Entrust Datacard™
Trusted Identities | Secure Transactions

Entrust Managed Services
Non-Federal Identity (NFI)
Public Key Infrastructure
Certificate Policy

Version 1.6.4
December 8, 2016

This is a publicly releasable document that may be distributed without restriction.

Signature Page

Rusty Atkinson
VP, Customer Success

12/12/16

Entrust Managed Services
PKI Policy Authority

Date

Version 1.6.4
December 8, 2016

Revision History

Document Version	Document Date	Revision Details
1.0	April 24, 2009	Initial draft.
1.1	May 15, 2009	Align document more closely with FBCA CP
1.11	May 26, 2009	Align Section 5.3.1 with the FBCA CP and other minor corrections
1.12	June 09, 2009	Updates based upon comments from the FBCA CPWG mapping review.
1.2	December 8, 2009	Changes throughout to align with SAFE Bio-Pharma "SAFE CP Version 2.4 4 March 2009"
1.3	April 7, 2010	Revised Section 7.3.2 to replace support of OCSP nonces with requirement for time-based caching responders.
1.4	November 10, 2010	Updates to align with PIV-I changes in Common Policy.
1.5	March 20, 2014	Updated to reflect Federal PKI PA mandatory policy mapping requirements for medium hardware assurances.
1.6	April 15, 2016	Update to align with FBCA CP 2.27
1.6.1	May 16, 2016	Updated with comments from FPKI PA for FBCA CP 2.28
1.6.2	May 17, 2016	Updated with additional comments from FPKI PA
1.6.3	October 16, 2016	Updated with additional comments from FPKI PA, to align with FBCA CP 2.29.
1.6.4	December 8, 2016	Updated with additional comments from FPKI PA, and to align with FBCA CP 2.30 and change proposals.

Table of Contents

1 INTRODUCTION

This Certificate Policy (CP) includes sixteen (16) policies for use by the Entrust Non-Federal Identity (NFI) PKI, and to facilitate interoperability between the NFI PKI and other Entity PKI domains. The policies represent six 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).

This policy applies to certificates issued to state and, local governments, and commercial employees, contractors, and other affiliated personnel for the purposes of authentication, signature, and confidentiality.

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

1.1 OVERVIEW

1.1.1 Certificate Policy (CP)

Certificates issued under this policy contain a registered certificate policy object identifier (OID), which may be used by a relying party to decide whether a certificate is trusted for a particular purpose. The OID corresponds to a specific level of assurance established by this CP which shall be available to Relying Parties. Each certificate issued under this policy will assert the appropriate level of assurance in the *certificatePolicies* extension.

1.1.2 Relationship between the CP and the CPS

This CP states what assurance can be placed in a certificate issued by the CA. The certification practice statement (CPS) states how the CA establishes that assurance. CAs that issue certificates under this CP shall have a corresponding CPS. It is permissible to combine two CPS documents into one document if the CAs are related (e.g., a Root CA and its subordinate CA).

1.1.3 Scope

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

1.1.4 Interoperation with CAs Issuing under Different Policies

Interoperation with CAs that issue under different policies will be achieved through policy mapping and cross-certification through the Federal Bridge Certification Authority.

1.2 DOCUMENT NAME AND IDENTIFICATION

There are sixteen policies specified at six 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 NFI Root CA and Issuing CAs. The policy OIDs for the NFI PKI are registered in the ISO/ITU-T Objects Registry as follows:

Table 1: Certificate Policy Identifiers

Policy Name	Policy OID
certpolicy OBJECT IDENTIFIER	::= {2 16 840 1 114027 200 3 10 7}
id-emspki-nfssp-medium-policy	::= {certpolicy 1}
id-emspki-nfssp-medium-hardware	::= {certpolicy 2}
id-emspki-nfssp-medium-devices	::= {certpolicy 3}
id-emspki-nfssp-medium-authentication	::= {certpolicy 4}
id-emspki-nfssp-medium-cardAuth	::= {certpolicy 5}
id-emspki-nfssp-pivi-hardware	::= {certpolicy 6}
id-emspki-nfssp-basic-policy	::= {certpolicy 7}
id-emspki-nfssp-rudimentary-policy	::= {certpolicy 8}
id-emspki-nfssp-pivi-contentsigning	::= {certpolicy 9}
id-emspki-nfssp-contentsigning	::= {certpolicy 10}
id-emspki-nfssp-cardauth	::= {certpolicy 11}
id-emspki-nfssp-derived-credential	::= {certpolicy 12}
id-emspki-nfssp-pivi-cardAuth	::= {certpolicy 13}
id-emspki-nfssp-medium-CBP	::= {certpolicy 14}
id-emspki-nfssp-mediumHW-CBP	::= {certpolicy 15}
id-emspki-nfssp-medium-devicesHW	::= {certpolicy 16}

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

The requirements associated with the medium-devices policy are identical to those defined for the Medium policy with the exception of identity proofing, re-key, and activation data. The requirements associated with the medium-devicesHW 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 medium-device and medium-deviceHW policies are restricted to devices and systems. However, this does not restrict certificates issued to non-person entities from asserting one or more other policies if all requirements for those policies are met.

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 MediumHW 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.

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

1.3 PKI PARTICIPANTS

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

1.3.1 PKI Authorities

1.3.1.1 Entrust Managed Services PKI Policy Authority (Entrust Policy Authority)

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

1.3.1.2 Certification Authority

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

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

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

1.3.1.3 Root Certification Authorities

It is the responsibility of the PA to designate which CAs shall be cross-certified with external entity CAs as a "Root CA". A CA that is to be designated as a Root CA:

- Shall be a self-signed CA;

- Shall comply with the requirements of a Root CA under the policies of any external entity to which it cross-certifies; and
- Shall not issue certificates to subscribers as defined in section 1.3.5.

