.

Policy Asserted	Activation Requirements
id-XTec-nfissp-basic-policy id-XTec-PIVC-basic	Passphrases or PINs. When passphrases are used, they must be a minimum of twelve (12) alphanumeric characters. When PINs are used, they must be a minimum of six (6) characters. Entry of activation data must be protected from disclosure (i.e., the data should not be displayed while it is entered).
id-XTec-nfissp-mediumDevice id-XTec-nfissp-mediumDeviceHardware id-XTec-PIVC-mediumDevice Id-XTec-ops-mediumDevice id-XTec-ops- mediumDeviceHardware	May be configured to activate the private key without requiring a human sponsor or authorized administrator to authenticate to the cryptographic token. The appropriate physical and logical access controls must be implemented for the device and its cryptographic token
id-XTec-nfissp-medium id-XTec-nfissp-mediumHardware id-XTec-nfissp-medium-authentication id-XTec-nfissp-pivi-hardware id-XTec-nfissp-medium-derived id-XTec-nfissp-medium-derivedHW id-XTec-AATL-HardwareMFA id-XTec-AATL-HardwareToken id-XTec-PIVC-medium id-XTec-PIVC-mediumHardware id-XTec-PIVC-mediumAuthentication id-XTec-PIVC-medium-derived id-XTec-PIVC-medium-derivedHardware id-XTec-ops-mediumHardware id-XTec-ops-mediumHardwareAuth	Passphrases, PINs or biometrics. When passphrases are used, they must be a minimum of twelve (12) alphanumeric characters. When PINs are used, they must be a minimum of six (6) characters. Entry of activation data must be protected from disclosure (i.e., the data should not be displayed while it is entered).
id-XTec-nfissp-pivi-cardAuth id-XTec-nfissp-medium-cardAuth id-XTec-PIVC-cardAuth	No activation required.

Policy Asserted	Activation Requirements
id-XTec-nfissp-contentsigning id-XTec-PIVC-contentSigning	May be configured to activate the private key without requiring a human sponsor or authorized administrator to authenticate to the cryptographic token. The appropriate physical and logical access controls must be implemented for content signing operations conformant with PIV issuance requirements (see [FIPS 201]). The strength of the security controls must be commensurate with the level of threat in the PIV credential issuance system's environment, and must protect the hardware, software, and the cryptographic token and its activation data from compromise.

6.2.9. Method of Deactivating Private Key

Cryptographic modules that have been activated shall not be available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure or automatically after a period of inactivity as defined in the applicable CPS. CA cryptographic modules shall be physically secured, as described in Section 5.1, when not in use.

6.2.10. Method of Destroying Private Key

Individuals in trusted roles shall destroy CA, RA, RSSP and CSS private signature keys and activation data (e.g. operator card set or tokens) when they are no longer needed. Subscribers shall either surrender their cryptographic module to CA/RA personnel for destruction or destroy their private signature keys, when they are no longer needed or when the certificates to which they correspond expire or are revoked. Physical destruction of hardware is not required.

To ensure future access to encrypted data, subscriber private key management keys should be secured in long-term backups or archived.

Practice Note: Destruction must be performed by executing a "zeroize" command or through physical destruction of the token.

6.2.11. Cryptographic Module Rating

See section 6.2.1.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

The public key is archived as part of the certificate archival, per section 5.5.

6.3.2. Certificate Operational Periods and Key Usage Periods

The usage period for the XTec PKI Root CA key pair is a maximum of 20 years.

For all other CAs operating under this policy, the usage period for a CA key pair is a maximum of ten years. The CA private key may be used to sign CRLs and OCSP responder certificates for the entire usage period. All certificates signed by a specific CA private key must expire before the end of that key pair's usage period.

Subscriber public keys in certificates that assert the id-PIV-content-signing OID in the extended key usage extension have a maximum usage period of eight years. The private keys corresponding to the public keys in these certificates have a maximum usage period of two years.

Subscriber public keys in certificates that assert id-XTec-nfissp-mediumHardware, id-XTec-PIVC-mediumHardware, id-XTec-nfissp-pivi-hardware, id-XTec-PIVC-cardAuth or id-XTec-nfissp-medium-cardAuth OID shall have a certificate expiration that is the lesser of 3 years or a period that does not exceed the date of expiration of the token on which the certificates reside.

For OCSP responders, all other subscriber public keys, including RA, DDS, KRA and KRO public keys, the maximum usage period is three years except for OCSP responders that service PIV-I subscribers, in which case the maximum certificate lifetime for the OCSP responder is 120 days. Subscriber signature private keys have the same usage period as their corresponding public key. The usage period for subscriber key management private keys is not restricted.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

The activation data used to unlock Entity CA or subscriber private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected.

If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

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

The strength of the activation data must meet or exceed the requirements for authentication mechanisms stipulated for Level 2 in FIPS 140-2.

Subscriber activation data presented to an RSSP to access subscriber keys must be changed, at a minimum, whenever the private key is changed.

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 mechanism shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the respective CP or CPS.

