
# X.509 Certificate Policy

# for the

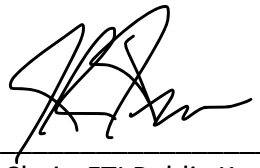
# FTI Certification Authority

**Version 1.6**

**December 16, 2024**

Object Identifier Number for this Version 1.6:
1.3.6.1.4.1.47951.2.2

# Signature Page



Chair, FTI Public Key Infrastructure Policy Authority

# Revision History

| Document Version | Document Date | Revision Details |
|---|---|---|
| 1.0 | June 10, 2016 | Built off STRAC-ID CA Certificate Policy ver. 1.1 |
| 1.1 | July 27, 2017 | Revised to reflect auditor suggestions and include flow-down FBCA CP requirements. |
| 1.2 | October 22, 2018 | Revised to reflect auditor suggestions and include flow-down FBCA CP requirements through change proposal 2018-6. |
| 1.3 | October 6, 2019 | Revised to reflect auditor suggestions and include flow-down FBCA CP requirements through change proposal 2019-1 and SBCA CP flow-down provisions responsive to 2018 FPKI Annual Review of SBCA. |
| 1.4 | November 30, 2020 | Revised to reflect changes in SBCA CP ver. 1.5 suggested by FPKI in response to SBCA's 2019 Annual Review package. |
| 1.5 | November 2, 2023 | Revised to reflect changes in SBCA CP ver. 1.7 suggested by FPKI in response to SBCA's 2020 Annual Review package. |
| 1.6 | December 16, 2024 | Revised to reflect changes in SBCA CP ver. 1.8. |

# Table of Contents

# 1. INTRODUCTION

This Certificate Policy (CP) defines eleven certificate policies for use by the FTI Certification Authority (FTI CA) to issue digital certificates for customers and affiliates. The policies represent five different assurance levels (Rudimentary, Basic, Medium, PIV-I Card Authentication, and Medium Hardware) for public key certificates. In addition, two device certificate policies at the Medium Assurance level are defined to facilitate server to server authentication. The level of assurance refers to the strength of the binding between the public key and the individual whose subject name is cited in the certificate, the mechanisms used to control the use of the private key, and the security provided by the PKI itself.

Personal Identity Verification Interoperable (PIV-I) policies for PIV-I Hardware, PIV-I Card Authentication, and PIV-I Content Signing are for use with PIV-I smart cards (see Appendix A for more information).

The FTI CA issues certificates only to individuals and devices except as necessary to effectuate cross-certification with the STRAC Bridge Certification Authority. Any use of or reference to this FTI CA CP outside the purview of the FTI PKI Policy Authority is completely at the using party's risk. In this CP, the term "FTI PKI Policy Authority" refers to the individual(s) or entity designated by FTI's Executive Director to serve as the policy authority governing the FTI CA and its associated PKI.

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

The terms and provisions of this FTI CA CP shall be interpreted under and governed by applicable Texas law.

## *1.1 OVERVIEW*

### 1.1.1 Certificate Policy (CP)

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

### 1.1.2 Relationship between the FTI CA CP and the FTI CPS

The FTI CA CP states what assurance can be placed in a certificate issued by the FTI CA. Rather than developing another, separate Certification Practices Statement (CPS) to state how the FTI CA establishes that assurance, the FTI CA adopts and shall comply with the CPS that STRAC has adopted for the STRAC BCA, called the "Certification Practices Statement for the STRAC Bridge

Certification Authority and the Participant Certification Authority" and referred to herein as the "FTI CPS." All provisions in the FTI CPS that apply to the "Participant CA" equally apply the FTI CA except for FTI CA-specific items (such as Object Identifiers) as detailed in the Section 13.1 of the FTI CPS.

### 1.1.3 Southwest Texas Regional Advisory Council for Trauma (STRAC)

STRAC is a non-profit corporation created by the Texas state legislature to develop and implement the regional trauma and emergency healthcare system for the 22 county region in and around San Antonio, Texas. STRAC operates the STRAC Bridge Certification Authority subject to the governance of entities with CAs cross-certified to the STRAC Bridge CA, pursuant to the STRAC Bridge CA Charter.

STRAC created Foundation for Trusted Identity (FTI), a separate Texas non-profit corporation of which STRAC is the sole Member.

### 1.1.4 Foundation for Trusted Identity (FTI)

FTI is a non-profit Texas corporation that owns and maintains the FTI PKI, including the FTI Certification Authority (FTI CA). FTI has established the framework for the interoperable FTI PKI and established the FTI PKI Policy Authority (FTI PKIPA) and FTI PKI Management Authority (FTI PKIMA) to implement, guide and oversee the FTI PKI. In particular, this CP was established by FTI. In this CP, the term FTI PKI refers to the PKI that includes the FTI CA; the terms FTI PKI Policy Authority and FTI PKI Management Authority refer to the individual(s) or entities designated by FTI to serve in those roles for the FTI PKI and the FTI CA within the FTI PKI.

The FTI PKI and governance structure are separate and distinct from those of the STRAC Bridge CA. FTI intends to cross-certify the FTI CA with the STRAC Bridge CA. If it applies for cross-certification with the STRAC Bridge CA, FTI CA will meet any requirements that its CP maps to the STRAC Bridge CP.

### 1.1.5 Scope

The FTI CA exists primarily to facilitate trusted electronic business transactions for state, local, tribal, and territorial governmental and non-profit organizations, particularly those focused on public safety and healthcare. The FTI CA facilitates the missions of the organizations by enabling interoperability of identity credentials among these entities as well as Federal entities.

## *1.2 DOCUMENT IDENTIFICATION*

There are eleven policies specified at five different levels of assurance in this Certificate Policy, which are defined in subsequent sections. Each level of assurance has an Object Identifier (OID), to be asserted in certificates issued by the FTI CA. FTI CA will assert these OIDs in policyMappings extensions of certificates issued by FTI CA. The FTI CA policy OIDs are registered in the ISO OID Repository as follows:

*Table 1 – FTI CA Certificate Policies*

| | |
|---|---|

| | |
|---|---|
| iso-certpolicy OBJECT IDENTIFIER | ::= {1.3.6.1.4.1.47951.2.2} |
| fti-policies OBJECT IDENTIFIER | ::= {1.3.6.1.4.1.47951.2.2.5} |
| fti-certpcy-rudimentaryAssurance | ::= {1.3.6.1.4.1.47951.2.2.5.1} |
| fti-certpcy-basicAssurance | ::= {1.3.6.1.4.1.47951.2.2.5.2} |
| fti-certpcy-mediumAssurance | ::= {1.3.6.1.4.1.47951.2.2.5.3} |
| fti-certpcy-mediumHardware | ::= {1.3.6.1.4.1.47951.2.2.5.4} |
| fti-certpcy-medium-CBP | ::= {1.3.6.1.4.1.47951.2.2.5.5} |
| fti-certpcy-mediumHW-CBP | ::= {1.3.6.1.4.1.47951.2.2.5.6} |
| fti-certpcy-pivi-hardware | ::= {1.3.6.1.4.1.47951.2.2.5.7} |
| fti-certpcy-pivi-cardAuth | ::= {1.3.6.1.4.1.47951.2.2.5.8} |
| fti-certpcy-pivi-contentSigning | ::= {1.3.6.1.4.1.47951.2.2.5.9} |
| fti-certpcy-mediumDevice | ::= {1.3.6.1.4.1.47951.2.2.5.10} |
| fti-certpcy-mediumDeviceHardware | ::= {1.3.6.1.4.1.47951.2.2.5.11} |

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

Certificates that assert policies mapped to STRAC BCA policies and are issued to devices after October 1, 2016, shall assert policies mapped to STRAC BCA Medium Device, Medium Device Hardware, or PIV-I Content Signing policies. All other policies defined in this document are reserved for human subscribers when used in End-Entity certificates.

The requirements associated with the medium-CBP (commercial best practice) policy are identical to those defined for the Medium Assurance policy with the exception of personnel security requirements (see Section 5.3.1).

The requirements associated with the Medium Hardware policy are identical to those defined for the Medium Assurance policy with the exception of subscriber cryptographic module requirements (see Section 6.2.1).

The requirements associated with the mediumHW-CBP policy are identical to those defined for the Medium Hardware Assurance policy with the exception of personnel security requirements (see Section 5.3.1).

The requirements associated with PIV-I Hardware and PIV-I Content Signing are identical to Medium Hardware except where specifically noted in the text and further described in Appendix A.

In addition, the PIV-I Content Signing policy is reserved for certificates used by the Card Management System (CMS) to sign the PIV-I card security objects.

## *1.3 PKI ENTITIES*

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

### 1.3.1 PKI Authorities

#### *1.3.1.1 FTI PKI Policy Authority (FTI PKIPA)*

FTI shall identify an individual, group of individuals, or entity known as the FTI PKI Policy Authority (FTI PKIPA) to own this policy and direct the work of the FTI PKI Management Authority. No individual serving on the FTI PKIPA may also serve on the FTI PKI Management Authority. The FTI PKIPA is responsible for:

- maintaining this CP,
- ensuring that all FTI PKI components (e.g., CAs, CSSs, CMSs, RAs) are operated in compliance with this CP, and
- adopting and maintaining the FTI CPS as it applies to the FTI CA.

If it achieves cross-certification with the STRAC Bridge CA, the FTI PKIPA will execute any Memorandum of Agreement (MOA) required for that cross-certification.

The FTI PKIPA shall also be responsible for notifying the SPKIPA of any change to the infrastructure that has the potential to affect the Federal PKI operational environment at least two weeks prior to implementation; all new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the change shall be provided to the SPKIPA within 24 hours following implementation.

#### *1.3.1.2 FTI PKI Management Authority (FTI PKIMA)*

The FTI PKI Management Authority is the individual, group of individuals, or entity that operates and maintains the FTI CA on behalf of FTI, subject to the direction of the FTI PKIPA. No individual serving on the FTI PKIMA may also serve on the FTI PKIPA.

#### *1.3.1.3 FTI PKI Management Authority Program Manager*

The Program Manager is the individual within the FTI PKI Management Authority who has principal responsibility for overseeing the proper operation of the FTI CA including the FTI CA repository, and selecting the FTI PKI Management Authority Staff. The Program Manager is selected by the FTI PKI Policy Authority and reports to the FTI PKIPA.

#### *1.3.1.4 Certificate Status Servers*

PKIs may optionally include an authority that provides status information about certificates on behalf of a CA through online transactions. In particular, PKIs may include OCSP responders to provide online status information. Such an authority is termed 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 6960, are not covered by this policy. If it issues PIV-I certificates, the FTI CA must provide an OCSP responder.

#### *1.3.1.5 Entity Principal Certification Authority (CA)*

If it applies for cross-certification with the STRAC Bridge CA, the FTI PKIPA will designate the CA (whether a Root or a Subordinate CA) that will be cross-certified with the STRAC Bridge CA.

FTI shall ensure that no CA under its PKI shall have more than one trust path to the Federal Bridge CA (regardless of path validation results).

#### *1.3.1.6 STRAC Bridge Certification Authority (STRAC BCA)*

If it becomes cross-certified with the STRAC Bridge CA, the FTI CA will nonetheless be independent of the STRAC Bridge CA; it will not be subordinate to the STRAC Bridge CA. The FTI CA and the STRAC Bridge CA will be under separate governance, and each must adhere to policies and procedures required by the other in order to maintain cross-certification with the other.

### 1.3.2 Registration Authority (RA)

The RA collects and verifies each Subscriber's identity and information for inclusion in the Subscriber's public key certificate. The FTI PKI Management Authority acts as the RA for the FTI CA, and performs its function in accordance with a CPS approved by the FTI PKI Policy Authority. FTI CA may designate its own RAs. The requirements for RAs for the FTI CA are set forth elsewhere in this document.

A Trusted Agent is authorized by a PKI to act on its behalf and may record information from and verify biometrics (e.g., photographs) on presented credentials on behalf of an RA for Applicants who cannot appear before an RA. Trusted Agents are not Trusted Roles; however, the PKI must document any Trusted Agent authorization requirements to include:

- trustworthiness vetting, and
- training or government appointment (e.g., notary public).

**All identity proofing audit artifacts produced by a Trusted Agent must be traceable to an individual.1.3.3 Card Management System (CMS)**

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 PIV-I policies only. In issuing PIV-I certificates, the FTI CA is responsible for ensuring that its CMS meets the

requirements described in this document, including all requirements specified in Appendix B. In addition, the CMS shall not be issued any certificates that express the PIV-I Hardware or PIV-I Card Authentication policy OID.

### 1.3.4 Subscribers

A Subscriber is the user or device to whom or to which a certificate is issued. FTI CA Subscribers include only individuals who have been properly vetted as to their level of assurance, as well as network or hardware devices. Where certificates are issued to devices, the entity must have a human sponsor who is responsible for carrying out Subscriber duties. Note that CAs are sometimes technically considered "subscribers" in a PKI. However, the term "Subscriber" as used in this document does not refer to CAs.

All Subscribers that receive or use a certificate from the FTI CA must comply with the terms of the FTI CA Subscriber Agreement; use of a certificate issued by the FTI CA in violation of the FTI CA Subscriber Agreement is a violation of this CP. The FTI CA Subscriber Agreement, which may change from time to time, is posted at https://pki.fti.org/fti_CA/documents.

### 1.3.5 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.

### 1.3.6 Relying Parties

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

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

### 1.3.7 Other Participants

The FTI CA may require the services of other security, community, and application authorities. If required, the FTI CPS shall identify the parties, define the services, and designate the mechanisms used to support these services.

### 1.3.8 Key Recovery Authorities

FTI does not escrow private keys or support key recovery.

## *1.4 CERTIFICATE USAGE*

### 1.4.1 Appropriate Certificate Uses

The sensitivity of the information processed or protected using certificates issued by the FTI CA will vary significantly. Relying Parties must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each Relying Party for its application and is not controlled by this CP. To provide sufficient granularity, this CP specifies security requirements at five increasing, qualitative levels of assurance: Rudimentary, Basic, Medium, PIV-I Card Authentication, and Medium Hardware. It is assumed that the FTI CA will issue at least one Medium Hardware assurance certificate, so the FTI CA will be operated at that level. The FTI CA is intended to support applications involving unclassified information, which can include sensitive unclassified data protected pursuant to Federal statutes and regulations.

The following table provides a brief description of the appropriate uses for certificates at each level of assurance defined in this CP. These descriptions are intended as guidance and are not binding.

| Assurance Level | Appropriate Certificate Uses |
|---|---|
| Rudimentary | This level provides the lowest degree of assurance concerning identity of the individual. One of the primary functions of this level is to provide data integrity to the information being signed. This level is relevant to environments in which the risk of malicious activity is considered to be low. It is not suitable for transactions requiring authentication, and is generally insufficient for transactions requiring confidentiality, but may be used for the latter where certificates having higher levels of assurance are unavailable. |
| Basic | This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level that users are not likely to be malicious. |
| Medium | This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. This level of assurance includes the following certificate policies: Medium, Medium CBP, and Medium Device. |

| | |
|---|---|
| PIV-I Card Authentication | This level is relevant to environments where risks and consequences of data compromise are moderate. This may include contactless smart card readers where use of an activation pin is not practical. |
| Medium Hardware | This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk. This level of assurance includes the following certificate policies: Medium Hardware, Medium Hardware CBP, Medium Device Hardware, PIV-I Hardware, and PIV-I Content Signing. |

### 1.4.2 Prohibited Certificate Uses

No stipulation.