Root CAs may issue certificates for the purpose of administering the Root CA, or to internal devices such as certificate status servers (CSS).

Root CAs under this policy may issue end-entity certificates to trusted personnel where necessary for the internal operations of the Root CA. Root CAs will not issue end-entity certificates for any other reasons.

1.3.1.4 Issuing Certification Authorities

A CA that issues subscriber certificates, referred to as an "Issuing CA", shall not issue CA certificates, nor shall it be cross-certified with another infrastructure. Issuing CAs are subordinated to Root CAs, and comply with the policies of the Root CAs.

1.3.1.5 Certificate Status Servers

PKIs may optionally include an authority that provides status information about certificates on behalf of a CA through on-line transactions. In particular, PKIs may include OCSP responders to provide on-line status information. Such an authority is termed a certificate status server (CSS). Where the CSS is identified in certificates as an authoritative source for revocation information, the operations of that authority are considered within the scope of this CP. Examples include OCSP servers that are identified in the authority information access (AIA) extension. OCSP servers that are locally trusted, as described in RFC 2560, are not covered by this policy. Any CA that issues PIV-I certificates under this policy must provide OCSP status responses.

1.3.2 Registration Authorities

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

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

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

1.3.3 Card Management System

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. CAs issuing PIV-I certificates are responsible for ensuring that all CMSs meet the requirements described in this document, including all requirements specified in Appendix 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 Trusted Agents

The trusted agent is a person who satisfies all the trustworthiness requirements for an RA and who performs identity proofing as a proxy for the RA. The trusted agent records information from and verifies biometrics (e.g., photographs) on presented credentials for applicants who cannot appear in person at an RA. The CPS will identify the parties responsible for providing such services, and the mechanisms for determining their trustworthiness.

1.3.5 Subscribers

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

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

There may be a subset of human subscribers that can be issued role-based certificates. These certificates identify a specific role on behalf of which the subscriber is authorized to act rather than the subscriber’s name and are issued in the interest of supporting accepted business practices. The role-based certificate can be used in situations where non-repudiation is desired. Normally, role-based certificates are issued in addition to an individual subscriber certificate. A specific role may be identified in certificates issued to multiple subscribers, however, the key pair will be unique to each individual role-based certificate (i.e. there may be four individuals carrying a certificate issued in the role of “Controller” however, each of the four individual certificates will carry unique keys and certificate identifiers). Roles for which role-based certificates may be issued are limited to those that are held by a unique individual within an organization (e.g. *Chief Information Officer, Acme Inc* is a unique individual whereas *Program Analyst, Acme Inc* is not).

1.3.6 Affiliated Organizations

Subscriber certificates may be issued in conjunction with an organization that has a relationship with the subscriber; this is termed affiliation. The organizational affiliation will be indicated in the certificate. Affiliated Organizations are responsible for verifying the affiliation at the time of certificate application and requesting revocation of the certificate if the affiliation is no longer valid.

1.3.7 Relying Parties

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

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

1.3.8 Other Participants

The CAs and RAs operating under this CP may require the services of other security, community, and application authorities, such as compliance auditors and attribute authorities. The CPS will identify the parties responsible for providing such services, and the mechanisms used to support these services.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

The sensitivity of the information processed or protected using certificates issued by the CA will vary significantly. 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. CAs operated under this policy are 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:

Table 2: Certificate Policy Identifiers

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.

Federal Relying Parties should review more detailed guidance governing the use of electronic signatures (which include the use of digital certificates) issued by the Office of Management and Budget implementing the Government Paperwork Elimination Act (Federal Register May 2000: Volume 65, Number 85, Page 25508), as well as more detailed subordinate guidance issued by other agencies pursuant to OMB direction (such as Federal Information Processing Standards, NIST

Special Publications and electronic record retention guidance provided by the National Archives and Records Administration).

1.4.2 Prohibited Certificate Uses

No stipulation.

1.5 POLICY ADMINISTRATION

1.5.1 Organization Administering the Document

The Entrust Managed Services 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 Entrust Managed Services (Entrust) Policy Authority (PA), whose address can be found below:

Rusty Atkinson
VP, Customer Operations
5430 LBJ Freeway
Suite 1250
Dallas, TX 75240

1.5.3 Person Determining CPS Suitability for the Policy

The Certification Practices Statement (CPS) must conform to the corresponding CP. The PA shall approve the CPS for each CA that issues certificates under this policy.

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

All CAs operated under this policy will submit their CPS and the results of their compliance audit to the Entrust PA for approval. The Entrust PA shall make these documents and results available to the FPKIPA. CAs are not a permitted to issue waivers for any CP requirement; if a change is required the Entrust PA will inform the FPKPA and amend the CP in a mutually agreed manner.

1.6 DEFINITIONS AND ACRONYMS

See sections 11 and 12.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

All CAs that issue certificates under this policy are obligated to post all CA certificates issued by or to the CA and CRLs issued by the CA in a repository that is publicly accessible through the Hypertext Transport Protocol (HTTP).

Entrust operates an LDAP directory structure, and provides web servers that serve to provide repository functionality.

2.1.1 Repository Obligations

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

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

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 Publication of Certificates and Certificate Status

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

The publicly accessible repository system 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 Entrust Non-Federal PKI (NFSSP) CP shall be publicly available on the Entrust Managed Services website . The CPS will not be published; however a redacted version of the CPS may be requested from the PA.