Subscriber activation data presented to an RSSP in order to access subscriber keys must be protected from disclosure to unauthorized parties, from eavesdropping, and from replay.

6.4.3. Other Aspects of Activation Data

For PIV-I, in the event that activation data must be reset, a successful biometric 1:1 match of the applicant against the biometric collected in Section 3.2.3.1 is required. This biometric 1:1 match must be conducted by a trusted agent of the issuer.

Any additional aspects of activation data that are in use by a CA operating under this policy must be defined within the CA's CPS.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

Computer security controls are required to ensure CA, CSS, RSSP, RA and KRS operations are performed as specified in this policy. The following computer security functions pertaining to the CA, CSS, KEDs, DDSs and RA may be provided by the operating system, or through a combination of operating system, software, and physical safeguards, at all system software layers, as applicable**:**

- Require authenticated logins prior to permitting access;
- Provide discretionary access control;
- Provide a security audit capability, to meet the requirements of Section 5.4;
- Enforce access control for application services and PKI and PKI related roles;
- Enforce separation of duties for PKI and PKI related roles;
- Require identification and authentication of PKI and PKI related roles and associated identities;
- Prohibit object reuse or require separation for application random access memory;
- Require use of cryptography for session communication and database security;
- Archive application history and audit data;
- Require self-test for all security-related application services;
- Provide residual information protection;
- Require a trusted path for identification of PKI and PKI related roles and associated identities;
- Require a recovery mechanism for keys and the application systems, and
- Enforce domain integrity boundaries for security-critical processes.

All communications between any PKI Trusted Role and the CA shall be authenticated and protected from modification.

6.5.2. Computer Security Rating

CAs operating under this policy shall identify any Computer Security Rating requirements in the applicable CPS.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

The system development controls for the CA, CSS, RSSP, RA and KRS are as follows:

- The CA shall use software that has been designed and developed under a formal, documented development methodology.
- Hardware and software shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the vendor cannot identify the PKI component that will be installed on a particular device).
- All hardware and software shall be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location.
- Hardware and software developed specifically for the CA or CSS shall be developed in a controlled environment, and the development process shall be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.
- The CA hardware and software shall be dedicated to performing one task: the CA. There shall be no other applications, hardware devices, network connections, or component software installed that are not parts of the CA operation. Where the CA operation supports multiple CAs, the hardware platform may support multiple CAs.
- Proper care shall be taken to prevent malicious software from being loaded onto the CA, CMS, RSSP and CSS equipment. All applications required to perform the operation of the CA or CSS shall be obtained from documented sources. CA, CSS and RA hardware and software shall be scanned for malicious code on first use and periodically thereafter.
- Hardware and software updates shall be purchased or developed in the same manner as original equipment and shall be installed by trusted and trained personnel in a defined manner.

6.6.2. Security Management Controls

The configuration of the CA system, in addition to any modifications and upgrades, shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the software or configuration. The CA, CMS, RSSP and CSS software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use. The CA shall verify the integrity of the software on at least a weekly basis following the processes specified in the CPS.

6.6.3. Life Cycle Security Controls

CAs operating under this policy shall identify any Life Cycle Security Control requirements in the applicable CPS.

6.7. Network Security Controls

This section does NOT apply to CAs that operate in off-line mode only.

A network guard, firewall, or filtering router must protect network access to CA and KRS equipment. The network guard, firewall, or filtering router shall limit services allowed to and from the CA and KRS equipment to those required to perform CA and KRS functions.

Protection of CA and KRS equipment shall be provided against known network attacks. All unused network ports and services shall be turned off. Any network software present on the CA and KRS equipment shall be necessary to the functioning of the CA or KRS application.

The applicable CPS shall define the network protocols and mechanisms required for the operation of the PKI. 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.

Directories/repositories, certificate status servers, KRA/KRO, any device that asserts the id-XTec-nfissp-contentsigning or id-XTec-PIVC-contentSigning OID and remote workstations used to administer the CA or KRS, shall employ appropriate network security controls. Networking equipment shall turn off unused network ports and services. Any network software present shall be necessary to the functioning of the equipment.

The remote workstation used to administer the CA must use a 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 Trusted Role at a level of assurance commensurate with that of the CA.

6.8. Time-Stamping

The system clock time for all CA, CMS, RSSP, KRS and CSS components shall be derived, and periodically corrected, from a trusted third party time service. Time derived from the trusted time service shall be used for establishing the time of:

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

Asserted times shall be accurate to within three minutes. Clock adjustments are auditable events (see section 5.4.1).

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate Profile

Certificates issued by a CA under this policy shall conform to the X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards [FPKI-PIVI-PROF]. Where certificate types are not defined within [FPKI-PIVI-PROF] the rules defined in [FBCA-PROF] will be enforced, except in terms of naming which, at all times, will comply with Section 3 of this Certificate Policy.