## *1.5 POLICY ADMINISTRATION*

### 1.5.1 Organization Administering the Document

The FTI PKI 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 FTI PKI Policy Authority, whose address can be found at https://pki.fti.org/fti_CA/contact.

### 1.5.3 Person Determining Certification Practices Statement Suitability for the Policy

The Certification Practices Statement must conform to the corresponding Certificate Policy. The FTI PKI Policy Authority is responsible for asserting whether the FTI CPS conforms to the FTI CA CP.

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.

### 1.5.4 CPS Approval Procedures

The FTI PKI Management Authority shall submit the FTI CPS and the results of a compliance audit to the FTI PKIPA for approval. The FTI PKIPA shall vote to accept or reject the CPS. If rejected, the FTI PKI Management Authority shall resolve the identified discrepancies and resubmit to the FTI PKIPA. The FTI CA is required to meet all facets of the policy. The FTI PKIPA shall not issue waivers of CP requirements.

### *1.6 DEFINITIONS AND ACRONYMS*

See Sections 11 and 12.

# 2. PUBLICATION & REPOSITORY RESPONSIBILITIES

## 2.1 REPOSITORIES

The FTI PKI Management Authority shall operate repositories to support FTI CA operations. If it is cross-certified to the STRAC Bridge CA, the FTI CA will ensure access to and the ability to consume data posted to the STRAC Bridge CA repository.

#### 2.1.1 FTI CA Repository Obligations

The FTI PKI Management Authority may use a variety of mechanisms for posting information into a repository as required by this CP. These mechanisms at a minimum shall include:

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

### *2.2 PUBLICATION OF CERTIFICATION INFORMATION*

#### 2.2.1 Publication of Certificates and Certificate Status

CA and End Entity certificates shall only contain valid Uniform Resource Identifiers (URIs) that are accessible by relying parties.

The FTI PKI Management Authority shall publish all CA certificates issued by or to the FTI CA and all CRLs issued by the FTI CA in the FTI CA repository.

For the FTI CA, mechanisms and procedures shall be designed to ensure CA certificates and CRLs are available for retrieval 24 hours a day, 7 days a week, with a minimum of 99% availability overall per year and scheduled down-time not to exceed 0.5% annually.

#### 2.2.2 Publication of CA Information

The FTI PKI Management Authority shall publish such information concerning the FTI CA as it deems appropriate and necessary to support the FTI CA's use and operation. The FTI CA CP shall be publicly available on the FTI PKI website at https://pki.fti.org/fti_CA/documents.

#### 2.2.3 Interoperability

Where certificates and CRLs are published in directories, standards-based schemas for directory objects and attributes are recommended.

## 2.3 FREQUENCY OF PUBLICATION

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

## 2.4 ACCESS CONTROLS ON REPOSITORIES

The FTI PKI Management Authority shall protect any repository information not intended for public dissemination or modification. The FTI PKIMA shall make CA certificates and certificate status information publicly available through the Internet in the FTI CA repository.

Direct and/or remote access to information in FTI CA repositories shall be determined by FTI pursuant to applicable rules and statutes. Certificates and certificate status information in the FTI CA repository should be publicly available through the Internet. At a minimum, FTI CA repositories shall make CRLs issued by the FTI CA and CA certificates issued to the FTI CA available to Federal Relying Parties and FTI Relying Parties.

# 3. IDENTIFICATION & AUTHENTICATION

## *3.1 NAMING*

### 3.1.1 Types of Names

For FTI CA, the following rules apply: All CA and RA certificates shall include a non-NULL subject Distinguished Name (DN). All certificates issued to end entities, except those issued at the Rudimentary level of assurance, shall include a non-NULL subject DN. Certificates issued at the Rudimentary level of assurance may include a null subject DN if they include at least one alternative name form. Certificates at all levels of assurance may include alternative name forms. This CP does not restrict the types of names that can be used.

The table below summarizes the naming requirements that apply to each level of assurance.

| | |
|---|---|
| Rudimentary | Non-Null Subject Name, or Null Subject Name if Subject Alternative Name is populated and marked critical |
| Basic | Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical |
| Medium (all policies) | Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical |
| PIV-I Card Authentication | Non-Null Subject Name, and Subject Alternative Name |

PIV-I Hardware certificates shall indicate whether or not the Subscriber is associated with an Affiliated Organization by taking one of the following forms:

For certificates with an Affiliated Organization:

cn=*Subscriber's full name*, ou=*Affiliated Organization Name*, ou=*Certificate Type*, s=*State*, c=*Country*

For certificates with no Affiliated Organization:

cn=*Subscriber's full name*, ou=*Unaffiliated*, ou=*FTI Certification Authority*, ou=*Certificate Type*, s=*State*, c=*Country*

PIV-I Content Signing certificates shall clearly indicate the organization administering the CMS.

For PIV-I Card Authentication subscriber certificates, use of the subscriber common name is prohibited.

PIV-I Card Authentication certificates shall indicate whether or not the Subscriber is associated with an Affiliated Organization by taking one of the following forms:

For certificates with an Affiliated Organization:

serialNumber=*UUID*, ou=*Affiliated Organization Name*, ou=*Certificate Type*, s=*State*, c=*Country*

For certificates with no Affiliated Organization:

serialNumber=*UUID*, ou=Unaffiliated, ou=*FTI Certification Authority*, ou=*Certificate Type*, s=*State*, c=*Country*

The UUID shall be encoded within the serialNumber attribute using the UUID string representation defined in Section 3 of RFC 4122 (e.g., “f81d4fae-7dec-11d0-a765-00a0c91e6bf6”).

### 3.1.2 Need for Names to Be Meaningful

Names used in the certificates issued by the FTI CA must identify the person or object to which they are assigned.

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

When DNs are used, the common name must respect name space uniqueness requirements and must not be misleading. This does not preclude the use of pseudonymous certificates as defined in Section 3.1.3.

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

### 3.1.3 Anonymity or Pseudonymity of Subscribers

The FTI CA shall not issue anonymous certificates. Pseudonymous certificates may be issued by the FTI CA to support internal operations.

### 3.1.4 Rules for Interpreting Various Name Forms

The FTI CA shall follow the rules for interpreting names in CA or Subscriber certificates as specified in the FTI PKI Profile [FTI PKI-Prof].

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

### 3.1.5 Uniqueness of Names

Name uniqueness must be enforced by the FTI CA and its RAs.

The FTI PKI PA is responsible for ensuring name uniqueness in certificates issued by the FTI CA. Name uniqueness is not violated when multiple certificates are issued to the same entity.

### 3.1.6 Recognition, Authentication, & Role of Trademarks

The FTI PKIPA shall resolve any name collisions or disputes regarding FTI CA-issued certificates brought to its attention.

## *3.2 INITIAL IDENTITY VALIDATION*

### 3.2.1 Method to Prove Possession of Private Key

In all cases where the party named in a certificate generates its own keys that party shall be required to prove possession of the private key that corresponds to the public key in the certificate request.

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

### 3.2.2 Authentication of Organization Identity

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

The FTI PKI Policy Authority or RA 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

PIV-I Hardware certificates shall only be issued to human subscribers.

#### *3.2.3.1 Authentication of Human Subscribers*

For Subscribers, the FTI PKI Management Authority and/or associated RAs shall ensure that the applicant's identity information is verified in accordance with the process established by the applicable CP and CPS. Process information shall depend upon the certificate level of assurance and shall be addressed in the FTI CPS. The documentation and authentication requirements shall vary depending upon the level of assurance.

For Medium Assurance, identity shall be established no more than 30 days before initial certificate issuance.

The FTI PKI Management Authority and/or RAs shall record the information set forth below for issuance of each certificate:

- The identity of the person performing the identification;
- A signed declaration by that person that he or she verified the identity of the applicant as required using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law. The signature on the declaration may be either a handwritten or digital signature using a certificate that is of equal or higher level of assurance as the credential being issued;
- If in-person or supervised remote[1] identity proofing is done, a unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- The date of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature or appropriate digital signature (see Practice Note) and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

**For All Levels except PIV-I**: If an applicant is unable to perform face-to-face, either in-person or supervised remote, registration (e.g., a network device), the applicant may be represented by a trusted person already issued a digital certificate by the Entity. The trusted person will present information sufficient for registration at the level of the certificate being requested, for both himself/herself and the applicant whom the trusted person is representing.

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

**For the Basic and Medium Assurance Levels:** 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.

[1] The minimum requirements associated with supervised remote identity proofing are described in NIST SP 800-63A, *Digital Identity Guidelines: Enrollment and Identity Proofing*, Section 5.3.3.

**For PIV-I Certificates:** The following biometric data shall be collected during the identity proofing and registration process, and shall be formatted in accordance with [NIST SP 800-76] (see Appendix 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
- Two electronic fingerprints to be stored on the card for automated authentication during card usage.

The table below summarizes the identification requirements for each level of assurance.

| Assurance Level | Identification Requirements |
|---|---|
| Rudimentary | No identification requirement; applicant may apply and receive a certificate by providing his or her e-mail address |
| Basic | Identity may be established by in-person proofing before a Registration Authority or Trusted Agent; or 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, and confirms that: name, DoB, address and other personal information in records are consistent with the application and sufficient to identify a unique individual.<br><br>Address confirmation:<br><br>a) Issue credentials in a manner that confirms the address of record supplied by the applicant; or<br><br>b) 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. |
| Medium (all policies) | Identity shall be established by in-person proofing before the Registration Authority, Trusted Agent or an entity certified by a State or Federal Entity as being authorized to confirm identities; information provided shall be verified to ensure legitimacy. A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement.[2] Credentials required are one Federal Government-issued Picture I.D., one REAL ID Act compliant picture ID, or two Non-Federal Government I.D.s, one of which shall be a photo I.D. Any credentials presented must be unexpired. |

[2] Clarification on the trust relationship between the Trusted Agent and the applicant, which is based on an in-person antecedent identity proofing event, can be found in the *FBCA Supplementary Antecedent, In-Person Definition* document.

| | |
|---|---|
| | For PIV-I, credentials required 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). For PIV-I, the use of an in-person antecedent is not applicable. |

In the event an applicant is denied a credential based on the results of the identity proofing process, FTI shall provide a mechanism for appeal or redress of the decision.

#### *3.2.3.2 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 FTI CA or an RA 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.

#### *3.2.3.3 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 FTI CA 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).

#### *3.2.3.4 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 shall be issued only to devices under the sponsoring entity's control. In the case a human sponsor is changed, the new sponsor shall review the status of each device under his/her sponsorship to ensure it is still authorized to receive certificates. The CPS shall describe procedures to ensure that certificate accountability is maintained.

The registration information shall be verified to an assurance level commensurate with the certificate assurance level being requested. For certificates issued with the medium Device and mediumDeviceHardware policies, registration information shall be verified commensurate with the Medium assurance level. Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

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

### 3.2.4 Non-verified Subscriber Information

Except for the rudimentary assurance level, information that is not verified shall not be included in certificates.

#### 3.2.5 Validation of Authority

For cross-certification, the FTI PKI Management Authority shall validate the representative's authorization to act in the name of the organization.

#### 3.2.6 Criteria for Interoperation

The FTI PKI Policy Authority shall determine the criteria for cross-certification with the FTI CA. Under no circumstances shall any certificate have more than one intentional trust path to the Federal Bridge CA, irrespective of extension processing.

*Note:* Multiple trust paths created as a result of certificate renewal or CA rekey do not violate the single trust path requirement above.

### *3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS*

In the event that a subscriber re-key is required, a new certificate will be issued to the subscriber by the FTI CA. See Section 4.7.1 for circumstances when re-key is appropriate. Identification and authentication for re-key requests follow the provisions for identification and authentication for initial certificate application in Sec. 3.2.

### *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.

## 4. CERTIFICATE LIFE-CYCLE

### *4.1 APPLICATION*

This section specifies requirements for initial application for certificate issuance.

The FTI CA may issue end user certificates to trusted personnel where necessary for the internal operations of the FTI CA. The FTI CA may also issue end-user certificates for any other valid reason as described in this CP. FTI CA shall not issue CA certificates to other entities except for cross-certification with the STRAC Bridge CA.

#### 4.1.1 Submission of Certificate Application

FTI CA shall not issue CA certificates to other entities except for cross-certification with the STRAC Bridge CA. Otherwise, no stipulation.

#### 4.1.2 Enrollment Process and Responsibilities

If it applies for cross-certification to the STRAC Bridge CA, the FTI CA is responsible for providing accurate information on its certificate application.

For the FTI CA all communications among PKI authorities supporting the certificate application and issuance process shall be authenticated and protected from modification. If databases or

other sources are used to confirm Subscriber attributes, then these sources and associated information sent to a CA shall require:

- When information is obtained through one or more information sources, an auditable chain of custody be in place.
- All data received be protected and securely exchanged in a confidential and tamper evident manner, and protected from unauthorized access.

## *4.2 CERTIFICATE APPLICATION PROCESSING*

Information in certificate applications must be verified as accurate before certificates are issued.

The procedures for verifying information in certificate applications to the FTI CA are specified in this Section 4.2.

### 4.2.1 Performing Identification and Authentication Functions

For the FTI CA, 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.

### 4.2.2 Approval or Rejection of Certificate Applications

The FTI CA may approve or reject a certificate application, at its discretion.

### 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 ISSUANCE*

### 4.3.1 CA Actions during Certificate Issuance

Upon receiving a request for a certificate, the FTI CA/RAs must:

- Verify the identity of the requestor.
- Verify the authority of the requestor and the integrity of the information in the certificate request.
- Verify all attribute information received from a Subscriber before inclusion in a certificate.
- 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 the obligations described in Section 9.6.3.

The FTI CA shall verify the source of a certificate request before issuance.

#### 4.3.2 Notification to Subscriber of Certificate Issuance

When the FTI CA sends a signed certificate to the subscriber, there need not be any separate notice sent.

#### 4.3.3 Prohibition on Issuance of Production Certificates to Test CAs

The FTI CA is prohibited from issuing production certificates to test CAs.

## *4.4 CERTIFICATE ACCEPTANCE*

Before a subscriber can make effective use of its private key, an FTI CA Registration Authority shall convey to the subscriber its responsibilities as defined in Section 9.6.3.

#### 4.4.1 Conduct constituting certificate acceptance

For the FTI CA, failure to object to the certificate or its contents constitutes acceptance of the certificate.

#### 4.4.2 Publication of the Certificate by the CA

The FTI CA shall publish all certificates it issues to or receives from the STRAC Bridge CA; this CP contains no stipulation regarding publication of Subscriber certificates.

#### 4.4.3 Notification of Certificate Issuance by the CA to other entities

FTI CA shall not issue CA certificates to other entities except for cross-certification with the STRAC Bridge CA, in which case it shall notify the STRAC Bridge CA at least two weeks prior to issuance of such CA certificates. Such notification shall assert that the new CA cross-certification does not introduce multiple paths to a CA already participating in the Federal PKI. In addition, all new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the CA certificate issuance shall be provided to the SPKIPA within 24 hours following issuance.

## *4.5 KEY PAIR AND CERTIFICATE USAGE*

#### 4.5.1 Subscriber Private Key and Certificate Usage

For Medium Hardware, Medium, and Basic Assurance, subscribers shall protect their private keys from access by other parties. For Rudimentary assurance, no stipulation.