2.2.3 Interoperability

Where certificates and CRLs are published in directories, standards-based schemas for directory objects and attributes shall be used. Entrust utilized standard LDAP schema, ensuring compliance with FKIPA *Shared Service Provider Repository Service Requirements* [SSP REP], as well as the X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity

Verification Interoperable (PIV-I) Cards [PIV-I Prof] for technical guidance in establishing the schema.

2.3 TIME OR 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 Entrust PKI PA shall protect repository information not intended for public dissemination or modification. CA certificates and certificate status information issued to the Entrust PKI shall be publicly available through the Internet.

Access to other information in the CA repositories shall be determined by Entrust in conjunction with customers pursuant to their requirements and authorizing and controlling statutes.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

All CAs operating under this policy shall only generate and sign CA certificates that contain a non-null subject Distinguished Name (DN). Certificates issued by these CAs may also include alternative name forms.

All CA and RA certificates shall include a non-NULL subject 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,{Base DN}

For certificates with no Affiliated Organization:

*cn=Subscriber's full name, ou=Unaffiliated, ou=Entity CA's Name,
{Base
DN}*

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,{Base DN}

For certificates with no Affiliated Organization:
serialNumber=UUID, ou=Unaffiliated, ou=Entity CA's Name,{Base DN}

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-a76500a0c91e6bf6").

3.1.2 Need for Names to Be Meaningful

Names used in the certificates issued by the CAs operating under this policy 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

CAs operated under this policy shall not issue anonymous certificates. Pseudonymous certificates may be issued by the NFI CAs to support internal operations. CA certificates issued by CAs under this policy shall not contain anonymous or pseudonymous identities.

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

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Names

Name uniqueness must be enforced by all CAs Entrust operates under this policy.

The Entrust Policy Authority is responsible for ensuring name uniqueness in certificates issued by the Entrust Managed Service. Name uniqueness is not violated when multiple certificates are issued to the same entity.

3.1.6 Recognition, Authentication, and Role of Trademarks

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

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

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

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

3.2.2 Authentication of Organization Identity

Requests for 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 issuing 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. Requests for CA certificates, as well as any questions or concerns will be referred to the Entrust Policy Authority for adjudication.

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

Procedures for Subscribers: a CA, and/or associated RAs shall ensure that the applicant's identity information is verified in accordance with the process established by this CP and the applicable CPS. Process information shall depend upon the certificate level of assurance and shall be addressed in the 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. CAs being considered for cross certification must comply with this requirement.

The 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 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 and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

In 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 All Levels: If an applicant is unable to perform face-to-face 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 who the trusted person is representing.

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.

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. Address confirmation: a) Issue credentials in a manner that confirms the address of record supplied by the applicant; or 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. 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. (e.g., Non-REAL ID Act compliant Drivers License). Any credentials presented must be unexpired. 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.

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 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.

When an RA is making the determination whether a role-based certificate is authorized, the RA will consider whether the role carries inherent authority beyond the job title. Role-based certificates may also be used for individuals on temporary assignment, where the temporary assignment carries an authority not shared by the individuals in their usual occupation, for example: "Watch Commander, Task Force 1". Questions regarding the scope of role-based certificates may be referred to the Entrust Policy Authority for adjudication.

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 RA 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 issuing entity's control (i.e., require registration and validation that meets all issuing agency's requirements, as well as requiring re-validation prior to being re-issued). 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 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 rudimentary policies, information that is not verified shall not be included in certificates.

3.2.5 Validation of Authority

Before issuing CA certificates or signature certificates that assert organizational authority, the CA shall validate the individual's authority to act in the name of the organization.

3.2.6 Criteria for Interoperation

The Entrust Policy Authority, in conjunction with the FPKIPA, shall determine the interoperability criteria for CAs operating under this policy. Root CAs operating under this policy only cross-certify with CAs operated by the FPKIPA. Issuing CAs do not support cross-certification.

3.3 *IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS*

3.3.1 Identification and Authentication for Routine Re-key

Root and Issuing CA certificate re-key shall follow the same procedures as initial certificate issuance.

Subscribers of Issuing CAs shall identify themselves for the purpose of re-keying as required in table below.

Assurance Level	Routine Re-key Identity Requirements for Subscriber Signature, Authentication and Encryption Certificates
Rudimentary	Identity may be established through use of current signature key.
Basic	Identity may be established through use of current signature key, except that identity shall be reestablished through initial registration process at least once every 15 years from the time of initial registration.
Medium (all policies)	Identity may be established through use of current signature key, except that identity shall be established through initial registration process at least once every nine years from the time of initial registration. For mediumDevice and mediumDeviceHardware certificates, identity may be established through the use of current signature key or using means commensurate with the strength of the certificate being requested, except that identity shall be established through initial registration process at least once every nine years from the time of initial registration.

PIV-I Card Authentication	Identity may be established through use of the current signature key certificate, except that identity shall be established through initial registration process at least once every nine years from the time of initial registration.

3.3.2 Identification and Authentication for Re-key after Revocation

After a certificate has been revoked, other than during a renewal or update action, the subscriber is required to go through the initial registration process per section 3.2 above to obtain a new certificate.

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 OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

This section specifies requirements for initial application for certificate issuance.

Subscribers to this PKI shall be limited to those individuals filling Trusted Roles within the PKI and the employees, contractors, business partners and affiliates of Entrust Managed Services NFI PKI customer organizations.

Application for Certificates issued under this policy may be submitted in person or via electronic means, as long as the identification and authentication requirements applicable to the assurance level of the certificates being requested are satisfied.