7.1.1. Version Number(s)

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

7.1.2. Certificate Extensions

Rules for the inclusion, assignment of value, and processing of extensions are defined in [FBCA-PROF]. For CAs that issue certificates that assert PIV-I OIDs the inclusion, assignment of value, and processing of extensions are defined in [FBCA-PROF]. Where certificate types are not defined within [FBCA-PROF] the rules defined in [CCP-PROF] will be enforced, except in terms of naming which, at all times, will comply with Section 3 of this Certificate Policy.

For all CAs, use of standard certificate extensions shall comply with [RFC 5280].

CA certificates issued by the XTec PKI shall not include critical private extensions. Subscriber certificates issued by the XTec PKI may include critical private extensions so long as interoperability within the community of use is not impaired.

7.1.2.1 Basic Constraints for CA Certificates

CA certificates shall assert a `basicConstraints` extension with `cA = TRUE`.

7.1.3. Algorithm Object Identifiers

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

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}
sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13}
RSA with PSS padding	id-RSASSA-PSS ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10}

The PSS padding scheme OID is independent of the hash algorithm; the hash algorithm is specified as a parameter (for details, see [PKCS#1]). Certificates issued under this CP must use the SHA-256 hash algorithm when generating RSASSA-PSS signatures. The following OID shall be used to specify the hash in an RSASSA-PSS digital signature:

SHA-256	id-sha256 ::= {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1}

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

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

7.1.4. Name Forms

The subject field in certificates issued under the policies in this document shall be populated with an X.500 distinguished name as specified in section 3.1.1.

The issuer field of certificates issued under the policies in this document shall be populated with a non-empty X.500 Distinguished Name as specified in section 3.1.1.

7.1.5. Name Constraints

The CAs may assert name constraints in CA certificates.

7.1.6. Certificate Policy Object Identifier

Certificates issued under this CP shall assert at least one of the OIDs from Section 1.2, Table 1: Certificate Policy Identifiers in the certificate policies extension, as appropriate.

Certificates that express the id-fpki-common-cardAuth, id-fpki-common-pivi-cardAuth, id-fpki-common-piv-contentSigning, or id-fpki-common-pivi-contentSigning policy OID 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

The CAs may assert policy constraints in CA certificates. When this extension appears, at least one of requireExplicitPolicy or inhibitPolicyMapping must be present. When present, this extension may be marked critical.

For certificates issued to the Federal Bridge CA, inhibitPolicyMapping skip certs must be set to 2.

7.1.8. Policy Qualifiers Syntax and Semantics

Certificates may contain policy qualifiers identified in [RFC 5280].

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

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

7.2. CRL Profile

CRLs issued by a CA under this policy shall conform to the CRL profile specified in [FBCA-PROF].

7.2.1. Version Number(s)

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

7.2.2. CRL and CRL Entry Extensions

Detailed CRL profiles addressing the use of each extension are specified in [FBCA-PROF].

7.3. OCSP Profile

Certificate status servers (CSSs) operated under this policy shall sign responses using algorithms designated for CRL signing.

CSSs shall be able to process SHA-1 hashes when included in the CertID field and the keyHash in the responderID field. CSS may accept and return additional hash algorithms within the CertID fields. CSSs must not return any response containing a hash algorithm in the CertID that differs from the CertID in the request.

7.3.1. Version Number(s)

CSSs operated under this policy shall use OCSP version 1 requests and responses in accordance with RFC 2560.

7.3.2. OCSP Extensions

Critical OCSP extensions shall not be used.

Where nonces are not supported, CSSs shall provide time-based caching responders.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

CAs operating under this policy shall have a compliance audit mechanism in place to ensure that the requirements of their CPS are being implemented and enforced.

The XTec PKI Policy Authority shall have a compliance audit mechanism in place to ensure that the requirements of this CP are being implemented and enforced by its CPS.

This specification does not impose a requirement for any particular assessment methodology.

8.1. Frequency or Circumstances of Assessment

CAs, CMS, CSSs, RAs and supporting repositories operating under this policy shall be subject to a periodic compliance audit at least once per year.

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

Further, the XTec PKI Policy Authority has the right to require aperiodic compliance audits of CAs, CSSs and RAs operating under this policy. The XTecPA shall state the reason for any aperiodic compliance audit.

8.2. Identity/Qualifications of Assessor

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

8.3. Assessor's Relationship to Assessed Entity

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

8.4. Topics Covered by Assessment

The purpose of a compliance audit shall be to verify that a CA and its recognized CMS, CSSs, RAs and supporting repositories comply with all the requirements of the current versions of this CP and the CA's CPS, as well as any Memorandum Of Agreement (MOA) between the XTec PKI and any other PKI (such as the FBCA). All aspects of operations shall be subject to compliance audit inspections.

Components other than CAs may be audited fully or by using a representative sample.

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

8.5. Actions Taken as a Result of Deficiency

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

- The compliance auditor shall note the discrepancy;
- The compliance auditor shall notify the parties identified in section 8.6 of the discrepancy;
- The XTecPA shall determine what further notifications or actions are necessary to meet the requirements of this CP, the CA's CPS, and any relevant MOA provisions. The XTecPA shall proceed to make such notifications and take such actions without delay; and
- The party responsible for correcting the discrepancy will propose a remedy, including expected time for completion to the XTecPA.