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

All Subscribers are required to comply with the FTI CA Subscriber Agreement.

#### 4.5.2 Relying Party Public Key and Certificate Usage

FTI CA-issued certificates specify restrictions on use through critical certificate extensions, including the basic constraints and key usage extensions. The FTI CA issues CRLs and maintains

OCSP service to indicate the current status of FTI CA certificates. It is recommended that relying parties process this information whenever using FTI CA issued certificates in a transaction.

All parties that rely upon certificates issued by the FTI CA must comply with the FTI CA Relying Party Agreement.

## *4.6 CERTIFICATE RENEWAL*

Certificate renewal consists of issuing a new certificate with a new validity period and serial number while retaining all other information in the original certificate including the public key. Frequent renewal of certificates may assist in reducing the size of CRLs. After certificate renewal, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

### 4.6.1 Circumstance for Certificate Renewal

A certificate may be renewed if the 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. In addition, the validity period of the certificate must meet the requirements specified in Section 6.3.2.

### 4.6.2 Who may request Renewal

For subscriber certificates, renewal requests shall only be accepted by the FTI CA from certificate subjects, PKI sponsors or RAs. Additionally, the FTI CA may perform renewal of its subscriber certificates without a corresponding request. For any cross-certificate with the STRAC Bridge CA, the FTI CA shall accept renewal requests only from the STRAC Bridge CA or the FTI PKI Management Authority.

### 4.6.3 Processing Certificate Renewal Requests

No stipulation.

### 4.6.4 Notification of new certificate issuance to Subscriber

No stipulation.

### 4.6.5 Conduct constituting acceptance of a Renewal certificate

No stipulation.

### 4.6.6 Publication of the Renewal certificate by the CA

The FTI CA does not publish Subscriber certificates. As specified in 2.2.1, all CA certificates shall be published in the FTI CA repositories.

### 4.6.7 Notification of Certificate Issuance by the CA to other entities

No stipulation.

## *4.7 CERTIFICATE RE-KEY*

The FTI CA supports re-key by following the same procedure as applies to the initial application for and issuance of certificates.

### 4.7.1 Circumstance for Certificate Re-key

Re-key is appropriate when requested by an individual or entity as provided in Sec. 4.7.2.

### 4.7.2 Who may request certification of a new public key

The Subscriber or the Affiliated Organization (if any) may request re-key.

### 4.7.3 Processing certificate Re-keying requests

The processing of re-key requests follows the provisions for certificate application processing in Sec. 4.2. For re-keying any cross-certification with the STRAC Bridge CA, the validity period associated with the new certificate must not extend beyond the period of the MOA with the STRAC Bridge PKI PA.

### 4.7.4 Notification of new certificate issuance to Subscriber

Notification to the Subscriber of new certificate issuance follows the provisions for notification in Sec. 4.3.2.

### 4.7.5 Conduct constituting acceptance of a Re-keyed certificate

Failure to object to the certificate or its contents constitutes acceptance of the certificate.

### 4.7.6 Publication of the Re-keyed certificate by the CA

The FTI CA does not publish certificates issued to Subscribers. As specified in 2.2.1, all CA certificates shall be published in the FTI CA repositories.

### 4.7.7 Notification of certificate issuance by the CA to other Entities

FTI CA does not issue CA certificates to other entities except for cross-certification with the STRAC Bridge CA, in which case it shall notify the STRAC Bridge CA of such CA certificates.

## *4.8 MODIFICATION*

Certificate modification consists of creating new certificates with subject information (e.g., a name or email address) that differs from the old certificate.

The FTI CA does not support certificate modification.

### 4.8.1 Circumstance for Certificate Modification

The FTI CA does not support certificate modification.

### 4.8.2 Who may request Certificate Modification

The FTI CA does not support certificate modification.

#### 4.8.3 Processing Certificate Modification Requests

The FTI CA does not support certificate modification.

#### 4.8.4 Notification of new certificate issuance to Subscriber

The FTI CA does not support certificate modification.

#### 4.8.5 Conduct constituting acceptance of modified certificate

The FTI CA does not support certificate modification.

#### 4.8.6 Publication of the modified certificate by the CA

The FTI CA does not support certificate modification.

#### 4.8.7 Notification of certificate issuance by the CA to other Entities

The FTI CA does not support certificate modification.

## *4.9 CERTIFICATE REVOCATION & SUSPENSION*

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

For Medium Hardware, Medium, and Basic Assurance, all CAs shall publish CRLs.

The FTI CA shall notify the SPKIPA at least two weeks prior to the revocation of a CA certificate, whenever possible. For emergency revocation, the FTI CA shall follow the notification procedures in Section 5.7.

#### 4.9.1 Circumstances for Revocation

For the FTI CA, a certificate shall be revoked when the binding between the subject and the subject's public key defined within a certificate is no longer considered valid. There are three circumstances under which certificates issued by the FTI CA will be revoked:

- The first circumstance is when the FTI PKI Policy Authority requests a FTI CA-issued certificate be revoked. This will be the normal mechanism for revocation in cases where the FTI PKI Policy Authority determines that a Subscriber does not meet the FTI PKI policy requirements or the FTI PKIPA in its discretion elects to discontinue certification of the Subscriber.
- The second circumstance is when the Management Authority receives an authenticated request from a previously designated official of the Entity responsible for the Subscriber, or from a FTI Registration Authority.
- The third circumstance is when the FTI CA Operational personnel determine that an emergency has occurred that may impact the integrity of the certificates issued by the FTI CA. Under such circumstances, the following individuals may authorize immediate certificate revocation:
    - Chair, FTI PKI Policy Authority;

- Program Manager of the FTI PKIMA; or
- An individual designated by the FTI PKI Policy Authority.

The FTI PKI Policy Authority shall meet as soon as practicable to review the emergency revocation.

FTI CA utilizes certificate revocation and shall revoke certificates for the reason of key compromise upon receipt of an authenticated request from an appropriate entity.

For Certificates that express an organizational affiliation, FTI CA shall require that the organization must inform the FTI CA of any changes in the subscriber affiliation. If the affiliated organization no longer authorizes the affiliation of a Subscriber, FTI CA shall revoke any certificates issued to that Subscriber containing the organizational affiliation. If an organization terminates its relationship with FTI CA such that it no longer provides affiliation information, the FTI CA shall revoke all certificates affiliated with that organization.

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

### 4.9.2 Who Can Request Revocation

FTI CA shall, at a minimum, accept revocation requests from subscribers or the STRAC Bridge CA. FTI CA issues certificates in association with Affiliated Organizations and shall accept revocation requests from authorized representatives of the Affiliated Organization named in the certificate, as well as from FTI RAs. Requests for certificate revocation from other parties may be supported by the FTI CA.

### 4.9.3 Procedure for Revocation Request

The FTI CA shall revoke certificates upon receipt of sufficient evidence of compromise or loss of the subscriber's corresponding private key. 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). Where subscribers use hardware tokens, but excluding PIV-I certificates, revocation is optional (though still recommended) if all the following conditions are met:

- the revocation request was not for key compromise;
- the hardware token does not permit the user to export the signature private key;
- the Subscriber surrendered the token to the PKI;
- the token was zeroized or destroyed promptly upon surrender;
- the token has been protected from malicious use between surrender and zeroization or destruction.

For PIV-I and in all other cases not identified above, revocation of the certificates is mandatory.

If the FTI CA determines that a private key used to authorize the issuance of one or more certificates may have been compromised, it shall verify that all certificates directly or indirectly

authorized by that private key since the date of actual or suspected compromise were appropriately issued; if it cannot so verify, it shall revoke those certificates.

If the FTI CA determines that revocation is required, it shall revoke the associated certificate and places the certificate on the CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

FTI CA shall collect and destroy PIV-I Cards from Subscribers whenever the cards are no longer valid, whenever possible. FTI CA shall record destruction of PIV-I Cards.

### 4.9.4 Revocation Request Grace Period

The revocation request grace period is the time available to the subscriber within which the subscriber or the STRAC Bridge CA must make a revocation request after reasons for revocation have been identified.

In the case of key compromise, FTI CA Subscribers and the STRAC Bridge CA are required to request revocation within one hour. For all other reasons, FTI CA subscribers and the STRAC Bridge CA are required to request revocation within 24 hours.

### 4.9.5 Time within which CA must Process the Revocation Request

The FTI CA 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 validated within two hours of CRL issuance. Revocation requests validated within two hours of CRL issuance shall be processed before the following CRL is published.

### 4.9.6 Revocation Checking Requirements for Relying Parties

No stipulation.

### 4.9.7 CRL Issuance Frequency

For this CP, CRL issuance encompasses both CRL generation and publication.

For the FTI CA, the interval between CRLs shall not exceed the period indicated in the table below. CRLs may be issued more frequently than specified below.

**Table 2 CRL Issuance Frequency**

| Assurance Level | Maximum Interval for Routine CRL Issuance |
|---|---|
| Rudimentary | No stipulation |
| Basic | 24 hours |
| Medium (all policies) | 24 hours |
| PIV-I Card Authentication | 24 hours |

### 4.9.8 Maximum Latency of CRLs

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

Note: If pre-generation of CRLs is implemented, the thisUpdate field will be the date of generation. The nextUpdate value will be beyond the date of planned publication.

### 4.9.9 On-line Revocation/Status Checking Availability

On-line revocation/status checking is supported by the FTI CA, and the latency of certificate status information distributed on-line by the FTI CA must meet or exceed the requirements for CRL issuance stated in 4.9.7.

For PIV-I certificates, FTI CA shall support on-line status checking via OCSP [RFC 6960].

### 4.9.10 On-line Revocation Checking Requirements

No stipulation.

### 4.9.11 Other Forms of Revocation Advertisements Available

FTI 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 FTI 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

When a FTI CA Subscriber's certificate is revoked because of compromise, or suspected compromise, of a private key, a CRL must be issued as specified below:

| Assurance Level | Maximum Latency for Emergency CRL Issuance |
|---|---|
| Rudimentary | No stipulation |
| Basic | 24 hours after notification |
| Medium (all policies) | 18 hours after notification |
| PIV-I Card Authentication | 18 hours after notification |

### 4.9.13 Circumstances for Suspension and Restoration

FTI CA 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 provide details as specified in sections 4.9.14, 4.9.15, and 4.9.16.

Practice Note: Certificate suspension should only be used in circumstances where there is a reasonable possibility that the certificate will need to be restored Additionally, a certificate must be permanently revoked if it meets the circumstances stated in Section 4.9.1.

.

### 4.9.14 Who can Request Suspension and Restoration

Personnel authorized to request suspension and restoration of a certificate must be identified.

### 4.9.15 Procedure for Suspension and Restoration Requests

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." Restored certificate serial numbers must not be present on the next full CRL published by the CA.

Practice Note: A certificate is considered restored only if its status at the time of CRL generation is neither suspended nor revoked.

A request to suspend or restore a certificate must include:

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

If a CA or CMS product conducts certificate suspensions and restorations in an automated fashion (*e.g.*, without a formal request outlined above), the circumstances or parameters associated with those automated suspensions and restorations must be documented in the CPS.

If a subscriber is requesting restoration of their suspended certificate, the identity of the subscriber must be re-established before restoring the certificate. The subscriber's identity may be re-established using processes defined in Section 3.2.3.1, through the use of biometrics on file, or by the use of another private signature key of equivalent or greater assurance level issued to the subscriber.

The private key associated with any suspended certificate must not be used to authenticate the identity of the certificate subject.

### 4.9.16 Limits on Suspension Period

No stipulation.

## *4.10 CERTIFICATE STATUS SERVICES*

No stipulation.

### 4.10.1 Operational Characteristics

No stipulation.

### 4.10.2 Service Availability

No stipulation.

### 4.10.3 Optional Features

No stipulation.

## *4.11 END OF SUBSCRIPTION*

No stipulation.

## *4.12 KEY ESCROW & RECOVERY*

No stipulation.

### 4.12.1 Key Escrow and Recovery Policy and Practices

FTI CA does not escrow Private Keys.

When implemented, key recovery requirements must be documented in a Key Recovery Policy (KRP). The KRP may be a separate document or may be combined with the CP.

Under no circumstances will a subscriber signature key be held in trust by a third party.

### 4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

# 5. FACILITY MANAGEMENT & OPERATIONS CONTROLS

## *5.1 PHYSICAL CONTROLS*

All CA equipment including CA cryptographic modules shall be protected from unauthorized access at all times.

All the physical control requirements specified below apply equally to the FTI CA, CMSs, and any remote workstations used to administer the FTI CA except where specifically noted.

### 5.1.1 Site Location & Construction

The location and construction of the facility housing the FTI CA equipment, as well as sites housing remote workstations used to administer the FTI CA shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security

locks, and intrusion sensors, shall provide robust protection against unauthorized access to the FTI CA equipment and records.

### 5.1.2 Physical Access

#### *5.1.2.1 Physical Access for CA Equipment*

The FTI CA equipment, to include remote workstations used to administer the FTI CA, shall always be protected from unauthorized access. The security mechanisms shall be commensurate with the level of threat in the equipment environment. Since the FTI CA must plan to issue certificates at all levels of assurance up to and including Medium Hardware, it shall be operated and controlled on the presumption that it will be issuing at least one Medium Hardware Assurance certificate.

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

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

In addition to those requirements, the following requirements shall apply to Medium or Medium Hardware assurance certificates:

- Ensure manual or electronic monitoring for unauthorized intrusion at all times
- Ensure an access log is maintained and inspected periodically
- Require two person physical access control to both the cryptographic module and computer systems

Removable cryptographic modules, activation information used to access or enable cryptographic modules, and other sensitive CA equipment shall be placed in secure containers when not in use. Activation data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module or removable hardware associated with remote workstations used to administer the CA.

A security check of the facility housing the FTI CA equipment or remote workstations used to administer the CA (operating at the Basic Assurance level or higher) 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 FTI CA, that all equipment other than the repository is shut down);
- Any security containers are properly secured;
- Physical security systems (e.g., door locks, vent covers) are functioning properly; and
- The area is secured against unauthorized access.

A person or group of persons shall be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each

instance shall be maintained. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

#### *5.1.2.2 Physical Access for RA Equipment*

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

#### *5.1.2.3 Physical Access for CSS Equipment*

Physical access control requirements for CSS equipment (if implemented), shall meet the CA physical access requirements specified in 5.1.2.1.

#### *5.1.2.4 Physical Access for CMS Equipment*

Physical access control requirements for CMS equipment containing a PIV-I Content Signing key shall meet the CA physical access requirements specified in 5.1.2.1.

### 5.1.3 Power and Air Conditioning

The FTI CA (operating at the Basic Assurance level or higher) shall have backup capability sufficient to automatically lock out input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. The FTI CA shall employ appropriate mechanisms to ensure availability of repositories as specified in Section 2.2.1.

### 5.1.4 Water Exposures

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

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

### 5.1.5 Fire Prevention & Protection

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

### 5.1.6 Media Storage

FTI CA media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic). Sensitive FTI CA media shall be stored so as to protect it from 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

For the FTI CA operating at the Basic Assurance level or higher, full system backups sufficient to recover from system failure shall be made on a periodic schedule. Backups are to be performed and stored off-site not less than once per week. At least one full backup copy shall be stored at an off-site location separate from the FTI 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 FTI CA.