4.1.1 Who Can Submit a Certificate Application

No stipulation.

4.1.2 Enrollment Process and Responsibilities

The Entrust Policy Authority will ensure that applications for cross-certification contain accurate information.

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

4.2.1 Performing Identification and Authentication Functions

The identification and authentication of the subscriber must meet the requirements specified for subscriber authentication as specified in sections 3.2 and 3.3 of this CP.

RAs and their delegates, LRAs, are responsible for authenticating the subscriber's identity. The Entrust Policy Authority is responsible for identifying individual RAs and LRAs that are responsible for authenticating the subscriber's identity in each case, and approving automated issuance systems that are compliant with sections 3.2 and 3.3 of this CP.

4.2.2 Approval or Rejection of Certificate Applications

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

For all other certificates, approval or rejection of certificate applications is at the discretion of the Entrust Policy Authority.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 ISSUANCE

4.3.1 CA Actions During Certificate Issuance

Upon receiving the request, the RAs will verify the source of a request. This will include:

- Verify the identity of the requester.
- Verify the authority of the requester and the integrity of the information in the certificate request.
- Build and sign a certificate if all certificate requirements have been met (in the case of an RA, have the CA sign the certificate).
- Notify the subscriber that certificates have been generated.
- Make the certificate available to the subscriber.

The procedures for verifying prospective subscriber data are described in the CA's CPS.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

CAs operating under this policy shall inform the subscriber of the creation of certificates and make the certificates available to the subscriber. Procedures for notifying subscribers are described in the CA's CPS.

4.4 CERTIFICATE ACCEPTANCE

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

4.4.1 Conduct Constituting Certificate Acceptance

For subscriber certificates, failure to object to the certificate or its contents constitutes acceptance of the certificate.

4.4.2 Publication of the Certificate by the CA

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

This specification makes no stipulation regarding publication of subscriber certificates, except as noted in section 9.4.3.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The Entrust Policy Authority must be notified whenever a CA operating under this policy issues a CA certificate. The Entrust Policy Authority will notify the FPKIPA of the certificate issuance. The process for notification is described in the Memorandum of Understanding (MOU) between Entrust and the FPKIPA.

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.

4.5.2 Relying Party Public key and Certificate Usage

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

4.6 CERTIFICATE RENEWAL

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.

Certificates may also be renewed when a CA re-keys.

4.6.2 Who May Request Renewal

The Entrust Policy Authority may request renewal of a Root CA's cross certificate with the other entities, including the FBCA.

For Issuing CAs that support renewal, such requests shall only be accepted from certificate subjects, PKI sponsors or RAs. Additionally, a CA may perform renewal of its subscriber certificates without a corresponding request, such as when the CA re-keys.

4.6.3 Processing Certificate Renewal Requests

For Root CAs, CA certificate renewal for reasons other than re-key shall be approved by the Entrust Policy Authority.

For issuing CAs, no stipulation.

4.6.4 Notification of New Certificate Issuance to Subscriber

No stipulation beyond the requirements in section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Refer to section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

All CA certificates shall be published in the Repositories; see section 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.7 CERTIFICATE RE-KEY

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

Subscribers shall identify themselves for the purpose of re-keying as required in section 3.3.1.

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

4.7.1 Circumstance for Certificate Re-key

No stipulation.

4.7.2 Who May Request Certification of a New Public Key

The Entrust Policy Authority may request certification of a new public key by the FPKIPA for cross-certification with the FBCA.

For Issuing CAs that support re-key, such requests shall only be accepted from the subject of the certificate or PKI sponsors. Additionally, CAs and RAs may initiate re-key of a subscriber's certificates without a corresponding request.

4.7.3 Processing Certificate Re-keying Requests

See sections 3.2 and 3.3.

4.7.4 Notification of New Certificate Issuance to Subscriber

See section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

See section 4.4.1.

4.7.6 Publication of the Re-keyed Certificate by the CA

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

This policy makes no stipulation regarding publication of subscriber certificates, except as noted in section 9.4.3.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.8 CERTIFICATE MODIFICATION

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

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

4.8.1 Circumstance for Certificate Modification

No stipulation.

4.8.2 Who May Request Certificate Modification

No stipulation.

4.8.3 Processing Certificate Modification Requests

For Issuing CAs, proof of all subject information changes must be provided to the RA or other designated agent and verified before the modified certificate is issued.

4.8.4 Notification of New Certificate Issuance to Subscriber

The CA notifies the Subscriber of the issuance of a modified certificate under the same process for notifying a first-time Subscriber of a newly issued certificate (see Section 4.3.2).

4.8.5 Conduct Constituting Acceptance of Modified Certificate

The modified certificate acceptance process is the same as that used for a new certificate (see Section 4.4.1).

4.8.6 Publication of the Modified Certificate by the CA

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

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

The CA notifies other entities of the issuance of a modified certificate under the same process for notifying other entities of a newly issued certificate (see Section 4.4.3).

4.9 CERTIFICATE REVOCATION AND SUSPENSION

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

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

4.9.1 Circumstances for Revocation

A certificate shall be revoked when the binding between the subject and the subject's public key defined within the certificate is no longer considered valid.

Issuing CAs that implement certificate revocation shall, at a minimum, 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, Issuing CAs shall require that the organization must inform the Issuing CA of any changes in the subscriber affiliation. If the affiliated organization no longer authorizes the affiliation of a Subscriber, the CA shall revoke any certificates issued to that Subscriber containing the organizational affiliation. If an organization terminates its relationship with an Issuing CA such that it no longer provides affiliation information, the Issuing 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

Within the Entrust NFI PKI, a CA may summarily revoke certificates within its domain. A written notice and brief explanation for the revocation shall subsequently be provided to the Subscriber(s) whose certificates were revoked.