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

8.6. Communication of Results

An Audit Compliance Report shall be provided to the entity responsible for PKI operations. The Audit Compliance Report and identification of corrective measures shall be provided to both the XTecPA within 30 days of completion. A special compliance audit may be required to confirm the implementation and effectiveness of the remedy.

The CP/CPS compliance report shall identify the versions of the CP and CPS used in the assessment.

On an annual basis, the XTecPA shall submit an audit compliance package any entity with which it has an ongoing MoA for interoperation. This package shall be prepared in accordance with the "Compliance Audit Requirements" defined within the MoA and include an assertion from the XTecPA 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 XTec PKI CP and XTec PKI CPS used in the assessment. Additionally, where necessary, the results shall be communicated as set forth in Section 8.5 above.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

No Stipulation.

9.1.2. Certificate Access Fees

Section 2 of this policy requires that CA certificates be publicly available. CAs operating under this policy must not charge additional fees for access to this information.

9.1.3. Revocation or Status Information Access Fees

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

9.1.4. Fees for other Services

No Stipulation.

9.1.5. Refund Policy

No Stipulation.

9.2. Financial Responsibility

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

9.2.1. Insurance Coverage

No stipulation.

9.2.2. Other Assets

No stipulation.

9.2.3. Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3. Confidentiality of Business Information

CA information not requiring protection shall be made publicly available. Public access to organizational information shall be determined by the respective organization.

9.3.1. Scope of Confidential Information

No stipulation.

9.3.2. Information not within the Scope of Confidential Information

No stipulation.

9.3.3. Responsibility to Protect Confidential Information

Confidential business information provided to the XTecPA is protected in accordance with the terms of the agreements entered into between the applicable entity and XTec.

Information clearly marked or labeled as confidential that is shared with the XTecPA or any CA operating under this CP shall protect that information and not disclose to additional parties with express written consent of the owner of the confidential information. The entity must treat such information with the same degree of care and security as it treats its own confidential information.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

The XTecPA shall conduct a Privacy Impact Assessment. If deemed necessary, the XTecPA shall have a Privacy Plan to protect personally identifying information from unauthorized disclosure. For the XTec PKI Root CA, the XTec PKI Policy Authority shall approve the Privacy Plan. Privacy plans will be implemented in accordance with the requirements of the Privacy Act of 1974, as amended.

9.4.2. Information Treated as Private

Entities acquiring services under this policy shall protect all subscriber personally identifying information (PII) from unauthorized disclosure. The collection of PII must be limited to that required to meet the needs of operations under this policy. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. The contents of the archives maintained by CAs operating under this policy shall not be released except as required by law.

9.4.3. Information not Deemed Private

Information included in certificates is not subject to protections outlined in section 9.4.2 but may not be sold to a third party.

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).

9.4.4. Responsibility to Protect Private Information

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

All information collected as part of the identity proofing process must be protected to ensure confidentiality and integrity. In the event the Entity terminates PKI activities, the entity is responsible for securely disposing of or destroying sensitive information, including PII, and maintaining its protection from unauthorized access until destruction.

9.4.5. Notice and Consent to Use Private Information

The XTecPA is not required to provide any notice or obtain the consent of the subscriber or Authorized Agency Personnel in order to release private information in accordance with other stipulations of section 9.4.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

The XTecPA shall not disclose private information to any third party unless authorized by this policy, required by law, government rule or regulation, or order of a court of competent jurisdiction. Any request for release of information shall be processed according to 41 CFR 105-60.605.

9.4.7. Other Information Disclosure Circumstances

None.

9.5. Intellectual Property Rights

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

9.6. Representations and Warranties

The obligations described below pertain to the XTecPA.

The XTec PKI Policy Authority shall—

- Review, or direct review, of the CP to ensure compliance with the business needs of the subscribers and relying parties;
- Approve the CP after review;
- Review, or direct review, of the CPS for each CA, that operates under this policy, for compliance to this CP;
- Approve the CPS for each CA that issues certificates under this policy;
- Review periodic compliance audits to ensure that CAs are operating in compliance with their approved CPSs;
- Review name space control procedures to ensure that distinguished names are uniquely assigned for all certificates issued under this CP;
- Revise this CP to maintain the level of assurance and operational practicality;
- Publicly distribute this CP;
- Coordinate modifications to this CP to ensure continued compliance by CAs operating under approved CPSs; and
- Review and approve any investment in additional facilities and equipment, ensuring that such investment meets the requirements of this CP.

9.6.1. CA and KED Representations and Warranties

CAs operating under this policy shall warrant that their procedures are implemented in accordance with this CP, and that any certificates issued that assert the policy OIDs identified in this CP were issued in accordance with the stipulations of this policy.

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

- Providing to the XTecPA a CPS, as well as any subsequent changes, for conformance assessment.