## *5.2 PROCEDURAL CONTROLS*

### 5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for all uses of the FTI CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion. An auditable record must be created identifying when personnel are added or removed from a trusted role, as well as who added or removed them from the role. The individual who authorized the role assignment, or any series of role assignments over a given period of time, must also be traceable via audit and archive records.

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

1. *Administrator* – authorized to install, configure, and maintain the CA; establish and maintain system accounts; configure profiles or templates and audit parameters; establish and maintain user accounts; and generate component keys.

2. *Officer* – authorized to register new subscribers, request, approve, or perform certificate issuance, revocations, and/or verify the identity of subscribers and accuracy of information included in certificates.

3. *Auditor* – authorized to review, maintain, and archive audit logs, and perform or oversee internal compliance audits to ensure that the CA is operated in accordance with its CPS.

4. *Operator* – authorized to perform system backup and recovery.

Administrators do not issue certificates to subscribers.

The roles required for each level of assurance are identified in Section 5.2.4. Separation of duties shall comply with 5.2.4, and requirements for two person control with 5.2.2, regardless of the titles and numbers of Trusted Roles.

### 5.2.2 Number of Persons Required per Task

Only one person is required per task for CAs operating at the Rudimentary and Basic Levels of Assurance.

Two or more persons are required for CAs operating at the Medium (all policies) Level of Assurance for the following tasks:

- CA key generation;
- CA signing key activation;
- CA private key backup.

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

Physical access to the CAs does not constitute a task as defined in this section. Therefore, two-person physical access control may be attained as required in Section 5.1.2.1.

### 5.2.3 Identification and Authentication for Each Role

At all assurance levels other than Rudimentary, 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 Separation of Roles

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

Requirements for the separation of roles, and limitations on use of procedural mechanisms to implement role separation, are described below for each level of assurance:

| Assurance Level | Role Separation Rules |
|---|---|
| Rudimentary | No stipulation |
| Basic | Individual personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume more than one role; however, no one individual shall assume both the Officer and Administrator roles. This may be enforced procedurally. No individual shall be assigned more than one identity. |
| Medium (all policies) | Individual personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may only assume one of the |

| | |
|---|---|
| | Officer, Administrator, and Auditor roles, but any individual may assume the Operator role. The CA, CMS, and RA software and hardware shall identify and authenticate its users and shall ensure that no user identity can assume both an Administrator and an Officer role, assume both the Administrator and Auditor roles, and assume both the Auditor and Officer roles. No individual shall have more than one identity. |
| PIV-I Card Authentication | Individual personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Role separation duties follow the requirements for Medium assurance above. |

## *5.3 PERSONNEL CONTROLS*

### 5.3.1 Background, Qualifications, Experience, & Security Clearance Requirements

The FTI CA shall identify at least one individual or group responsible and accountable for the operation of the CA.

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity. For the FTI CA, 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.

### 5.3.2 Background Check Procedures

FTI 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 consistent with Executive Order 12968 August 1995 or later, or an equivalent level of investigation and adjudication.

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

### 5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the FTI CA shall receive comprehensive training in all operational duties they are expected to perform, including disaster recovery and business continuity procedures.

In addition, personnel performing duties with respect to the operation of the FTI CA shall receive comprehensive training, or demonstrate competence, in the following areas:

- CA/RA security principles and mechanisms;
- All PKI software versions in use on the CA system.

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

### 5.3.4 Retraining Frequency & Requirements

Individuals responsible for PKI roles shall be aware of any changes in the FTI 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 FTI CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

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

### 5.3.5 Job Rotation Frequency & Sequence

No stipulation.

### 5.3.6 Sanctions for Unauthorized Actions

The FTI PKI Management Authority and FTI PKIPA shall take appropriate actions where personnel have performed actions involving the FTI CA or its repository not authorized in this CP, the FTI CPS, or other procedures published by the FTI PKI Management Authority and FTI PKIPA.

### 5.3.7 Independent Contractor Requirements

Contractor personnel employed to perform functions pertaining to the FTI CA shall meet the personnel requirements set forth in this CP.

### 5.3.8 Documentation Supplied to Personnel

For the FTI CA, documentation sufficient to define duties and procedures for each trusted role, including this CP and the FTI CPS, shall be provided to the personnel filling that role. Specifically, individuals serving trusted roles will receive the relevant CP and CPS.

## *5.4 AUDIT LOGGING PROCEDURES*

The objective of audit log processing is to review all actions to ensure they are made by authorized parties and for legitimate reasons.

At a minimum, audit records must be generated for all applicable events identified in Section 5.4.1 of this policy and must be available during audit reviews and third-party audits. If the FTI CA is operated in a virtual environment, audit records must be generated for all applicable events on application software and all system software layers.

Where possible, the security audit logs must be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism must be used. All security audit logs, both electronic and non-electronic, must be retained and made available during compliance audits. Implementation and documentation of automated tools must describe how relevant events and anomalies are recorded.

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.

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

When Key escrow and Recovery is supported, 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.

Real-time alerts are neither required nor prohibited by this policy.

### 5.4.1 Types of Events Recorded

A message from any source received by the FTI CA requesting an action related to the operational state of the CA is an auditable event. 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,
- A success or failure indicator, where appropriate
- The identity of the operator of the FTI CA that caused the event,

Detailed audit requirements are listed in the table below according to the level of assurance. All security auditing capabilities of the FTI CA operating system and CA applications required by this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. Where events cannot be automatically recorded, the CA shall implement manual procedures to satisfy this requirement.

| Auditable Event | Rudimentary | Basic | Medium (all policies) & PIV-I Card Authentication | |
|---|---|---|---|---|
| **SECURITY AUDIT** | | | | |
| Any changes to the Audit parameters, e.g., audit frequency, type of event audited | | X | X | |
| Any attempt to delete or modify the Audit logs | | X | X | |
| Obtaining a third-party time-stamp | | X | X | |
| **IDENTIFICATION AND AUTHENTICATION** | | | | |
| Successful and unsuccessful attempts to assume a role | | X | X | |
| The value of *maximum authentication attempts* is changed | | X | X | |
| The number of unsuccessful authentication attempts exceeds the *maximum authentication attempts* during user login | | X | X | |

| Auditable Event | Rudimentary | Basic | Medium (all policies) & PIV-I Card Authentication | |
|---|---|---|---|---|
| An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts | | X | X | |
| An Administrator changes the type of authenticator, e.g., from password to biometrics | | X | X | |
| **LOCAL DATA ENTRY** | | | | |
| All security-relevant data that is entered in the system | | X | X | |
| **REMOTE DATA ENTRY** | | | | |
| All security-relevant messages that are received by the system | | X | X | |
| **DATA EXPORT AND OUTPUT** | | | | |
| All successful and unsuccessful requests for confidential and security-relevant information | | X | X | |
| **KEY GENERATION** | | | | |
| Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys) | X | X | X | |
| **PRIVATE KEY LOAD AND STORAGE** | | | | |
| The loading of Component private keys | X | X | X | |
| All access to certificate subject private keys retained within the CA for key recovery purposes | X | X | X | |
| **TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE** | | | | |
| All changes to the trusted public keys, including additions and deletions | X | X | X | |
| **SECRET KEY STORAGE** | | | | |
| The manual entry of secret keys used for authentication | | | X | |

| Auditable Event | Rudimentary | Basic | Medium (all policies) & PIV-I Card Authentication | |
|---|---|---|---|---|
| **PRIVATE AND SECRET KEY EXPORT** | | | | |
| The export of private and secret keys (keys used for a single session or message are excluded) | X | X | X | |
| **CERTIFICATE REGISTRATION** | | | | |
| All certificate requests | X | X | X | |
| | | | | |
| | | | | |
| **CERTIFICATE REGISTRATION** | | | | |
| All certificate revocation requests | | X | X | |
| **CERTIFICATE STATUS CHANGE** | | | | |
| All records, including request, authorization, approval and execution related to certificate status changes request, authorization, approval and execution (e.g., revocation, suspension, or restoration) whether generated directly on the CA or generated by a related external system or process | | X | X | |
| **CA CONFIGURATION** | | | | |
| Any security-relevant changes to the configuration of the CA | | X | X | |
| **ACCOUNT ADMINISTRATION** | | | | |
| Roles and users are added or deleted | X | X | X | |
| The access control privileges of a user account or a role are modified | X | X | X | |
| **CERTIFICATE PROFILE MANAGEMENT** | | | | |
| All changes to the certificate profile | X | X | X | |
| **REVOCATION PROFILE MANAGEMENT** | | | | |
| All changes to the revocation profile | | X | X | |
| **CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT** | | | | |
| All changes to the certificate revocation list profile | | X | X | |

| Auditable Event | Rudimentary | Basic | Medium (all policies) & PIV-I Card Authentication | |
|---|---|---|---|---|
| **MISCELLANEOUS** | | | | |
| Record of an individual being added or removed from a Trusted Role, and who added or removed them from the role | X | X | X | |
| Designation of personnel for multiparty control | | | X | |
| Installation of the Operating System | | X | X | |
| Installation of the CA | | X | X | |
| Installing hardware cryptographic modules | | | X | |
| Removing hardware cryptographic modules | | | X | |
| Destruction of cryptographic modules | | X | X | |
| System Startup | | X | X | |
| Logon Attempts to CA Applications | | X | X | |
| Receipt of Hardware/Software | | X | X | |
| Attempts to set passwords | | X | X | |
| Attempts to modify passwords | | X | X | |
| Backing up CA internal database | | X | X | |
| Restoring CA internal database | | X | X | |
| File manipulation (e.g., creation, renaming, moving) | | | X | |
| Posting of any material to a repository | | | X | |
| Access to CA internal database | | | X | |
| All certificate compromise notification requests | | X | X | |
| Loading tokens with certificates | | | X | |
| Shipment of Tokens | | | X | |
| Zeroizing tokens | | X | X | |
| All records of authentication, authorization, recovery, agreement and delivery of key management keys to a key recovery requestor. | X | X | X | |
| Re-key of the CA | X | X | X | |

| Auditable Event | Rudimentary | Basic | Medium (all policies) & PIV-I Card Authentication | |
|---|---|---|---|---|
| Configuration changes to the CA server involving: | | | | |
| - Hardware | | X | X | |
| - Software | | X | X | |
| - Operating System | | X | X | |
| - Patches | | X | X | |
| - Security Profiles | | X | X | |
| **PHYSICAL ACCESS / SITE SECURITY** | | | | |
| Personnel Access to room housing CA | | | X | |
| Access to the CA server | | | X | |
| Known or suspected violations of physical security | | X | X | |
| **ANOMALIES** | | | | |
| Software Error conditions | | X | X | |
| Software check integrity failures | | X | X | |
| Receipt of improper message | | | X | |
| Misrouted messages | | | X | |
| Network attacks (suspected or confirmed) | | X | X | |
| Equipment failure | X | X | X | |
| Electrical power outages | | | X | |
| Uninterruptible Power Supply (UPS) failure | | | X | |
| Obvious and significant network service or access failures | | | X | |
| Violations of Certificate Policy | X | X | X | |
| Violations of Certification Practice Statement | X | X | X | |
| Resetting Operating System clock | | X | X | |

### 5.4.2 Frequency of Processing Log

Audit logs shall be reviewed in accordance with the table below. 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 log. Examples of irregularities include discontinuities in the logs and loss of audit data. Actions taken as a result of these reviews shall be documented.

For the FTI CA, the FTI PKI Management Authority shall explain all significant events in an audit log summary.

| Assurance Level | Review Audit Log |
|---|---|
| Rudimentary | Only required for cause |
| Basic | At least once per month |
| Medium (all policies) | At least once per month<br>Statistically significant set of security audit data generated by the FTI CA since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity |
| PIV-I Card Authentication | At least once per month<br>Statistically significant set of security audit data generated by the FTI CA since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity |

For the FTI CA, a representative sample (as defined by the FTI PKIPA) of security audit data generated by the FTI CA since the last review shall be examined.

### 5.4.3 Retention Period for Audit Logs

For Medium and Medium Hardware Assurance, audit logs shall be retained on-site until reviewed, as well as being retained in the manner described below. For Rudimentary and Basic Assurance, audit logs shall be retained on-site for at least two months or until reviewed, as well as being retained in the manner described below. The individual who removes audit logs from the FTI CA system shall be an official different from the individuals who, in combination, command the FTI CA signature key.

### 5.4.4 Protection of Audit Logs

FTI CA system configuration and procedures must be implemented together to ensure that:

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

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

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

#### 5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up at least monthly. A copy of the audit log shall be sent off-site on a monthly basis.

#### 5.4.6 Audit Collection System (internal vs. external)

The audit log collection system may or may not be external to the FTI CA system. Automated audit processes shall be invoked at system (or application) startup, and cease only at system (or application) shutdown. Audit collection systems must 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 must be suspended until the problem is remedied.

#### 5.4.7 Notification to Event-Causing Subject

This CP imposes no requirement to provide notice that an event was audited to the individual, organization, device, or application that caused the event.

#### 5.4.8 Vulnerability Assessments

For FTI CA, personnel shall perform routine assessments for evidence of malicious activity.

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

### *5.5 RECORDS ARCHIVE*

FTI CA archive records shall be sufficiently detailed as to verify that the FTI CA was properly operated as well as verify the validity of any certificate (including those revoked or expired) issued by the FTI CA. The FTI CA shall comply with respective records retention policies in accordance applicable laws.

#### 5.5.1 Types of Events Archived

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

| Data to Be Archived | Rudimentary | Basic | Medium (all policies) & PIV-I Card Authentication |
|---|---|---|---|
| CA accreditation (if applicable) | X | X | X |
| Certificate Policy | X | X | X |
| Certification Practice Statement | X | X | X |
| Contractual obligations | X | X | X |
| Other agreements concerning operations of the CA | X | X | X |
| System and equipment configuration | X | X | X |
| Modifications and updates to system or configuration | X | X | X |
| Certificate requests | X | X | X |
| Revocation requests | X | X | X |
| Subscriber identity Authentication data as per Section 3.2.3 | | X | X |
| Documentation of receipt and acceptance of certificates (if applicable) | | X | X |
| Subscriber Agreements | | X | X |
| Documentation of receipt of tokens | | X | X |
| All certificates issued or published | X | X | X |
| Record of CA Re-key | X | X | X |
| All CRLs issued and/or published | | X | X |
| Other data or applications to verify archive contents | | X | X |
| Compliance Auditor reports | | X | X |

| Data to Be Archived | Rudimentary | Basic | Medium (all policies) & PIV-I Card Authentication |
|---|---|---|---|
| Any changes to the Audit parameters, e.g., audit frequency, type of event audited | | X | X |
| Any attempt to delete or modify the Audit logs | | X | X |
| Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys) | X | X | X |
| All access to certificate subject private keys retained within the CA for key recovery purposes | X | X | X |
| All changes to the trusted public keys, including additions and deletions | X | X | X |
| The export of private and secret keys (keys used for a single session or message are excluded) | X | X | X |
| The approval or rejection of a certificate status change request | | X | X |
| Record of an individual being added or removed from a trusted role, and who added or removed them from the role | X | X | X |

| Data to Be Archived | Rudimentary | Basic | Medium (all policies) & PIV-I Card Authentication |
|---|---|---|---|
| Evidence of qualification for Trusted Agents and the associated validity period(s) for which they are authorized to act as Trusted Agents | | X | 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 | X |
| Destruction of cryptographic modules | | X | X |
| All certificate compromise notifications | | X | X |
| Remedial action taken as a result of violations of physical security | | X | X |
| Violations of Certificate Policy | X | X | X |
| Violations of Certification Practice Statement | X | X | X |

### 5.5.2 Retention Period for Archive

The FTI CA shall comply with records retention policies in accordance with applicable law. The minimum retention period for these records, described in the table below, is intended only to facilitate the operation of the FTI CA:

| Assurance Level | Minimum Retention Period |
|---|---|
| Rudimentary | 7 Years & 6 Months |
| Basic | 7 Years & 6 Months |
| Medium (all policies) | 10 Years & 6 Months |
| PIV-I Card Authentication | 10 Years & 6 Months |

### 5.5.3 Protection of Archive

No unauthorized user shall be permitted to write to or delete the archive. For the FTI CA, archived records may be moved to another medium when authorized by the FTI PKI Management Authority Program Manager. The contents of the archive shall not be released except in accordance with Sections 9.3 & 9.4. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. Archive media shall be stored in a safe, secure storage facility separate from the FTI CA itself.