The RA can request the revocation of a Subscriber's certificate on behalf of any authorized party as specified in the CPS.

The Entrust NFI CA accepts revocation requests from Affiliated Organizations named in the certificates. A Subscriber may request that its own certificate be revoked. The human sponsor of a device can request the revocation of the device's certificate. Other authorized Affiliated Organization and customer officials may request revocation as described in the CPS.

4.9.3 Procedure for Revocation Request

Issuing CAs 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 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. Even where all the above conditions have been met, revocation of the associated certificates is recommended.

RAs (or delegate) shall collect and destroy PIV-I Cards from Subscribers whenever the cards are no longer valid, whenever possible. RAs (or delegate) shall record destruction of PIV-I Cards. Certificates issued by a PIV-I policy Issuing CA shall whenever possible, collect and destroy PIV-I Cards from Subscribers whenever the cards are no longer valid. RAs (or delegate) shall record the 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 must make a revocation request after reasons for revocation have been identified.

See section 9.6.3.

4.9.5 Time within which CA must Process the Revocation Request

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

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. Issuing CAs under this policy will issue CRLs in accordance with the following table:

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

For Root CAs that are operated in an off-line manner, routine CRLs may be issued less frequently than specified above if the CA only issues:

- CA certificates
- (optionally) CSS certificates, and
- (optionally) end user certificates solely for the administration of the Root CA.

However, the interval between routine CRL issuance shall not exceed 31 days. Such CAs must meet the requirements specified in section 4.9.12 for issuing Emergency CRLs.

(Note: such CAs are required to notify the FPKIMA upon Emergency CRL issuance. This requirement is included in the MOA between the FPKIPA and Entrust.)

4.9.8 Maximum Latency for 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.

4.9.9 On-line Revocation/Status Checking Availability

CAs operated under this policy support on-line revocation/status checking via OCSP [RFC 2560]. The latency of certificate status information distributed on-line by these CAs or their delegated status responders must meet or exceed the requirements for CRL issuance stated in 4.9.7.

For PIV-I certificates, CAs operated under this policy shall support on-line status checking via OCSP [RFC 2560].

4.9.10 On-line Revocation Checking Requirements

No stipulation.

4.9.11 Other Forms of Revocation Advertisements Available

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

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

4.9.12 Special Requirements Related To Key Compromise

In the event of a Root CA private key compromise or loss, the cross-certificate shall be revoked and a CRL shall be published at the earliest feasible after revocation. .

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

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

For CA certificates, suspension is not permitted.

For end entity certificates, no stipulation.

4.9.14 Who Can Request Suspension

No stipulation for end entity certificates.

4.9.15 Procedure for Suspension Request

No stipulation for end entity certificates.

4.9.16 Limits on Suspension Period

No stipulation for end entity certificates.

4.10 CERTIFICATE STATUS SERVICES

Entrust NFI CAs shall use OCSP and CRLs to distribute status information. See sections 4.7 through 4.9.11.

4.10.1 Operational Characteristics

Entrust NFI CAs shall describe the Operational Characteristics of CSS systems in the CPS.

4.10.2 Service Availability

See Section 2.2.1, Publication of Certificates and Certificate Status.

4.10.3 Optional Features

No stipulation.

4.11 END OF SUBSCRIPTION

No stipulation.

4.12 KEY ESCROW AND RECOVERY

No stipulation.

4.12.1 Key Escrow and Recovery Policy and Practices

CA private keys are never escrowed.

Subscriber key management keys may be escrowed to provide key recovery. The NFI PKI supports private key escrow for subscriber key management keys. These keys shall be stored in a secure manner to be specified in the Entrust NFI CPS.. Escrowed keys shall be protected at no less than the level of security in which they are generated, delivered, and protected by the subscriber.

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

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Issuing CAs that support session key encapsulation and recovery shall identify the document describing the practices in the applicable CP.

There are no CAs operated under this policy that support session key encapsulation and recovery.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

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

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

5.1.1 Site Location and Construction

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

5.1.2 Physical Access

5.1.2.1 Physical Access for CA Equipment

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

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

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

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

- Be manually or electronically monitored for unauthorized intrusion at all times.
- Ensure an access log is maintained and inspected periodically.
- Require two-person physical access control to both the cryptographic module and computer system.

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 CA equipment or remote workstations used to administer the CAs (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., those cryptographic modules are in place when "open," and secured when "closed," and for off-line Root CAs, 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 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 CAs (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. In addition, the Repositories (containing issued certificates and CRLs) shall be provided with Uninterrupted Power sufficient for a minimum of six hours operation in the absence of commercial power. CAs 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 and Protection

No stipulation.

5.1.6 Media Storage

CA media shall be stored so as to protect them it accidental damage (e.g., water, fire, or electromagnetic). Sensitive 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 CAs 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 CA equipment. Only the latest full backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible, or the integrity of the CA will be weakened. The functions performed in these roles form the basis of trust for the entire PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

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

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 audit parameters; and generate component keys.

2 *Officer* – authorized to request or approve certificate issuance and revocations.

3 *Auditor* – authorized to review, maintain, and archive audit logs.

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.

Entrust maps Entrust-specific roles to the FBCA-provided role set. These roles are:

- Security Officer/Master User (SOMU)
- System Administrator
- Auditor/System Security Officer (Auditor)

These roles map to the FBCA role definitions:

FBCA Role	Equivalent Entrust Role
Officer	SOMU
Administrator	SA
Operator	SA
Auditor	Auditor

The Administrator and Operator functions as defined for the FBCA are performed by the SA as described in section 5.2.4. No individual may hold more than one role (SOMU, SA or Auditor).