- Maintaining its operations in conformance to the stipulations of the approved CPS.
- Ensuring that registration information is accepted only from approved RAs operating under an approved CPS.
- Including only valid and appropriate information in certificates and maintaining evidence that due diligence was exercised in validating the information contained in the certificates.
- Revoking the certificates of subscribers found to have acted in a manner counter to their obligations in accordance with section 9.6.3.
- Operating or providing for the services of an on-line repository, and informing the repository service provider of their obligations if applicable.
- Maintaining an agreement with Affiliated Organizations concerning the obligations pertaining to authorizing affiliation with Subscribers of PIV-I certificates.

A KED that provides escrowed keys to Requestors under this policy must conform to the stipulations of this document. In particular, the following stipulations apply:

- The XTecPA must approve the CPS/KRPS prior to initiation of key escrow services.
- The KED must operate in accordance with the stipulations of the CPS/KRPS and this policy.
- The CA/KED must automatically notify the subscribers when their private keys have been escrowed during the subscriber registration process (e.g., a dialog box may appear on a subscriber's screen during the certificate request process).
- The KED must monitor KRA and KRO activity for patterns of potentially anomalous activity as indicators of possible problems in the infrastructure, and initiate inquiries or investigations as appropriate.

9.6.2. RA and KRA/KRO Representations and Warranties

9.6.2.1 RA Obligations

An RA that performs registration functions as described in this policy shall comply with the stipulations of this policy and comply with a CPS approved by the XTecPA for use with this policy. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities. An RA supporting this policy shall conform to the stipulations of this document, including—

- Maintaining its operations in conformance to the stipulations of the approved CPS.
- Including only valid and appropriate information in certificate requests and maintaining evidence that due diligence was exercised in validating the information contained in the certificate.
- Ensuring that obligations are imposed on subscribers in accordance with section 9.6.3, and that subscribers are informed of the consequences of not complying with those obligations.

9.6.2.2 KRA Obligations

KRAs that submit requests as described in this policy must comply with the stipulations of this policy and the applicable CPS/KRPS. In particular, the following stipulations apply:

- KRAs must keep a copy of this policy and the applicable CPS/KRPS.
- KRAs must protect subscribers' escrowed keys from unauthorized disclosure, including the encrypted files and associated decryption keys.
- KRAs must protect all information associated with key recovery, including the KRA's own key(s), that could be used to recover subscribers' escrowed keys.
- KRAs must release Subscribers' escrowed keys only for properly authenticated and authorized requests from Requestor.
- KRAs may rely upon the KROs for authentication and verification of the identity and authority of the Requestor. However, KRAs must also authenticate the identity of the Requestor when the Requestor digital signature is available.
- KRAs must authenticate the KROs as described in Section 3.5.4.
- KRAs must validate the authorization of the KRO by ensuring that the KRO is an authorized KRO for the Subscriber for whom key recovery has been requested.
- KRAs must protect all information regarding all occurrences of key recovery.
- KRAs must communicate knowledge of a recovery process only to the KRO and Requestor involved in the key recovery.
- KRAs must not communicate any information concerning a key recovery to the Subscriber except when the Subscriber is the Requestor.
- KRAs must monitor KRO activity for patterns of potentially anomalous behavior as indicators of possible problems in the infrastructure, and initiate inquiries or investigations as appropriate.

9.6.2.1 **KRO Obligations**

A KRO initiates a key recovery request for a Requestor. When using the services of a KRO, the Requestor is generally a third party, but this policy does not preclude the Subscriber from seeking the assistance of a KRO to recover the Subscriber's private key.

- The KRO must protect Subscribers' recovered keys from compromise.
- After providing the Requestor with the encrypted key, the KRO must destroy the copy of the key in his/her system.
- The KRO must request the Subscriber's keys only upon receipt of a request from an authorized Requestor.
- The KRO, as an intermediary for the KRA, must validate the identity of any Requestor seeking a key recovery.
- When the Requestor is authenticated on the basis of digital signature, the KRO must forward the Requestor's digitally signed object to the KRA in a form verifiable by the KRA.
- In the case of persons other than the Subscriber seeking a key recovery, the KRO must ensure that the Requestor has the authority to request the Subscriber's private decryption key.

- The KRO, as an intermediary for the KRA, must validate the authorization for the request, to include consultation with legal counsel when appropriate.
- The KRO must protect all information associated with key recovery, including the KRO's own private key(s), that could be used to obtain the Subscriber's recovered private decryption key(s).
- The KRO must protect all information regarding all occurrences of key recovery.
- The KRO must communicate knowledge of any recovery process only to the Requestor.
- The KRO must not communicate any information concerning a key recovery to the Subscriber except when the Subscriber is the Requestor.
- The KRO must accurately represent himself when requesting key recovery services.
- The KRO must keep records of all recovery requests and disposition, including acknowledgement of receipt by the Requestor.

If an Issuing Organization chooses not to implement the KRO role, then these obligations become the responsibility of the KRA in addition to the obligations in Section 9.6.2.2 above.

9.6.3. Subscriber and Data Decryption Server Representations and Warranties

9.6.3.1 Subscriber Representations and Warranties

A subscriber (or human sponsor for device certificates) shall be required to sign a document containing the requirements the subscriber must meet respecting protection of the private key and use of the certificate before being issued the certificate.