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site. Applications required to process the archive data shall also be maintained for a period determined by the FTI PKI Management Authority.

### 5.5.4 Archive Backup Procedures

The FTI CA shall back up its archive records. It adheres to the Archive Backup Procedures defined in the FTI CPS.

### 5.5.5 Requirements for Time-Stamping of Records

CA archive records shall be automatically time-stamped as they are created. The CPS shall describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

### 5.5.6 Archive Collection System (internal or external)

Archive data may be collected in any expedient manner but must be documented in the associated CPS.

### 5.5.7 Procedures to Obtain & Verify Archive Information

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

The contents of the archive shall not be released except as determined by the FTI PKI Policy Authority for the FTI CA or as required by law. Records of individual transactions may be

released upon request of any subscribers involved in the transaction or their legally recognized agents.

## *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 for certificate signing purposes. 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 CRLs that cover certificates signed with that key, then the old key must be retained and protected.

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

For the FTI CA, key changeover procedures will establish key rollover certificates where a certificate containing the old public key will be signed by the new private key, and a certificate containing the new public key will be signed by the old private key. If cross certified with the STRAC BCA, the FTI CA must be able to continue to interoperate with the STRAC BCA after the STRAC BCA performs a key rollover, whether or not the STRAC BCA DN is changed.

## *5.7 COMPROMISE & DISASTER RECOVERY*

### 5.7.1 Incident and Compromise Handling Procedures

If any of the following cases occur, the FTI PKI Management Authority shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the FTI CPS:

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

In the event of an incident as described above, the Entity shall notify the SPKIPA within 24 hours of incident discovery, along with preliminary remediation analysis.

Within 10 business days of incident resolution, the FTI CA shall post a notice on its public web page identifying the incident and provide notification to the SPKIPA. The public notice shall include the following:

1. Which CA components were affected by the incident
2. The CA's interpretation of the incident.
3. Who is impacted by the incident

4. When the incident was discovered
5. A complete list of all certificates that were either issued erroneously or not compliant with the CP/CPS as a result of the incident
6. A statement that the incident has been fully remediated

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

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

When computing resources, software, and/or data are corrupted, the FTI CA 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 4.9.7, Table 1.
- 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 FTI CA shall post a notice on its web page identifying the incident and provide notification to the SPKIPA. See Section 5.7.1 for contents of the notice.

### 5.7.3 CA Private Key Compromise Procedures

If the FTI CA signature keys are compromised or lost (such that compromise is possible even though not certain):

- The FTI PKI Policy Authority shall be notified;
- A new FTI CA key pair shall be generated by the FTI CA in accordance with procedures set forth in the FTI CPS; and
- New FTI CA certificates shall be issued to Subscribers also in accordance with the FTI CPS.
- If the CA distributes its key in a self-signed certificate, the new self-signed certificate shall be distributed as specified in Section 6.1.4.

The FTI PKI Management Authority shall also investigate and report to the FTI PKI Policy Authority what caused the compromise or loss, and what measures have been taken to preclude recurrence.

The FTI CA shall post a notice on its web page describing the compromise. See Section 5.7.1 for contents of the notice.

### 5.7.4 Business Continuity Capabilities after a Disaster

The FTI CA repository system shall be deployed so as to provide 24 hour, 365 day per year availability. The FTI PKI Management Authority shall implement features to provide high levels of repository reliability.

The FTI CA operations shall be designed to restore full service within 24 hours of primary system failure.

The FTI PKI Management Authority shall at the earliest feasible time securely advise the FTI PKI Policy Authority and all affiliated and member entities of the FTI CA in the event of a disaster where the FTI CA installation is physically damaged and all copies of the FTI CA signature keys are destroyed.

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

## *5.8 CA & RA TERMINATION*

In the event of termination of the FTI CA operation, certificates signed by the FTI CA shall be revoked and the FTI PKI Policy Authority shall advise entities that have entered into MOAs with the FTI PKI Policy Authority that FTI CA operation has terminated so they may revoke certificates they have issued to the FTI CA. Prior to FTI CA termination, the FTI PKI Management Authority shall provide all archived data to an archival facility. Any issued certificates that have not expired shall be revoked and a final long term CRL with a nextUpdate time past the validity period of all issued certificates shall be generated. This final CRL shall be available for all relying parties until the validity period of all issued certificates has past. Once the last CRL has been issued, the private signing key(s) of the FTI CA will be destroyed.

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

Whenever possible, FTI shall notify the SPKIPA at least two weeks prior to the termination of any CA operated by FTI cross certified with the STRAC Bridge CA. For emergency termination, CAs shall follow the notification procedures in Section 5.7.

# 6. TECHNICAL SECURITY CONTROLS

## *6.1 KEY PAIR GENERATION & INSTALLATION*

### 6.1.1 Key Pair Generation

#### *6.1.1.1 CA Key Pair Generation*

Cryptographic keying material used to sign certificates, CRLs or status information by the FTI CA shall be generated in FIPS 140 validated cryptographic modules or modules validated under equivalent international standards.

For the FTI CA, the modules shall meet or exceed Security Level requirements specified in Section 6.2.1. Multiparty control is required for CA key pair generation for the FTI CA operating at the Medium, or Medium Hardware levels of assurance, as specified in Section 6.2.2.

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

For Medium Hardware and Medium Assurance, 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.

#### *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 approved method or equivalent international standard.

For PIV-I Hardware certificates, to be used for digital signatures and/or authentication, and PIV-I Card Authentication certificates, subscriber key generation shall be performed on hardware tokens that meet the requirements of Appendix A. For all other certificates at the Medium Hardware assurance levels, subscriber key generation shall be performed using a validated hardware cryptographic module. For Medium and Basic assurance, either validated software or validated hardware cryptographic modules shall be used for key generation.

#### *6.1.1.3 CSS Key Pair Generation*

Cryptographic keying material used by CSSs to sign status information must be generated in [FIPS 140] validated cryptographic modules as specified in Section 6.2.1.

#### *6.1.1.4 PIV-I Content Signing Key Pair Generation*

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

### 6.1.2 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 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.
    - For shared key applications, organizational identities, and network devices, see also Section 3.2.

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

### 6.1.3 Public Key Delivery to Certificate Issuer

For CAs operating at the Basic, Medium, or Medium Hardware level of assurance, the following requirements apply:

- 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.

For Rudimentary Assurance, no stipulation.

### 6.1.4 CA Public Key Delivery to Relying Parties

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

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

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

### 6.1.5 Key Sizes

This CP requires use of RSA PKCS #1, RSASSA-PSS, or ECDSA signatures; additional restrictions on key sizes and hash algorithms are detailed below. Certificates must contain 2048-, 3072-, or 4096-bit RSA keys, or 256- or 384-bit elliptic curve keys.

| | CA certificates that expire on or before December 31, 2030 | CA certificates that expire after December 31, 2030 |
|---|---|---|

| | | |
|---|---|---|
| Minimum Key Size | RSA: 2048<br>Elliptic Curve: 256 | RSA: 3072<br>Elliptic Curve: 256 |
| Hash Algorithm | SHA-256, SHA-384, or SHA-512 | SHA-256, SHA-384, or SHA-512 |

| | Subscriber certificates that expire on or before December 31, 2030 | Subscriber certificates that expire after December 31, 2030 |
|---|---|---|
| Minimum Key Size | RSA: 2048<br>Elliptic Curve: 256 | RSA: 3072<br>Elliptic Curve: 256 |
| Hash Algorithm | SHA-256, SHA-384, or SHA-512 | SHA-256, SHA-384, or SHA-512 |

All Subscriber certificates associated with PIV-I must contain public keys and algorithms that conform to [NIST SP 800-78].

Use of Transport Layer Security (TLS) or another protocol providing similar security to accomplish any of the requirements of this CP must 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. After December 31, 2030, use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP must require at a minimum AES (128 bits) or equivalent for the symmetric key, and at least 3072-bit RSA or equivalent for the asymmetric keys.

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

### 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.

Parameter quality checking (including primality testing for prime numbers) shall be performed in accordance with FIPS 186; additional tests may be specified by the FTI PKI Policy Authority.

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

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

FTI CA certificates issued to CAs shall set two key usage bits: *cRLSign* and/or *keyCertSign*. Where the subject signs OCSP responses, the certificate may also set the *digitalSignature* and/or *nonRepudiation* bits.

Subscriber certificates shall assert key usages based on the intended application of the key pair. In particular, certificates to be used for digital signatures (including authentication) shall set the *digitalSignature* and/or *nonRepudiation* bits. Certificates to be used for key or data encryption shall set the *keyEncipherment* and/or *dataEncipherment* bits. Certificates to be used for key agreement shall set the *keyAgreement* bit.

Entities are encouraged at all levels of assurance to issue Subscribers two key pairs, one for key management and one for digital signature and authentication.

For FTI CA End Entity certificates, the Extended Key Usage extension shall always be present and shall not contain anyExtendedKeyUsage {2.5.29.37.0}. Extended Key Usage OIDs shall be consistent with key usage bits asserted.

If a certificate is used for authentication of ephemeral keys, the Key Usage bit in the certificate shall assert the DigitalSignature bit and may or may not assert Key Encryption and Key Agreement depending on the public key in the certificate.

PIV-I Content Signing certificates shall include an extended key usage of *id-fpki-pivi-content-signing* (see [PIV-I Profile]).

## *6.2 PRIVATE KEY PROTECTION & CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS*

### 6.2.1 Cryptographic Module Standards & Controls

The relevant standard for cryptographic modules is FIPS 140, *Security Requirements for Cryptographic Modules*.

Cryptographic modules must be minimally validated to the FIPS 140 level identified in this section. The FTI PKI Policy Authority reserves the right to review technical documentation associated with any cryptographic modules under consideration for use by the FTI CA.

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

| Assurance Level | CA, CMS & CSS | Subscriber | RA |
|---|---|---|---|
| **Rudimentary** | Level 1 (Hardware or Software) | N/A | Level 1 (Hardware or Software) |
| **Basic** | Level 2 (Hardware or Software) | Level 1 | Level 1 (Hardware or Software) |

| | | | |
|---|---|---|---|
| **Medium** | Level 3 (Hardware) | Level 1 | Level 2 (Hardware) |
| **PIV-I Card Authentication** | Level 3 (Hardware) | Level 2 (Hardware) | Level 2 (Hardware) |
| **Medium Hardware** | Level 3 (Hardware) | Level 2 (Hardware) | Level 2 (Hardware) |

PIV-I Cards are PKI tokens that have private keys associated with certificates asserting policies mapped to PIV-I hardware or PIV-I-cardAuth. PIV-I Cards shall 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 SPKIPA/SPKIMA. On an annual basis, for each PCI configuration used (as defined by the FIPS 201 Evaluation Program), one populated, representative sample PIV-I Card shall be submitted to the SPKIMA for testing by the FIPS 201 Evaluation Program.

For hardware tokens associated with PIV-I, see Appendix A for additional requirements.

#### *6.2.1.1 Custodial Subscriber Key Stores*

Custodial Subscriber Key Stores hold keys for a number of Subscriber certificates in one location. When a collection of private keys for Subscriber certificates are held in a single location, there is a higher risk associated with compromise of that cryptographic module than that of a single Subscriber.

Cryptographic modules for Custodial Subscriber Key Stores at the Rudimentary Assurance Level shall be no less than FIPS 140 Level 1 (Hardware or Software). For all other levels, the cryptographic module shall be no less than FIPS 140 Level 2 Hardware.

In addition, authentication to the Cryptographic Device in order to activate the private key associated with a given certificate shall require authentication commensurate with the assurance level of the certificate.

### 6.2.2 Private Key Multi-Person Control

Use of the FTI CA private signing key shall require action by multiple persons as set forth in Section 5.2.2 of this CP.

### 6.2.3 Private Key Escrow

#### *6.2.3.1 Escrow of FTI CA private signature key*

Under no circumstances shall a FTI CA signature key used to sign certificates or CRLs be escrowed.

#### *6.2.3.2 Escrow of CA encryption keys*

No stipulation.

#### *6.2.3.3 Escrow of Subscriber private signature keys*

Subscriber private signature keys shall not be escrowed.

#### *6.2.3.4 Escrow of Subscriber private encryption and dual use keys*

Subscriber private dual use keys shall not be escrowed. If a device has a separate key management key certificate, the key management private key may 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 FTI CA Private Signature Key*

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

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

#### *6.2.4.2 Backup of subscriber private signature key*

At the Medium Hardware assurance levels, Subscriber private signature keys may not be backed up or copied.

At the Rudimentary, Basic, or Medium levels of assurance, Subscriber private signature keys may be backed up or copied, but must be held in the Subscriber's control.

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

#### *6.2.4.3 Backup of Subscriber Key Management Private Keys*

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

#### *6.2.4.4 Backup of CSS Private Key*

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

#### *6.2.4.5 Backup of PIV-I Content Signing Key*

Backup of PIV-I Content Signing private signature keys may be required to facilitate disaster recovery. In which case, PIV-I Content Signing private signature keys shall be backed up under multi-person control.

#### *6.2.4.6 Backup of Device Private Keys*

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

### 6.2.5 Private Key Archival

Private signature keys shall not be archived.

For private encryption keys (key management or key transport), no stipulation.

### 6.2.6 Private Key Transfer into or from a Cryptographic Module

FTI 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 plain text 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 protected using a FIPS approved algorithm and at a bit strength commensurate with the key being transported; 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 Keys

For the FTI CA operating at the Medium or Medium Hardware level of assurance, CA signing key activation requires multiparty control as specified in Section 5.2.2.

In addition, PIV-I Content Signing key activation requires the same multiparty control established for the CA (see Section 5.2.2).

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

For PIV-I Card Authentication, mediumDevice and mediumDeviceHardware user activation of the private key is not required.

For certificates issued under the mediumDevice and mediumDeviceHardware policy OIDs, the device may be configured to activate its private key without requiring its human sponsor or authorized administrator to authenticate to the cryptographic token, provided that appropriate physical and logical access controls are implemented for the device and its cryptographic token. The strength of the security controls shall be commensurate with the level of threat in the device's environment, and shall protect the device's hardware, software, and the cryptographic token and its activation data from compromise.