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) Levels of Assurance for the following tasks:

- CA key generation;
- CA signing key activation;

- CA private key backup.

Where multiparty control is required, at least one of the participants shall be an Administrator. All participants must serve in a trusted role as defined in section 5.2.1. Multiparty control 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 SOMU, SA, and Auditor roles. The CA, CMS, CSS, and RA software and hardware shall identify and authenticate its users and shall ensure that no user identity can assume both an SA and SOMU role, assume both the SA and Auditor roles, and assume both the Auditor and SOMU roles. No individual shall have more than one role.
PIV-I Card Authentication	Individual personnel shall be specifically designated to the three 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, and Security Clearance Requirements

The Entrust Policy Authority, and its delegate the Operational Authority, are responsible and accountable for the operation of each CA under this policy.

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity. For PKIs operated at Medium Assurance and Medium Hardware, each person filling a trusted role must satisfy at least one of the following:

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

For PKIs operated at Rudimentary, Basic, Medium-CBP and Medium Hardware-CBP, there is no citizenship requirement or security clearance specified.

5.3.2 Background Check Procedures

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

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

The period of investigation must cover at least the last five years for each area, excepting the residence check which must cover at least the last three years. Regardless of the date of award, the highest educational degree shall be verified.

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

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 CAs operated under this policy 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 CAs shall receive comprehensive training, or demonstrate competence, in the following areas:

- CA (or 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 and Requirements

All individuals responsible for PKI roles shall be made aware of changes in the CA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

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

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

No stipulation.

5.3.7 Independent Contractor Requirements

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

5.3.8 Documentation Supplied to Personnel

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

5.4 AUDIT LOGGING PROCEDURES

Audit log files shall be generated for all events relating to the security of the CA. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

5.4.1 Types of Events Recorded

A message from any source received by the 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 entity and/or operator of the 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 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			
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
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 REVOCATION			
All certificate revocation requests		X	X
CERTIFICATE STATUS CHANGE APPROVAL			
The approval or rejection of a certificate status change request		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
MISCELLANEOUS			
Appointment of an individual to a Trusted 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			
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
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
Re-key of the CA	X	X	X
Configuration changes to the CA server involving:			
- Hardware		X	X
- Software		X	X
- Operating System		X	X
- Patches		X	X
- Security Profiles			X
PHYSICAL ACCESS / SITE			
SECURITY			
Personnel Access to room housing 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 messages			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 to 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.

Assurance Level	Review Audit Log
Rudimentary	Only required for cause
Basic	Only required for cause
Medium (all policies)	At least once every two months Statistically significant set of security audit data generated by CAs 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 every two months Statistically significant set of security audit data generated by CAs 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

A statistically significant sampling of the security audit data generated since the last review will be examined

5.4.3 Retention Period for Audit Log

For Medium, Medium Hardware, and PIV-I Assurance levels, 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 CA system shall be an official different from the individuals who, in combination, command the CA signature key.

5.4.4 Protection of Audit Log

The CA system configuration and procedures will 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 system 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 CA system. Automated audit processes shall be invoked at system (or application) startup, and cease only at system (or application) shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the Entrust Policy Authority shall determine whether to suspend operations until the problem has been remedied.

5.4.7 Notification to Event-Causing Subject

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

5.4.8 Vulnerability Assessments

Entrust personnel will perform routine assessments to determine whether the CA system or its components have been attacked or breached.

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

5.5 RECORDS ARCHIVAL

Entrust shall comply with company records retention policies in accordance with internal requirements and any laws that may apply. Entrust shall at minimum comply with the retention period for CA archive records stipulated in 5.5.2, regardless of company records retention policies. CA archive records shall be sufficiently detailed as to verify that the CA was properly operated as well as verify the validity of any certificate (including those revoked or expired) issued by the CA.

5.5.1 Types of Events Archived

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

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
Subscriber identity Authentication data as per Section 3.2.3		X	X
Documentation of receipt and acceptance of certificates (if applicable)		X	X

Data To Be Archived	Rudimentary	Basic	Medium (all policies) & PIV-I Card Authentication
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
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,	X	X	X

Data To Be Archived	Rudimentary	Basic	Medium (all policies) & PIV-I Card Authentication
including additions and deletions			
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
Appointment of an individual to a Trusted Role	X	X	X
Destruction of cryptographic modules	X	X	X
All certificate compromise notifications	X	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 minimum retention periods for archive data are identified below. In addition, Entrust will comply with internal policies and applicable laws and regulations.

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.

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 CA itself.

Alternatively, Entrust may retain data using whatever procedures have been approved by NARA for that category of documents. Applications required to process the archive data shall also be maintained for a period determined by Entrust Policy Authority in order to comply with section 5.5.2.

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.

5.5.4 Archive Backup Procedures

If Entrust chooses to back up its archive records, the CPS or a referenced document shall describe how the records are backed up and managed.

5.5.5 Requirements for Time-Stamping of Records

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

5.5.6 Archive Collection System (Internal or External)

No stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

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

The contents of the archive shall not be released except as determined by the Entrust Policy Authority 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, the old key must be retained and protected.

Entrust performs periodic key rollovers as described above. The procedure is described in the CPS.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

The Entrust Policy Authority shall notify the FPKIPA as required by the applicable MOU if any of the following cases occur:

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

The Entrust Policy Authority will reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the CA's CPS.