Subscribers shall—

- Accurately represent themselves in all communications with the PKI authorities.
- Protect their private key(s) at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements and local procedures.
- Promptly notify the appropriate CA upon suspicion of loss or compromise of their private key(s). Such notification shall be made directly, or indirectly through mechanisms consistent with the CA's CPS.
- Abide by all the terms, conditions, and restrictions levied on the use of their private key(s) and certificate(s).
- Subscribers must provide accurate identification and authentication information during key recovery requests.
- When the Subscriber is notified that his or her escrowed key has been recovered, the Subscriber must determine whether revocation of the public key certificate associated with the recovered key is necessary. The Subscriber must request the revocation, if necessary.

If the human sponsor for a device is not physically located near the sponsored device, and/or does not have sufficient administrative privileges on the sponsored device to protect the device's private key and ensure that the device's certificate is only used for authorized purposes, the device sponsor may delegate these responsibilities to an authorized administrator for the device.

9.6.3.2 Data Decryption Server Representations and Warranties

Prior to the beginning of the operation of a DDS, the Issuing Organization must formally acknowledge and agree to the obligations described here by signing an appropriate document.

- The DDS must protect Subscribers' recovered key(s) from compromise. The DDS must 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 DDS must destroy Subscribers' keys when no longer required (i.e., when the data has been recovered).
- The DDS must request the Subscriber's escrowed key(s) only upon receiving a request to decrypt subscriber data from an authenticated authorized Enterprise system (e.g., an e-mail Server)
- The DDS must use the Subscriber's recovered keys only to recover Subscriber's data requested from an authenticated authorized Enterprise system.

The DDS must provide accurate identification and authentication information at the same or higher assurance level as required for issuing new PKI certificates at the assurance level of the key being requested.

9.6.4. Relying Parties Representations and Warranties

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

9.6.5. Representations and Warranties of Affiliated Organizations

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

9.6.6. Representations and Warranties of Other Participants

9.6.6.1 CSS Representations and Warranties

A CSS, who provides revocation status and/or complete validation of certificates represents and warrants that it shall conform to the stipulations of this CP, including:

- Providing a CPS, as well as any subsequent changes, for conformance assessment;
- Conforming to the stipulations of this CP and the approved CPS;
- Ensuring that certificate and revocation information is accepted only from valid CAs; and
- Including only valid and appropriate response, and to maintain evidence that due diligence was exercised in validating the certificate status.

A CSS who is found to have acted in a manner inconsistent with these obligations is subject to action as described in Section 8.5.

9.6.6.2 RSSP Obligations

A RSSP that securely stores and uses roaming credentials when requested by the subscribers represents and warrants that it must conform to the stipulations of this CP, including:

- Providing a CPS, as well as any subsequent changes, for conformance assessment;
- Conforming to the stipulations of this CP and the approved CPS;
- Ensuring that subscriber private keys are protected from disclosure, modification and destruction at all times; and
- Subscriber private keys are used only when the subscriber appropriately authenticates to the RSSP and requests the use of their key.

A RSSP that is found to have operated in a manner inconsistent with these obligations is subject to action as described in Section 8.5.

9.6.6.3 Third-party Key recovery Requestors Obligations

Third-party key recovery Requestors must formally acknowledge and agree to the obligations described here, prior to receiving a recovered key:

- Requestor must protect Subscribers' recovered key(s) from compromise. Requestor must 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.
- Third-Party Requestor must destroy Subscribers' keys when no longer required (i.e., when the data has been recovered).
- Requestor must request and use the Subscriber's escrowed key(s) only to recover Subscriber's data they are authorized to access.
- Requestor must accurately represent themselves to all entities during any key recovery service.
- When the request is made, the Requestor must 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 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 must protect information concerning each key recovery operation.
- Upon receipt of the recovered key(s), the Third-Party Requestor must sign an acknowledgement of agreement to follow the law and the subscriber's organizational policies relating to the protection and release of the recovered key. Such agreement MUST contain the following provisions:
    - Third Party Requestor has accurately represented their identity to all key recovery entities;
    - Third Party Requestor has truthfully described the reason(s) for the key recovery 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 will use the recovered key(s) only for the stated purpose(s);
- Third Party Requestor will protect the recovered key(s) 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; and
- Third Party Requestor is 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

CAs operating under this policy may not disclaim any responsibilities described in this CP.

9.8. Limitations of Liability

No stipulation.

9.9. Indemnities

No stipulation.

9.10. Term and Termination

9.10.1. Term

This CP becomes effective when approved by the XTec PKI Policy Authority. This CP has no specified term.

9.10.2. Termination

Termination of this CP is at the discretion of the XTec PKI Policy Authority.

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 and Communications with Participants

The XTecPA shall establish appropriate procedures for communications with CAs operating under this policy via contracts or memoranda of agreement as applicable.

For all other communications, no stipulation.