#### 6.2.9 Methods of Deactivating Private Keys

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

#### 6.2.10 Method of Destroying Private Keys

Individuals in trusted roles shall destroy CA, RA and status server (e.g., OCSP server) private signature keys when they are no longer needed. Subscriber private signature keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, this can be overwriting the data. For hardware cryptographic modules, this will likely be executing a "zeroize" command. Physical destruction of hardware is not required.

#### 6.2.11 Cryptographic Module Rating

See Section 6.2.1.

### *6.3 OTHER ASPECTS OF KEY MANAGEMENT*

#### 6.3.1 Public Key Archival

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

#### 6.3.2 Certificate Operational Periods/Key Usage Periods

A 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 key pair must expire before the end of that key pair's usage period.

| Key | Private Key | Certificate |
|---|---|---|
| Root CA certificate (self-signed) | 30 years | 30 years |
| Intermediate/Signing CA certificate | 10 years | 10 years |
| Subscriber Authentication | 3 years | 3 years |

| | | |
|---|---|---|
| Subscriber Signature | 3 years | 3 years |
| Subscriber Encryption | Unrestricted | 3 years |
| PIV-I Card Authentication | 3 years | 3 years |
| PIV-I Content Signing | 3 years | 9 years* |
| Code Signing | 3 years | 8 years |
| OCSP Responder | 3 years | 120 days |
| Device | 3 years | 3 years |

* Expiration of the Content Signing certificate must be later than the expiration of the Subscriber certificates on the same PIV-I credential. Subscriber certificates on a PIV-I card must expire no later than the expiration date of the PIV-I hardware token on which they reside. The validity period of the subscriber certificate must not exceed the routine re-key Identity Requirements as specified in Section 3.3.1.

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

## *6.4 ACTIVATION DATA*

### 6.4.1 Activation Data Generation & Installation

The activation data used to unlock FTI 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 FTI CA uses passwords as activation data for the CA signing key, at a minimum the activation data shall be changed upon CA re-key.

### 6.4.2 Activation Data Protection

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

- memorized
- biometric in nature,
- contained within an organizationally approved device or software tool (*e.g.*, password manager) that leverages encryption commensurate with the bit-strength of the key it activates, or
- physically recorded and secured at the level of assurance associated with the activation of the cryptographic module, and stored separately from the cryptographic module.

Practice Note: For [FIPS 140] level 2 and higher modules, the protection mechanism should include an ability to temporarily lock the account, or terminate the application, after a

predetermined number of failed login attempts to protect against repeated guessing attacks, as set forth in the respective CP.

### 6.4.3 Other Aspects of Activation Data

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

## *6.5 COMPUTER SECURITY CONTROLS*

### 6.5.1 Specific Computer Security Technical Requirements

For FTI CA, the computer security functions listed below are required. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. FTI CA and its ancillary parts shall include the following functionality (in a VME, these functions are applicable to both the VM and hypervisor):

- 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.

For Certificate Status Servers, the computer security functions listed below are required (in a VME, these functions are applicable to both the VM and hypervisor):

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- enforce domain integrity boundaries for security critical processes; and
- support recovery from key or system failure.

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

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

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

### 6.5.2 Computer Security Rating

No Stipulation.

## *6.6 LIFE-CYCLE SECURITY CONTROLS*

### 6.6.1 System Development Controls

The System Development Controls for FTI CA at the Basic Assurance level and above are as follows:

- For commercial off-the-shelf software, the software shall be designed and developed under a formal, documented development methodology.
- For hardware and software developed specifically for a particular CA, the applicant shall demonstrate that security requirements were achieved through a combination of software verification & validation, structured development approach, and controlled development environment.
- Where open source software has been utilized, the applicant shall demonstrate that security requirements were achieved through software verification & validation and structured development/life-cycle management.
- Hardware and software procured to operate the CA shall be purchased and shipped in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).
- The CA hardware and software, including the VME hypervisor, shall be dedicated to operating and supporting the CA (*i.e.*, the systems and services dedicated to the issuance and management of certificates). There shall be no other applications; hardware devices, network connections, or component software installed which are not part of the CA operation. In a VME, a single hypervisor may support multiple CAs and their supporting systems, provided all systems have comparable security controls and are dedicated to the support of the CA.
- In a VME, all VM systems must operate in the same security zone as the CA.
- Proper care shall be taken to prevent malicious software from being loaded onto the CA equipment. 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 be installed by trusted and trained personnel in a defined manner.

### 6.6.2 Security Management Controls

The configuration of the FTI CA system as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the FTI CA software or configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance of the FTI CA system. The

FTI CA software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use.

#### 6.6.3 Life Cycle Security Ratings

No stipulation.

### *6.7 NETWORK SECURITY CONTROLS*

Network security controls shall be employed to protect the FTI CA. Networking equipment shall turn off unused network ports and services.

FTI CA, RAs, CMSs, repositories, remote workstations used to administer the CA, and certificate status servers 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 CA shall establish connection with a remote workstation used to administer the CA only after successful mutual authentication of the remote workstation at a level of assurance commensurate with that of the CA. 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 remote workstation to CA communications, to include CA boundary control devices, must incorporate data integrity and confidentiality services. The remote workstation to CA network communications must be encrypted and must not be vulnerable to replay or machine-in-the-middle attacks.

Once the connection is established between the remote workstation and the CA or boundary control devices the CA must 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*

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

## 7. CERTIFICATE, CARL/CRL, AND OCSP PROFILES FORMAT

### *7.1 CERTIFICATE PROFILE*

#### 7.1.1 Version Numbers

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

#### 7.1.2 Certificate Extensions

For all CAs, use of standard certificate extensions shall comply with [RFC 5280], unless otherwise specified in the appropriate certificate profile in [FTI PKI-Prof].

Certificates issued by the FTI CA shall comply with *FTI Public Key Infrastructure X.509 Certificate and CRL Extensions Profile* [FTI PKI-Prof].

PIV-I Certificates shall comply with [PIV-I Profile].

> *Practice Note: If the FTI CA issues PIV-I certificates, any associated CSS certificates will also comply with [PIV-I Profile]*

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

### 7.1.3 Algorithm Object Identifiers

Certificates issued by FTI CA must identify the signature algorithm using one of the following OIDs:

| Signature Algorithm | Object Identifier |
|---|---|
| sha256WithRSAEncryption | { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 } (1.2.840.113549.1.1.11) |
| sha384WithRSAEncryption | { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12 } (1.2.840.113549.1.1.12) |
| sha512WithRSAEncryption | { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13 } (1.2.840.113549.1.1.13) |
| id-RSASSA-PSS | { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10 } (1.2.840.113549.1.1.10) |
| ecdsa-with-SHA256 | { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2 } (1.2.840.10045.4.3.2) |
| ecdsa-with-SHA384 | { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 } (1.2.840.10045.4.3.3 |

| | |
|---|---|
| ecdsa-with-SHA512 | { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4 } (1.2.840.10045.4.3.4 |

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

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

Certificates must use the following OIDs to identify the algorithm associated with the subject key:

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

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

| Curve | Object Identifier |
|---|---|
| ansip256r1 | { iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7 } (1.2.840.10045.3.1.7) |

| | |
|---|---|
| ansip384r1 | { iso(1) identified-organization(3) certicom(132) curve(0) 34 } (1.3.132.0.34) |

For PIV-I, signature algorithms are limited to those identified by NIST SP 800-78.

### 7.1.4 Name Forms

Where required as set forth in Section 3.1.1, the subject and issuer fields of the base certificate shall be populated with an X.500 Distinguished Name. Distinguished names shall be composed of standard attribute types, such as those identified in [RFC5280].

### 7.1.5 Name Constraints

No stipulation.

### 7.1.6 Certificate Policy Object Identifier

All certificates issued by the FTI CA shall include a certificate policies extension asserting the OID(s) appropriate to the level of assurance with which it was issued. See Section 1.2 for specific OIDs. The FTI CA will comply with the FTI PKI Profile [FTI PKI-Prof].

### 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 Subordinate CA certificates *inhibitPolicyMapping,* skip certs must be set to 0. For cross-certificates *inhibitPolicyMapping*, skip certs must be set appropriately. When *requireExplicitPolicy* is included skip certs must be set to 0.

Practice Note: *inhibitPolicyMapping*, skip certs is usually set to 1 in a cross-certificate issued to a Bridge so it can do another cross-certificate mapping to its CA members. A skip certs value of 2 may be required to allow transitive trust if that Bridge issues a cross-certificate to a CA that also allows mapping. If transitive trust is not the desired behavior other constraints such as name constraints may be required to control appropriate results.

### 7.1.8 Policy Qualifiers Syntax & Semantics

Certificates issued by the FTI CA may contain policy qualifiers identified in [RFC 6818].

### 7.1.9 Processing Semantics for the Critical Certificate Policy Extension

No stipulation.

#### 7.1.10 Inhibit Any Policy Extension

The FTI CA may assert InhibitAnyPolicy in CA certificates. When present, this extension should be marked as noncritical* to support legacy applications that cannot process InhibitAnyPolicy. Skip Certs shall be set to 0.

*Note: The recommended criticality setting is different from RFC 5280.

### *7.2 CRL PROFILE*

#### 7.2.1 Version Numbers

The FTI CA shall issue X.509 version two (2) CRLs.

#### 7.2.2 CRL Entry Extensions

For the FTI CA, CRL extensions shall conform to [FTI PKI-PROF].

### *7.3 OCSP PROFILE*

If implemented, Certificate Status Servers (CSS) shall sign responses using algorithms designated for CRL signing.

## 8. COMPLIANCE AUDIT & OTHER ASSESSMENTS

FTI CA shall have a compliance audit mechanism in place to ensure that the requirements of their CP/CPS are being implemented and enforced. The FTI PKI Policy Authority shall be responsible for ensuring audits are conducted for all PKI functions regardless of how or by whom the PKI components are managed and operated.

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

If the FTI CA is cross-certified with the STRAC BCA and the STRAC BCA is cross-certified with the Federal BCA, the FTI CA will participate as requested by the STRAC BCA in an annual review by the Federal PKIPA to ensure STRAC BCA policies and operations remain consistent with the policy mappings in the certificate issued to the STRAC BCA by the Federal BCA.

### *8.1 FREQUENCY OF AUDIT OR ASSESSMENTS*

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

The compliance audit of FTI CAs and RAs shall be carried out in accordance with requirements specified in the *FPKI Annual Review Requirements* document in effect at the time of the audit.

There is no audit requirement for CAs and RAs operating at the Rudimentary level of assurance.

The FTI CA has the right to require periodic and aperiodic compliance audits or inspections of subordinate CA or RA operations to validate that the subordinate entities are operating in accordance with the security practices and procedures described in their respective CPS. Further, the FTI PKI Policy Authority has the right to require aperiodic compliance audits of FTI CA under this CP. The FTI PKI Policy Authority 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. At the time of the audit, the FTI CA compliance auditor must be thoroughly familiar with requirements which the FTI PKI Policy Authority imposes on the issuance and management of FTI CA subscriber and CA certificates. The compliance auditor must perform such compliance audits as a regular ongoing business activity.

## *8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY*

For the FTI CA, the compliance auditor either shall be a private firm, that is independent from the entity being audited, or it shall be sufficiently organizationally separated from that entity to provide an unbiased, independent evaluation. To insure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining the entity's CA Facility or certificate practices statement.

The FTI PKI Policy Authority shall determine whether a compliance auditor meets this requirement.

## *8.4 TOPICS COVERED BY ASSESSMENT*

The compliance audit of the FTI CA shall verify that the FTI PKI Management Authority is implementing all provisions of a CPS approved by the FTI PKI Policy Authority consistent with this CP.

The purpose of a compliance audit of the FTI PKI shall be to verify that the requirements of this CP are met as applicable, as well as the requirements of any MOAs between the FTI PKI and any other PKI. 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 shall be considered in the sample. The samples shall vary on an annual basis.

A full compliance audit for the FTI CA covers all aspects within the scope identified above.

## *8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY*

When the FTI CA compliance auditor finds a discrepancy between how the FTI CA is designed or is being operated or maintained, and the requirements of the applicable FTI CA CP, any applicable MOAs, or the applicable CPS, the following actions shall be performed:

- The compliance auditor shall document the discrepancy;

- The compliance auditor shall notify the responsible party promptly;
- The FTI PKI Policy Authority shall determine what further notifications or actions are necessary to meet the requirements of the relevant CP, CPS, and any relevant MOA provisions. The FTI PKI Policy Authority shall proceed to make such notifications and take such actions without delay.

### *8.6 COMMUNICATION OF RESULTS*

On an annual basis, the FTI PKIMA shall submit an audit compliance package to the FTI PKI Policy Authority. This audit package shall be prepared in accordance with the *FPKI Annual Review Requirements* document as it exists at the time of the submittal and shall include an assertion from the FTI PKIMA that all PKI components have been audited - including any components that may be separately managed and operated. The package shall identify the versions of the CP and CPS used in the assessment. Additionally, where necessary, the results shall be communicated as set forth in Section 8.5 above. If the FTI CA is cross-certified to the STRAC Bridge CA, it shall meet the STRAC Bridge CA requirements for providing evidence of audit compliance.

## 9. OTHER BUSINESS & LEGAL MATTERS

### *9.1 FEES*

The FTI PKI Policy Authority reserves the right to charge fees for services provided by the FTI PKI.

#### 9.1.1 Certificate Issuance/Renewal Fees

No Stipulation.

#### 9.1.2 Certificate Access Fees

No Stipulation.

#### 9.1.3 Revocation or Status Information Access Fee

No Stipulation.

#### 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 by a Relying Party of any certificates issued by the FTI CA. Rather, Relying Parties shall determine the extent to which they wish to use certificates issued under this CP.

#### 9.2.1 Insurance Coverage

No stipulation.

#### 9.2.2 Other Assets

No stipulation.

#### 9.2.3 Insurance/warranty Coverage for End-Entities

No stipulation.

### *9.3 CONFIDENTIALITY OF BUSINESS INFORMATION*

Public access to FTI CA information shall be determined by the FTI PKIPA.

#### 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

No stipulation.

### *9.4 PRIVACY OF PERSONAL INFORMATION*

#### 9.4.1 Privacy Plan

The FTI PKI Management Authority shall protect any repository information not intended for public dissemination or modification.

#### 9.4.2 Information treated as Private

Collection of PII shall be limited to the minimum necessary to validate the identity of the subscriber, unless authorized in writing by the subscriber. Minimum PII necessary to validate the identity of the subscriber may include attributes that correlate identity evidence to authoritative sources. The RA shall provide explicit notice to the subscriber regarding the purpose for collecting and maintaining a record of the PII necessary for identity proofing and the consequences for not providing the information. PII collected for identity proofing purposes shall not be used for any other purpose.

#### 9.4.3 Information not deemed Private

For the FTI CA, 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 shall be protected to ensure confidentiality and integrity. In the event FTI terminates PKI activities, it shall be responsible for disposing of or destroying sensitive information, including PII, in a secure manner, and maintaining its protection from unauthorized access until destruction.

#### 9.4.5 Notice and Consent to use Private Information

No stipulation.

#### 9.4.6 Disclosure Pursuant to Judicial/Administrative Process

No stipulation.

#### 9.4.7 Other Information Disclosure Circumstances

None.