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

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

- Before returning to operation, ensure that the system's integrity has been restored.
- If the CA signature keys are not destroyed, CA operation will be reestablished, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in section 4.9.7.
- If the CA signature keys are destroyed, CA operation shall be reestablished as quickly as possible, giving priority to the generation of a new CA key pair.

5.7.3 Entity (CA) Private Key Compromise Procedures

In the event of a CA private key compromise, the following operations must be performed. If the CA signature keys are compromised or lost (such that compromise is possible even though not certain):

- The Entrust Policy Authority shall immediately inform the FPKIPA so that entities may issue CRLs revoking any cross-certificates issued to the compromised CA;
- New certificates shall be issued to Entities also in accordance with the applicable CA 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 Entrust Policy Authority shall also investigate and report to the FPKIPA what caused the compromise or loss, and what measures have been taken to preclude recurrence.

5.7.4 Business Continuity Capabilities after a Disaster

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

Entrust shall operate a hot backup site, whose purpose is to ensure continuity of operations in the event of failure of the primary site. Entrust shall have a disaster recovery plan in place to reconstitute the CA within 72 hours of failure, documented or referenced in the CPS.

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

5.8 CA & RA TERMINATION

In the event of termination of the Entrust NFI CA operation, certificates signed by the Entrust NFI CA shall be revoked. Prior to Entrust NFI CA termination, the Entrust NFI PA 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 unexpired, unrevoked certificates has past. Once the last CRL has been issued, the private signing key(s) of the Entrust NFI CA will be destroyed. The Entrust NFI CA will advise all other organizations to which it has issued certificates of its termination, with as much advance notice as circumstances permit.

In the event that an Entrust NFI CA cross certified with the FBCA terminates operation, the Entrust Policy Authority shall provide notice to the FPKIPA prior to termination.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

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

The modules shall meet or exceed Security Level 1 (for Rudimentary), or Security Level 2 (for Basic, Medium, or Medium Hardware). Multiparty control is required for CA key pair generation for the Entrust NFI CAs and for CAs operating at the Medium, or Medium Hardware, as specified in Section 5.2.2.

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, Medium Assurance and PIV-I Card Authentication, 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 140 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 FIPS validated hardware cryptographic module. For Medium and Basic assurance, either FIPS validated software or FIPS validated hardware cryptographic modules shall be used for key generation.

6.1.2 Private Key Delivery to Subscriber

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

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

- Anyone who generates a private signing key for a subscriber shall not retain any copy of the key after delivery of the private key to the subscriber.
- The private key(s) must be protected from activation, compromise, or modification during the delivery process.
- The subscriber shall acknowledge receipt of the private key(s).
- Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct subscribers.
    - For hardware modules, accountability for the location and state of the module must be maintained until the subscriber accepts possession of it.
    - For electronic delivery of private keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data shall be delivered using a separate secure channel.
    - For shared key applications, organizational identities, and network devices, see also Section 3.2.

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

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

- The CA loading a self-signed certificate onto tokens delivered to Relying Parties via secure mechanisms;
- Secure distribution of self-signed certificates through secure out-of-band mechanisms;
- Comparison of the hash of the self-signed certificate against a hash value made available via authenticated out-of-band sources (note that hashes posted in-band along with the certificate are not acceptable as an authentication mechanism); and
- Loading certificates from web sites secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded.

Other methods that preclude substitution attacks may be considered acceptable.

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

CA Certificates are signed with the issuing CA's current private key, so secure distribution is not required.

6.1.5 Key Sizes

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

For CAs that distribute self-signed certificates to relying parties, the CA's subject public keys in such certificates shall be at least 2048 bits for RSA, or at least 224 bits for ECDSA. Those CAs that distribute self-signed certificates and whose key pairs were generated before September 13, 2005 may be 1024 bits for RSA. Public keys in all self- signed certificates generated after 12/31/2010 that expire after 12/31/2030 shall be at least 3072 bits for RSA, or at least 256 bits for ECDSA.

CAs that generate certificates and CRLs under this policy shall use signature keys of at least 1024 bits for RSA or DSA, and at least 160 bits for ECDSA. Beginning 01/01/2011, all valid certificates shall be signed with keys of at least 2048 bits for RSA or at least 224 bits for ECDSA. All certificates, except self-signed certificates, that expire after 12/31/2030 shall be signed with keys of at least 3072 bits for RSA or at least 256 bits for ECDSA.

CAs that generate certificates and CRLs under this policy shall use SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512 hash algorithm when generating digital signatures. For Rudimentary and Basic Assurance, signatures on certificates and CRLs that are issued after 12/31/2013 shall be generated using, at a minimum, SHA-224. For Medium Assurance, signatures on certificates and CRLs that are issued after 12/31/2010 shall be generated using, at a minimum, SHA-224, however, RSA signatures on CRLs that are issued before January 1, 2012, and that include status information for certificates that were generated using SHA-1 may be generated using SHA-1. RSA signatures on CRLs that only provide status information for certificates that were generated using SHA-1 may continue to be generated using SHA-1. Signatures on certificates and CRLs that are issued after 12/31/2030 shall be generated using, at a minimum, SHA-256. Certificates issued to OCSP responders that only include SHA-1 certificates may be signed using SHA-1.

Where implemented, CSS systems shall sign responses using the same signature algorithm, key size, and hash algorithm used by the CA to sign CRLs. After December 31, 2010, for Medium Assurance, OCSP responders that generate signatures on OCSP responses using SHA-1 shall only provide signed responses that are pre-produced (i.e., any signed response that is provided to an OCSP client shall have been signed before the OCSP responder received the request from the client).