9.12. Amendments

9.12.1. Procedure for Amendment

The XTecPA shall review this CP at least once every year. Corrections, updates, or changes to this CP shall be publicly available. Suggested changes to this CP shall be communicated to the contact in section 1.5.2; such communication must include a description of the change, a change justification, and contact information for the person requesting the change.

9.12.2. Notification Mechanism and Period

Proposed changes to this CP shall be distributed electronically to XTecPA members and observers in accordance with the Charter and By-laws.

9.12.3. Circumstances under which OID must be Changed

OIDs will be changed if the XTecPA determines that a change in the CP reduces the level of assurance provided.

9.13. Dispute Resolution Provisions

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

9.14. Governing Law

The construction, validity, performance and effect of certificates issued under this CP for all purposes shall be governed by United States Federal law (statute, case law, or regulation).

9.15. Compliance with Applicable Law

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

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

No stipulation.

9.16.2. Assignment

No stipulation.

9.16.3. Severability

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in section 9.12.

9.16.4. Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation.

9.16.5. **Force Majeure**

No stipulation.

9.17. **Other Provisions**

No stipulation.

10. 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
CCP-PROF	Common Policy X.509 Certificate and Certificate Revocation List (CRL) Profiles https://www.idmanagement.gov/docs/fpki-x509-cert-profile-common.pdf
E-Auth	E-Authentication Guidance for Federal Agencies, M-04-04, December 16, 2003. http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf
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, FIPS 140-2, May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
FIPS 186-2	Digital Signature Standard (DSS), FIPS 186-2, January 27, 2000. http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf
FIPS 201-1	Personal Identity Verification (PIV) of Federal Employees and Contractors, FIPS 201-1, March 2006. http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf
FOIACT	5 U.S.C. 552, Freedom of Information Act. http://www4.law.cornell.edu/uscode/5/552.html
ISO9594-8	ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.
ITMRA	40 U.S.C. 1452, Information Technology Management Reform Act of 1996. http://www4.law.cornell.edu/uscode/40/1452.html
NAG69C	Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999.
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.
PACS	*Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems*, Version 2.2, The Government Smart Card Interagency

	Advisory Board's Physical Security Interagency Interoperability Working Group, July 30, 2004. http://www.smart.gov/information/TIG_SCEPACS_v2.2.pdf
PKCS#1	Jakob Jonsson and Burt Kaliski, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, RFC 3447, February 2003. http://www.ietf.org/rfc/rfc3447.txt
PKCS#12	PKCS 12 v1.0: Personal Information Exchange Syntax-June 24, 1999. ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf
RFC 2510	Certificate Management Protocol, Adams and Farrell, March 1999. http://www.ietf.org/rfc/rfc2510.txt
RFC 2560	X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol – OCSP, Michael Myers, Rich Ankney, Ambarish Malpani, Slava Galperin, and Carlisle Adams, June 1999. http://www.ietf.org/rfc/rfc2560.txt
RFC 2822	Internet Message Format, Peter W. Resnick, April 2001. http://www.ietf.org/rfc/rfc2822.txt
RFC 3647	Certificate Policy and Certification Practices Framework, Chokhani and Ford, Sabett, Merrill, and Wu, November 2003. http://www.ietf.org/rfc/rfc3647.txt
SP 800-37	Guide for the Security Certification and Accreditation of Federal Information Systems, NIST Special Publication 800-37, May 2004. http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf
SSP-REP	*Shared Service Provider Repository Service Requirements*, a publication of the Federal PKI Policy Authority Shared Service Provider Working Group http://www.idmanagement.gov/documents/shared-service-provider-repository-service-requirements

11. ACRONYMS AND ABBREVIATIONS

AATL	Adobe Approved Trust List
CA	Certification Authority
C&A	Certification and Accreditation
COMSEC	Communications Security
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Objects Registry
DN	Distinguished Name
XTecOA	XTec Operational Authority
XTecPA	XTec Policy Authority
XTec PKI	XTec Public Key Infrastructure
FIPS PUB	(US) Federal Information Processing Standards Publication
FPKI	Federal Public Key Infrastructure
FPKIPA	Federal PKI Policy Authority
HTTP	Hypertext Transfer Protocol
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
LDAP	Lightweight Directory Access Protocol
ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector
NARA	U.S. National Archives and Records Administration
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
PIN	Personal Identification Number
PIV	Personal Identity Verification

PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PSS	Probabilistic Signature Scheme
RA	Registration Authority
RDN	Relative Distinguished Name
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
RSASSA	RSA Signature Scheme with Appendix
RSSP	Remote Signing Service Provider
SHA	Secure Hash Algorithm
S/MIME	Secure/Multipurpose Internet Mail Extensions
SP	Special Publication
SSL	Secure Sockets Layer
SSP-REP	Shared Service Provider Repository Service Requirements
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
U.S.C.	United States Code
WWW	World Wide Web