### *9.5 INTELLECTUAL PROPERTY RIGHTS*

No stipulation.

### *9.6 REPRESENTATIONS & WARRANTIES*

The obligations described below pertain to the FTI CA (and, by implication, the FTI PKI Management Authority), and to Principal or other CAs, which either interoperate with the FTI CA or are in a trust chain up to a Principal CA that interoperates with the FTI CA. The obligations applying to Principal or other CAs pertain to their activities as issuers of certificates. Further, if the FTI CA cross-certifies with the STRAC Bridge CA, the obligations described below focus on the FTI CA's obligations affecting interoperability with the STRAC Bridge CA.

#### 9.6.1 CA Representations and Warranties

FTI CA certificates are issued and revoked at the sole discretion of the FTI PKI Policy Authority.

The FTI PKIPA will determine for itself whether this certificate policy meets its legal and policy requirements.

FTI represents and warrants that, to its knowledge, (1) the material information reflected in the certificates issued by the FTI CA is correct, and (2) the FTI CA is operated in material conformance with this CP.

Neither FTI, nor the FTI CA, nor the FTI CA PA or MA or RA makes any representation or warranty, other than those explicitly stated in this Certificate Policy or in separate agreements, regarding the products or services provided by the FTI CA or its associated PKI and personnel.

For PIV-I, FTI shall maintain agreements with Affiliated Organizations concerning the obligations pertaining to authorizing affiliation with Subscribers of PIV-I certificates.

### 9.6.2 RA Representations and Warranties

Neither FTI, nor the FTI CA, nor the FTI CA PA or MA or RA makes any representation or warranty, other than those explicitly stated in this Certificate Policy or in separate agreements, that the information in a cross-certificate or subscriber certificate is accurate.

### 9.6.3 Subscriber Representations and Warranties

For Medium and Medium Hardware Assurance levels, a Subscriber shall be required to sign a document (Subscriber Agreement) containing the requirements the Subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate. For Basic Assurance level, the Subscriber shall be required to acknowledge his or her obligations respecting protection of the private key and use of the certificate before being issued the certificate.

Subscribers of FTI at Basic and Medium Assurance Levels shall agree to the following:

- Accurately represent themselves in all communications with the PKI authorities.
- Protect their private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements and local procedures.
- Promptly notify the FTI CA upon suspicion of loss or compromise of their private keys. Such notification shall be made directly or indirectly through mechanisms consistent with the FTI CPS.
- Abide by all the terms, conditions, and restrictions levied on the use of their private keys and certificates.

### 9.6.4 Relying Parties Representations and Warranties

Neither FTI, nor the FTI CA, nor the PA or MA or RA for the FTI CA makes any representation or warranty, other than those explicitly stated in this Certificate Policy or in separate agreements, about the use by Relying Parties of certificates issued by the FTI CA.

### 9.6.5 Representations and Warranties of Affiliated Organizations

Neither FTI, nor the FTI CA, nor the FTI CA PA or MA or RA makes any representation or warranty, other than those explicitly stated in this Certificate Policy or in separate agreements, with regard to affiliated organizations. Affiliated Organizations shall authorize the affiliation of subscribers with the organization, and shall inform FTI CA of any severance of affiliation with any current subscriber.

### 9.6.6 Representations and Warranties of other Participants

Neither FTI, nor the FTI CA, nor the FTI CA PA or MA or RA makes any representation or warranty, other than those explicitly stated in this Certificate Policy or in separate agreements, with regard to other participants.

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

- The Third-Party Requestor must protect Subscribers' recovered key(s) from compromise. The Third-Party 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.
- The Third-Party Requestor must destroy or surrender Subscribers' keys when no longer required (*i.e.*, when the data has been recovered).
- The Third-Party Requestor must request and use the Subscriber's escrowed key(s) only to recover Subscriber's data they are authorized to access.
- The Third-Party Requestor must accurately represent themselves to all entities during any key recovery service.
- When the request is made, the Third-Party 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 Third-Party Requestor sends a digitally signed request using the credential issued by the Entity PKI at the same or higher assurance level as the key being recovered).
- The Third-Party Requestor 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 organization policies relating to protection and release of the recovered key. Such agreement should include the following attestations attestation:
    - 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 only for the stated purpose(s),
    - Third Party Requestor will protect the recovered key from unauthorized access. When no longer required, the Third Party Requestor shall either destroy the key(s) and inform the organization of destruction per organization requirements, or return any recovered key(s) stored on hardware to the organization.

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*

FTI, the FTI CA, the FTI PKIPA, and the FTI PKIMA disclaim all warranties, whether express or implied, including any warranty of merchantability or fitness for a particular purpose. The FTI CA, the FTI PKIPA, and the FTI PKIMA endeavor with best efforts to meet all of their responsibilities under this CP. Their success at meeting these responsibilities is evidenced by the cross-certification, based upon any required audit investigations, of the FTI CA by other CAs.

## *9.8 LIMITATIONS OF LIABILITY*

Neither FTI, nor the FTI CA, nor its PA or MA or RA shall be liable for loss of income, goodwill, or other special or consequential damages. Neither FTI, nor the FTI CA, nor its PA or MA or RA shall be liable for any direct or indirect damages of any kind arising out of or related to the FTI CA CP or the FTI CA CPS. Neither FTI, nor the FTI CA, nor its PA or MA or RA shall be liable for any losses incurred from directly or indirectly using its services.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL FTI, THE FTI CA, OR ITS PA OR MA OR RA BE LIABLE FOR ANY DIRECT OR INDIRECT DAMAGES OF ANY KIND, INCLUDING CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE, OR OTHER DAMAGES WHATSOEVER ARISING OUT OF OR RELATED TO THIS CP OR THE FTI CA CPS, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DISCLAIMERS OF REPRESENTATIONS, WARRANTIES, AND CONDITIONS AND THE LIMITATIONS OF LIABILITY IN THIS CP CONSTITUTE AN ESSENTIAL PART OF THIS CP. ALL SUBSCRIBERS, RELYING PARTIES, AND OTHER PERSONS, ENTITIES, AND ORGANIZATIONS ACKNOWLEDGE THAT BUT FOR THESE DISCLAIMERS OF REPRESENTATIONS, WARRANTIES, AND CONDITIONS AND LIMITATIONS OF LIABILITY, FTI AND THE FTI CA WOULD NOT ISSUE CERTIFICATE(S) TO SUBSCRIBERS AND NEITHER FTI NOR THE FTI CA NOR ANY INDEPENDENT THIRD-PARTY REGISTRATION AUTHORITIES OPERATING UNDER THE FTI CA, NOR ANY RESELLERS, CO-MARKETERS, OR ANY CONTRACTORS, SUBCONTRACTORS, DISTRIBUTORS, AGENTS, SUPPLIERS, EMPLOYEES, OR DIRECTORS OF ANY OF THE FOREGOING WOULD PROVIDE SERVICES IN RESPECT TO CERTIFICATE SERVICES AND THAT THESE PROVISIONS PROVIDE FOR A REASONABLE ALLOCATION OF RISK.

## *9.9 INDEMNITIES*

### 9.9.1 Indemnification by Subscribers

To the extent permitted by applicable law, each FTI CA Subscriber shall indemnify FTI, the FTI CA, the FTI PKIPA or the FTI PKIMA and their contractors, agents, assigns, employees, officers, and directors from and against any third party claims, liabilities, damages, costs and expenses (including reasonable attorney's fees), relating to or arising out of any certificates issued by the FTI CA, for:

- Falsehood or misrepresentation of fact by the Subscriber in the applicable documentation.

- Failure by the Subscriber to disclose a material fact in any applicable contractual agreement, if the misrepresentation or omission was made negligently or with intent to deceive any party,
- The Subscriber's failure to protect the Subscriber private key or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber private key, or
- The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

Any applicable contractual agreement between a Subscriber and FTI, the FTI CA, the FTI PKIPA or the FTI PKIMA may include additional indemnity obligations.

#### 9.9.2 Indemnification by Relying Parties

To the extent permitted by applicable law, each Relying Party shall indemnify FTI, the FTI CA, the FTI PKIPA or the FTI PKIMA and its contractors, agents, assigns, employees, officers, and directors from and against any third party claims, liabilities, damages, costs and expenses (including reasonable attorney's fees), relating to or arising out of use of or reliance by the Relying Party on any certificates issued by the FTI CA where:

- the certificate at the time of the use or reliance was expired, revoked, or unvalidated by the Relying Party);
- the Relying Party's reliance on a certificate was unreasonable, under the circumstances; or
- the Relying Party failed to check the status of the certificate on which it relied to determine if the certificate was expired or revoked.

Any applicable contractual agreement between a Relying Party and F, the FTI CA, the FTI PKIPA or the FTI PKIMA may include additional indemnity obligations.

## *9.10 TERM & TERMINATION*

#### 9.10.1 Term

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

#### 9.10.2 Termination

Termination of this CP is at the discretion of the FTI 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 & COMMUNICATIONS WITH PARTICIPANTS*

Other than as defined in this CP (including in Sec. 1.3.1.1 regarding changes to infrastructure), no other notices are stipulated.

## *9.12 AMENDMENTS*

### 9.12.1 Procedure for Amendment

If it cross-certifies with the STRAC Bridge CA, the FTI CA must amend this CP as required by the STRAC Bridge PKIPA to ensure that this CP maps to the STRAC Bridge CA CP, as it may be revised from time to time.

### 9.12.2 Notification Mechanism and Period

No stipulation.

### 9.12.3 Circumstances under which OID must be changed

OIDs will be changed if the FTI PKI Policy Authority determines that a change in the CP reduces the level of assurance provided.

## *9.13 DISPUTE RESOLUTION PROVISIONS*

The FTI PKIPA shall facilitate resolution of disputes regarding the use of certificates issued under this CP or otherwise arising out of this CP. For disputes with other parties, such as Subscribers, Relying Parties, and Affiliated Organizations, the dispute resolution mechanisms described in the Subscriber Agreement, the Relying Party Agreement, and the Affiliated Organization Agreement, respectively, apply. If the FTI CA cross-certifies with the STRAC Bridge CA, FTI CA disputes with STRAC, the STRAC Bridge CA, the STRAC Bridge PKIPA, or the STRAC Bridge PKIMA, or otherwise arising under the STRAC Bridge CA CP will be resolved pursuant to the terms of the STRAC Bridge CA CP.

## *9.14 GOVERNING LAW*

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

## *9.15 COMPLIANCE WITH APPLICABLE LAW*

The FTI CA is 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.

### 9.16.4 Enforcement (Attorney Fees/Waiver of Rights)

Failure by any person to enforce a provision of this CP will not be deemed a waiver of future enforcement of that or any other provision.

### 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. |
| CIMC | Certificate Issuing and Management Components Family of Protection Profiles, version 1.0, October 31, 2001. |
| FIPS 140 | Security Requirements for Cryptographic Modules, FIPS 140-3. https://csrc.nist.gov/publications/detail/fips/140/3/final |
| FIPS 186-2 | Digital Signature Standard, January 27, 2000. http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf |
| FIPS 201 | Personal Identity Verification (PIV) of Federal Employees and Contractors 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 |
| FPKI-E | Federal PKI Version 1 Technical Specifications: Part E-X.509 Certificate and CRL Extensions Profile, 7 July 1997 http://csrs.nist.gov/pki/FPKI7-10.DOC |
| FPKI-Prof | Federal PKI X.509 Certificate and CRL Extensions Profile |
| ISO9594-8 | Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 1997. |
| ITMRA | 40 U.S.C. 1452, Information Technology Management Reform Act of 1996. http://www4.law.cornell.edu/uscode/40/1452.html |
| NAG69C | Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999. |
| NIST SP 800-63-3 | Digital Identity Guidelines. https://csrc.nist.gov/publications/detail/sp/800-63/3/final |
| NIST SP 800-73 | Interfaces for Personal Identity Verification https://csrc.nist.gov/publications/detail/sp/800-73/4/final |
| NIST SP 800-76 | Biometric Specifications for Personal Identity Verification, NIST Special Publication 800-76 https://csrc.nist.gov/publications/detail/sp/800-76/2/final |
| NIST SP 800-78 | Cryptographic Algorithms and Key Sizes for Personal Identity Verification, NIST Special Publication 800-78 https://csrc.nist.gov/publications/detail/sp/800-78/4/final |

| | |
|---|---|
| NSD42 | National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990. http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt (redacted version) |
| NS4005 | NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997. |
| NS4009 | NSTISSI 4009, National Information Systems Security Glossary, January 1999. |
| PIV-I Profile | X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards, Date: April 23 2010, Reference Link: http://www.idmanagement.gov/fpkipa/documents/pivi_certificate_crl_profile.pdf |
| PKCS#1 | Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications https://www.ietf.org/rfc/rfc3447.txt |
| PKCS#12 | Personal Information Exchange Syntax https://www.ietf.org/rfc/rfc7290.txt |
| RFC 3647 | Certificate Policy and Certification Practices Framework, Chokhani and Ford, Sabett, Merrill, and Wu, November 2003. |
| RFC 5280 | Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile |
| RFC 6818 | Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile |
| RFC 6960 | X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP |

# 11. ACRONYMS & ABBREVIATIONS

| | |
|---|---|
| AID | Application Identifier |
| CA | Certification Authority |
| CARL | Certificate Authority Revocation List |
| CMS | Card Management System |
| COMSEC | Communications Security |
| CP | Certificate Policy |
| CPS | Certification Practice Statement |
| CRL | Certificate Revocation List |
| CSOR | Computer Security Object Registry |
| DDS | Data Decryption Server |
| DN | Distinguished Name |
| DSA | Digital Signature Algorithm |
| DSS | Digital Signature Standard |
| ERC | Enhanced Reliability Check |
| FAR | Federal Acquisition Regulations |
| FBCA | Federal Bridge Certification Authority |
| FPKIMA | Federal Public Key Infrastructure Management Authority |
| FED-STD | Federal Standard |
| FIPS PUB | (US) Federal Information Processing Standard Publication |
| FPKI | Federal Public Key Infrastructure |
| FPKI-E | Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile |
| FPKISC | Federal PKI Steering Committee |
| FPKIPA | Federal PKI Policy Authority |
| FTI | Foundation for Trusted Identity |
| FTI CA | FTI Certification Authority |
| FTI PKIMA | FTI Public Key Infrastructure Management Authority |
| FTI PKIPA | FTI Public Key Infrastructure Policy Authority |
| GPEA | Government Paperwork Elimination Act of 1998 |

| | |
|---|---|
| GSA | General Services Administration |
| HTTP | HyperText Transfer Protocol |
| HSM | Hardware Security Module |
| IETF | Internet Engineering Task Force |
| ISO | International Organization for Standardization |
| ISSO | Information Systems Security Officer |
| ITU | International Telecommunications Union |
| ITU-T | International Telecommunications Union – Telecommunications Sector |
| ITU-TSS | International Telecommunications Union – Telecommunications System Sector |
| KED | Key Escrow Database |
| KRA | Key Recovery Agent |
| KRO | Key Recovery Officer |
| KRP | Key Recovery Policy |
| KRPS | Key Recovery Practice Statement |
| LDAP | Lightweight Directory Access Protocol |
| MOA | Memorandum of Agreement (as used in the context of this CP, between an Entity and the FPKIPA allowing interoperation between the FBCA and Entity Principal CA) |
| 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-I | Personal Identity Verification – Interoperable |
| PKCS | Public Key Certificate Standard |
| PKI | Public Key Infrastructure |
| PKIX | Public Key Infrastructure X.509 |

| | |
|---|---|
| RA | Registration Authority |
| RFC | Request For Comments |
| RSA | Rivest-Shamir-Adleman (encryption algorithm) |
| SHA-1 | Secure Hash Algorithm, Version 1 |
| S/MIME | Secure Multipurpose Internet Mail Extension |
| STRAC | Southwest Texas Regional Advisory Council |
| SSL | Secure Sockets Layer |
| TSDM | Trusted Software Development Methodology |
| UPN | User Principal Name |
| UPS | Uninterrupted Power Supply |
| URL | Uniform Resource Locator |
| U.S.C. | United States Code |
| UUID | Universally Unique Identifier (defined by RFC 4122) |
| VME | Virtual Machine Environment |
| 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). |
| Affiliated Organization | Organizations that authorize affiliation with Subscribers of PIV-I certificates. |
| Affiliated Organization Agreement | An agreement setting out the responsibilities of an Affiliated Organization related to its affiliation with a Subscriber in possession of a certificate issued by a CA. The FTI CA Affiliated Organization Agreement is called “The FTI CA Sponsoring Organization Agreement” and is posted at https://pki.fti.org/fti_CA/documents. |
| 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 FTI PKIPA or comparable Entity body as having the authority to verify the association of attributes to an identity. |
| Audit | Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009] |
| Audit Data | Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"] |

| | |
|---|---|
| Authenticate | To confirm the identity of an entity when that identity is presented. |
| Authentication | Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009] |
| Backup | Copy of files and programs made to facilitate recovery if necessary. [NS4009] |
| Binding | Process of associating two related elements of information. [NS4009] |
| Biometric | A physical or behavioral characteristic of a human being. |
| Certificate | A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]. As used in this CP, the term “Certificate” refers to certificates that expressly reference the OID of this CP in the “Certificate Policies” field of an X.509 v.3 certificate. |
| Certification Authority (CA) | An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs. |
| Certification Authority Revocation List (CARL) | A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates, that have been revoked. |
| CA Facility | The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation. |
| Certificate | A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber’s public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG] |
| Certificate Management Authority (CMA) | A Certification Authority or a Registration Authority. |
| Certification Authority Software | Key Management and cryptographic software used to manage certificates issued to subscribers. |

| | |
|---|---|
| Certificate Policy (CP) | A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications. |
| Certification Practice Statement (CPS) | A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services). |
| Certificate-Related Information | Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates. |
| Certificate Revocation List (CRL) | A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date. |
| Certificate Status Authority | A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate. |
| Client (application) | A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server. |
| Common Criteria | A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products. |
| Compromise | Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009] |
| Computer Security Objects Registry (CSOR) | Computer Security Objects Registry operated by the National Institute of Standards and Technology. |

| | |
|---|---|
| Confidentiality | Assurance that information is not disclosed to unauthorized entities or processes. [NS4009] |
| Cross-Certificate | A certificate used to establish a trust relationship between two Certification Authorities. |
| Cryptographic Module | The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401] |
| Cryptoperiod | Time span during which each key setting remains in effect. [NS4009] |
| Data Integrity | Assurance that the data are unchanged from creation to reception. |
| Digital Signature | The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made. |
| Dual Use Certificate | A certificate that is intended for use with both digital signature and data encryption services. |
| Duration | A field within a certificate which is composed of two subfields; "date of issue" and "date of next issue". |
| E-commerce | The use of network technology (especially the internet) to buy or sell goods and services. |
| Encrypted Network | A network that is protected from outside access by NSA approved high-grade (Type I) cryptography. Examples are SIPRNET and TOP SECRET networks. |
| Encryption Certificate | A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes. |
| End-entity | Relying Parties and Subscribers. |
| Entity | For the purposes of this document, "Entity" refers to an organization, corporation, community of interest, or government agency with operational control of a CA. |

| | |
|---|---|
| Entity CA | A CA that acts on behalf of an Entity, and is under the operational control of an Entity. The Entity may be an organization, corporation, or community of interest. For the Federal Government, an Entity may be any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Federal Government. |
| FBCA Management Authority (FPKIMA) | The Federal Public Key Infrastructure Management Authority is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the Federal Bridge Certification Authority. |
| Federal Public Key Infrastructure Policy Authority (FPKI PA) | The FPKIPA is a federal government body responsible for setting, implementing, and administering policy decisions regarding inter Entity PKI interoperability that uses the FBCA. |
| Firewall | Gateway that limits access between networks in accordance with local security policy. [NS4009] |
| FTI Public Key Infrastructure X.509 Certificate and CRL Extensions Profile [FTI PKI-Prof] | [FTI PKI-Prof] describes the profiles defined in the most current versions of the *Federal Public Key Infrastructure X.509 Certificate and CRL Extensions Profile* [FPKI-Prof] and the *X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards* [PIV-I Prof], as they may be revised from time to time, up to the date of the latest version of the Certification Practice Statement for the STRAC Bridge Certification Authority (STRAC BCA) and the Participant Certification Authority (Participant CA), which typically is updated more frequently than the *X.509 Certificate Policy for the FTI Bridge Certification Authority ( FTI CA)* (this document). |
| FTI Public Key Infrastructure Management Authority | The FTI Public Key Infrastructure Management Authority is the body responsible for operating the FTI Certification Authority at the direction of the FTI Public Key Infrastructure Policy Authority. |
| FTI Public Key Infrastructure Policy Authority | The FTI Public Key Infrastructure Policy Authority is the organization responsible for setting, implementing, and administering policy decisions related to use of the FTI Certification Authority. The FTI Public Key Infrastructure Policy Authority directs the FTI Public Key Infrastructure Management Authority and may delegate work to it. |

| | |
|---|---|
| High Assurance Guard (HAG) | An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance. |
| Hypervisor | Computer software, firmware or hardware that creates and runs virtual machines. A hypervisor uses native execution to share and manage hardware, allowing for multiple environments which are isolated from one another, yet exist on the same physical machine. Also known as an isolation kernel or virtual machine monitor. |
| Information System Security Officer (ISSO) | Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, from design through disposal. [NS4009] |
| Inside threat | An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service. |
| Integrity | Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination. |
| Intellectual Property | Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation. |
| Intermediate CA | A CA that is subordinate to another CA, and has a CA subordinate to itself. |
| Key Escrow | A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"] |
| Key Exchange | The process of exchanging public keys in order to establish secure communications. |
| Key Generation Material | Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys. |

| | |
|---|---|
| Key Pair | Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key. |
| Key Recovery Policy (KRP) | A key recovery policy is a specialized form of administrative policy tuned to the protection and recovery of key management private keys (i.e. decryption keys) held in escrow. A key recovery policy addresses all aspects associated with the storage and recovery of key management certificates. |
| Key Recovery Practices Statement (KRPS) | A statement of the practices that a Key Recovery System employs in protecting and recovering key management private keys, in accordance with specific requirements (i.e., requirements specified in the KRP). |
| Local Registration Authority (LRA) | A Registration Authority with responsibility for a local community. |
| Memorandum of Agreement (MOA) | Agreement between the FTI PKIPA and an Entity allowing interoperability between the Entity Principal CA and the FTI CA. |
| Mission Support Information | Information that is important to the support of deployed and contingency forces. |
| Mutual Authentication | Occurs when parties at both ends of a communication activity authenticate each other (see authentication). |
| Naming Authority | An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain. |
| National Security System | Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA] |

| | |
|---|---|
| Non-Repudiation | Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established. |
| Object Identifier (OID) | A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI they are used to uniquely identify each of the seven policies and cryptographic algorithms supported. |
| Out-of-Band | Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online). |
| Outside Threat | An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service. |
| Physically Isolated Network | A network that is not connected to entities or systems outside a physically controlled space. |
| PKI Sponsor | 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) | The individual or group that is responsible for the creation and maintenance of Certificate Policies and Certification Practice Statements, and for ensuring that all Entity PKI components (e.g. CAs, CSSs, CMSs, RAs) are audited and operated in compliance with the entity PKI CP. The PMA evaluates non-domain policies for acceptance within the domain, and generally oversees and manages the PKI certificate policies. For the FTI CA, the PMA is the FTI PKIPA. |

| | |
|---|---|
| Principal CA | The Principal CA is a CA designated by an Entity to interoperate with the FTI CA. An Entity may designate multiple Principal CAs to interoperate with the FTI CA. |
| Privacy | Restricting access to subscriber or Relying Party information in accordance with Federal law and Entity policy. |
| Private Key | (1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret. |
| Public Key | (1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate. |
| Public Key Infrastructure (PKI) | A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates. |
| Registration Authority (RA) | An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA). |
| Re-key (a certificate) | To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key. |
| Relying Party | A person or Entity who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them. |
| Relying Party Agreement | An agreement setting out the Relying Party's responsibilities related to the use of certificates issued by a CA. The FTI CA Relying Party Agreement is posted at https://pki.fti.org/fti_CA/documents. |

| | |
|---|---|
| Remote Workstation | A workstation used to administer the CA, CMS, CSS and/or associated HSMs from a secure location outside the security perimeter of the equipment being administered. The secure location housing the Remote Workstation should be protected as a logical extension of the enclave in which the administered CA equipment resides. A remote workstation is not connected to the CA, CMS, CSS and/or HSM via a dedicated network.<br><br>Note: Reference Sections 5.1, 6.5, 6.6.1, and 6.7 for additional technical controls required of remote workstations. This term does not refer to consoles within the CA's security perimeter or to Registration Authority workstations. |
| Renew (a certificate) | The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate. |
| Repository | A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory. |
| Responsible Individual | A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor. |
| Revoke a Certificate | To prematurely end the operational period of a certificate effective at a specific date and time. |
| Risk | An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result. |
| Risk Tolerance | The level of risk an entity is willing to assume in order to achieve a potential desired result. |
| Root CA | In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain. |
| Server | A system entity that provides a service in response to requests from clients. |
| Signature Certificate | A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions. |
| Subordinate CA | In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA). |

| | |
|---|---|
| Subscriber | A Subscriber is an entity other than a CA 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 |
| Subscriber Agreement | An agreement setting out the Subscriber's responsibilities related to the possession and use of certificates issued by a CA. The FTI CA Subscriber Agreement is posted at https://pki.fti.org/fti_CA/documents. |
| Superior CA | In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA). |
| Supervised Remote Identity Proofing | A real-time identity proofing event where the RA/Trusted Agent is not in the same physical location as the applicant/subscriber. The RA/Trusted Agent controls a device which is utilized by the applicant/subscriber in order to ensure the remote identity proofing process employs physical, technical and procedural measures to provide sufficient confidence that the remote session can be considered equivalent to a physical, in-person identity proofing process. Supervised Remote Identity Proofing must meet the criteria specified in NIST SP 800-63A Section 5.3.3; and must have the capacity to capture an approved biometric when utilized for PIV-I credential issuance. |
| System Equipment Configuration | A comprehensive accounting of all system hardware and software types and settings. |
| System High | The highest security level supported by an information system. [NS4009] |
| Technical non-repudiation | The contribution public key mechanisms to the provision of technical evidence supporting a non-repudiation security service. |
| Threat | Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009] |
| Trust List | Collection of trusted certificates used by Relying Parties to authenticate other certificates. |

| | |
|---|---|
| Trusted Agent | Entity authorized to act as a representative of an Entity in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities. |
| Trusted Certificate | A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor". |
| Trusted Timestamp | A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time. |
| Trustworthy System | Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures. |
| Two-Person Control | Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements. [NS4009] |
| Update (a certificate) | The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate. |
| Virtual Machine Environment | An emulation of a computer system (in this case, a CA) that provides the functionality of a physical machine in a platform-independent environment. It consists of a host (virtual machine) and isolation kernel (hypervisor) and provides functionality needed to execute entire operating systems. At this time, allowed VMEs are limited to Hypervisor type virtual environments. Other technology, such as Docker Containers, is not permitted. |
| Zeroize | A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS1401] |

# APPENDIX A – PIV-INTEROPERABLE SMART CARD DEFINITION

The intent of PIV-I is to enable issuers to issue cards that are technically interoperable with Federal PIV Card and non-Federal PIV-I readers and applications, and that may be trusted for particular purposes through a decision of the Relying Party. Thus, reliance on PIV-I Cards requires compliance with technical specifications and specific trust elements. This appendix defines the specific requirements of a PIV-I Card. It relies heavily on relevant specifications from the National Institute of Standards and Technology (NIST).

The following requirements shall apply to PIV-I Cards:

1. To ensure interoperability with Federal systems, PIV-I Cards shall use a smart card platform that is on GSA's FIPS 201 Evaluation Program Approved Product List (APL) and uses the PIV application identifier (AID).
2. PIV-I Cards shall conform to [NIST SP 800-73[3]].
3. The mandatory X.509 Certificate for Authentication shall be issued under a policy that is cross certified with the FBCA PIV-I Hardware policy OID.
4. All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile].
5. PIV-I Cards shall contain an asymmetric X.509 Certificate for Card Authentication that:
    a. conforms to [PIV-I Profile];
    b. conforms to [NIST SP 800-73]; and
    c. is issued under the PIV-I Card Authentication policy.
6. PIV-I Cards shall contain an electronic representation (as specified in SP 800-73 and SP 800-76) of the Cardholder Facial Image printed on the card.
7. The X.509 Certificates for Digital Signature and Key Management described in [NIST SP 800-73] are optional for PIV-I Cards.
8. Visual distinction of a PIV-I Card from that of a Federal PIV Card is required to ensure no suggestion of attempting to create a fraudulent Federal PIV Card. At a minimum, images or logos on a PIV-I Card shall not be placed entirely within Zone 11, *Agency Seal*, as defined by [FIPS 201].
9. The PIV-I Card physical topography shall include, at a minimum, the following items on the front of the card:
    a. Cardholder facial image;
    b. Cardholder full name;
    c. Organizational Affiliation, if exists; otherwise the issuer of the card; and
    d. Card expiration date.
10. PIV-I Cards shall have an expiration date not to exceed 6 years of issuance.
11. Expiration of the PIV-I Card should not be later than expiration of PIV-I Content Signing certificate on the card.
12. The digital signature certificate that is used to sign objects on the PIV-I Card (e.g., CHUID, Security Object) shall contain a policy OID that has been mapped to the FBCA

[3] Special attention should be paid to UUID requirements for PIV-I.

PIV-I Content Signing policy OID. The PIV-I Content Signing certificate shall conform to [PIV-I Profile].

13. The PIV-I Content Signing certificate and corresponding private key shall be managed within a trusted Card Management System as defined by Appendix B.
14. At issuance, the RA shall activate and release the PIV-I Card to the subscriber only after a successful 1:1 biometric match of the applicant against the biometrics collected in Section 3.2.3.1.
15. PIV-I Cards may support card activation by the card management system to support card personalization and post-issuance card update. To activate the card for personalization or update, the card management system shall perform a challenge response protocol using cryptographic keys stored on the card in accordance with [SP800-73]. When cards are personalized, card management keys shall be set to be specific to each PIV-I Card. That is, each PIV-I Card shall contain a unique card management key. Card management keys shall meet the algorithm and key size requirements stated in Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification. [SP800-78]

# APPENDIX B – 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, 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 and 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.

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.