12. 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).
Agency	A state government, local government or commercial customer.
Applicant	The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]
Archive	Long-term, physically separate storage.
Attribute Authority	An entity, recognized by the FPKIPA or comparable body as having the authority to verify the association of attributes to an identity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
Backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
Binding	Process of associating two related elements of information. [NS4009]
Biometric	A physical or behavioral characteristic of a human being.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification

	authority issuing it. [ABADSG]. As used in this CP, the term "certificate" refers to X.509 certificates that expressly reference the OID of this CP in the certificatePolicies extension.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 public key certificates and CRLs.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a certification authority to perform certificate issuance and revocation.
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 that it has issued that are revoked prior to their stated expiration date.
Certificate Status Server (CSS)	A trusted entity that provides on-line verification to a relying party of a subject certificate's revocation status and may also provide additional attribute information for the subject certificate.
Client (application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.
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. [FIPS 140-2]
Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a relying party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.
Dual Use Certificate	A certificate that is intended for use with both digital signature and data encryption services.
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 Certificate	A certificate in which the subject is not a CA.
Federal Public Key Infrastructure Policy Authority (FPKIPA)	The FPKIPA is a Federal Government body responsible for setting, implementing, and administering policy decisions regarding the Federal PKI Architecture.
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.
Information Systems Security Officer (ISSO)	Person responsible to the Designated Approving Authority for ensuring the security of an information system throughout its life-cycle, 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 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 (public) key can be used to encrypt a message that can only be decrypted using the other (private) key, and (2) even knowing the public key, it is computationally infeasible to discover the private key.
Legacy Federal PKI	A PKI Implementation owned and managed by a Federal Agency and cross-certified with the Federal Bridge prior to 12/31/2005.
Modification (of a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
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.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization, the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the Federal PKI, OIDS are used to uniquely identify certificate policies and cryptographic algorithms.
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring on-line).
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	Fills the role of a subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of subscribers as defined throughout this CP.
Policy Management Authority (PMA)	Body established to oversee the creation and update of certificate policies, review certification practice statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.
Privacy	Restricting access to subscriber or relying party information in accordance with Federal law.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is normally made publicly available in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and

	public/private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a registration authority is delegated certain tasks on behalf of an authorized CA).
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate that contains the new public key.
Relying Party	A person or entity who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate and is in a position to rely on them.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
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.
Sensitive Information	Sensitive information is any information specifically labelled with “SENSTITIVE” or “CONFIDENTIAL” as well as any information concerning the operation of the system, including logs, archives, Internet Protocol Addressing, information about the security operations of the system and any information specified within the Privacy Assessment as Personally Identifiable Information.
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.
Structural Container	An organizational unit attribute included in a distinguished name solely to support local directory requirements, such as differentiation between human subscribers and devices.

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 that has certified the certificate signature key of another CA, and that constrains the activities of that CA. (See subordinate CA).
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]
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 a CA 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]
XTec PKI Management Authority (XTecOA)	The XTec PKI Operational Authority is the organization responsible for operating the XTec PKI Policy Root Certification Authority.

XTec PKI Policy Authority (XTecPA)	The XTecPA is the body responsible for setting, implementing, and administering policy decisions regarding the XTec PKI policy.
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS 140-2]

Appendix A. Card Management system requirements

PIV-I Cards are issued and managed through information systems called Card Management Systems (CMSs). The complexity and use of these trusted systems may vary. Nevertheless, Entity CAs have a responsibility to ensure a certain level of security from the CMSs that manage the token on which their certificates reside, and to which they issue certificates for the purpose of signing PIV-I Cards. This appendix provides additional requirements to those found above that apply to CMSs that are trusted under this Certificate Policy.

The Card Management Master Key shall be maintained in a FIPS 140-2 Level 2 Cryptographic Module and conform to [NIST SP 800-78] requirements. Diversification operations shall also occur on the Hardware Security Module (HSM). Use of these keys requires PIV-I Hardware or commensurate. Activation of the Card Management Master Key shall require strong authentication of Trusted Roles. Card management shall be configured such that only the authorized CMS can manage issued cards.

The PIV-I identity proofing, registration and issuance process shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV-I credential without the cooperation of another authorized person.

Individual personnel shall be specifically designated to the four Trusted Roles defined in Section 5.2.1. Trusted Role eligibility and Rules for separation of duties follow the requirements for Medium assurance in Section 5.

All personnel who perform duties with respect to the operation of the CMS shall receive comprehensive training. Any significant change to CMS operations shall have a training (awareness) plan, and the execution of such plan shall be documented.

Audit log files shall be generated for all events relating to the security of the CMS shall be treated the same as those generated by the CA (see Sections 5.4 and 5.5).

A formal configuration management methodology shall be used for installation and ongoing maintenance of the CMS. Any modifications and upgrades to the CMS shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the CMS.

The CMS shall have document incident handling procedures that are approved by the head of the organization responsible for operating the CMS. If the CMS is 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.

All Trusted Roles who operate a CMS shall be allowed access only when authenticated using a method commensurate with PIV-I Hardware. 104

The computer security functions listed below are required for the CMS:

- 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; and
- Support recovery from key or system failure.

Appendix B. Entities With Established Memorandum of Agreements (MoA) for Interoperation