End-entity certificates shall contain public keys that are at least 1024 bit for RSA, DSA, or Diffie-Hellman, or 160 bits for elliptic curve algorithms. The following special conditions also apply:

- End-entity certificates that expire after 12/31/2030 shall contain public keys that are at least 3072 bits for RSA or DSA, or 256 bits for elliptic curve algorithms.

- End-entity certificates that include a keyUsage extension that only asserts the digitalSignature bit that expire on or after 12/31/2013 shall contain public keys that are at least 2048 bits for RSA or DSA, or 224 bits for elliptic curve algorithms.

- Beginning 01/01/2011, all valid end-entity certificates that include a keyUsage extension that asserts the nonRepudiation, keyEncipherment, dataEncipherment, or keyAgreement bit shall contain public keys that are at least 2048 bits for RSA, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms.

- Beginning 01/01/2011, all valid end-entity certificates that do not include a keyUsage extension shall contain public keys that are at least 2048 bits for RSA, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms.

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

Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum triple-DES or equivalent for the symmetric key, and at least 1024 bit RSA or equivalent for the asymmetric keys through 12/31/2010. Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum AES (128 bits) or equivalent for the symmetric key, and at least 2048 bit RSA or equivalent for the asymmetric keys after 12/31/2010. Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum AES (128 bits) or equivalent for the symmetric key, and at least 3072 bit RSA or equivalent for the asymmetric keys after 12/31/2030.

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 Federal 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.

CA certificates issued by CAs operating under this policy 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.

Rudimentary, Basic, and Medium Assurance Level certificates may include a single key for use with encryption and signature in support of legacy applications. Such dual-use certificates shall be generated and managed in accordance with their respective signature certificate requirements, except where otherwise noted in this CP. Such dual-use certificates shall never assert the non-repudiation key usage bit, and shall not be used for authenticating data that will be verified on the basis of the dual-use certificate at a future time. 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.

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 AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS*

6.2.1 Cryptographic Module Standards and Controls

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

Cryptographic modules shall be validated to the FIPS 140 level identified in this section.

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 2 (Hardware)	Level 1	Level 2 (Hardware)
PIV-I Card Authentication	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)
Medium Hardware	Level 2 (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). On an annual basis, for each PCI configuration used (as defined by the FIPS 201 Evaluation Program), one populated, representative sample PIV-I Card shall be submitted to the FIPS 201 Evaluation Program for testing.

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

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

Use of the CA private signing key for any CA operated under this policy 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 CA private signature key

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

6.2.3.2 Escrow of CA encryption key

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

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 CA Private Signature Key

Backup of CA private signature keys is required to facilitate disaster recovery. Where required by Section 5.2.2, CA private signature keys shall be backed up under multi-person control.

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

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 whose corresponding public key is contained in a certificate asserting a rudimentary, basic or medium policy may be backed up or copied, but must be held in the Subscriber's control.

Backed up subscriber private signature keys shall not be stored in 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 Private Key Management Key

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

6.2.4.4 Backup of CSS Private Key

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

6.2.4.5 Backup of Content Signing Private Key

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 Signing 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

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

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

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

6.2.7 Private Key Storage on Cryptographic Module

No stipulation beyond that specified in FIPS 140.

6.2.8 Method of Activating Private Key

For CAs under this policy that operate 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. 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 Method of Deactivating Private Key

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

6.2.10 Method of Destroying Private Key

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 PAIR MANAGEMENT

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods and Key Usage Periods

CAs operated under this policy that distribute their self-signed certificates for use as trust anchors shall limit the use of the associated private key to a maximum of 20 years; the self-signed certificates shall have a lifetime not to exceed 37 years. For all other CAs, the CA shall limit the use of its private keys to a maximum of six years for subscriber certificates and ten years for CRL signing and OCSP responder certificates. Code and content signers may use their private keys for three years; the lifetime of the associated public keys shall not exceed eight years. Subscribers' signature private keys and certificates have a maximum lifetime of three years. Subscriber key management certificates have a maximum lifetime of 3 years; use of subscriber key management private keys is unrestricted.

PIV-I subscriber certificate expiration shall not be later than the expiration date of the PIV-I hardware token on which the certificates reside.

Subscriber public keys in certificates that assert the id-fpki-pivi-content-signing OID in the extended key usage extension have a maximum usage period of nine years. The private keys corresponding to the public keys in these certificates have a maximum usage period of three years. Expiration of the id-fpki-certpcy-pivi-contentSigning certificate shall be later than the expiration of the id-fpki-certpcy-pivi-hardware and id-fpki-certpcy-pivi-cardAuth certificates.

For PIV-I, CSS certificates that provide revocation status have a maximum certificate validity period of 31 days.

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

The validity period of the subscriber certificate must not exceed the routine re-key Identity Requirements as specified in section 3.3.1.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

The activation data used to unlock any 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 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; or
- recorded and secured at the level of assurance associated with the activation of the cryptographic module, and shall not be stored with the cryptographic module.

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

6.4.3 Other Aspects of Activation Data

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

6.5 *COMPUTER SECURITY CONTROLS*

6.5.1 Specific Computer Security Technical Requirements

For CAs operated under this policy, 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. The CA and its ancillary parts shall include the following functionality:

- 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:

- 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 TECHNICAL CONTROLS

6.6.1 System Development Controls

The system development controls for CAs operated under this policy 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 shall be dedicated to performing one task: the CA.

- There shall be no other applications; hardware devices, network connections, or component software installed which are not part of the CA operation.

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

No stipulation.

6.7 NETWORK SECURITY CONTROLS

CAs, RAs, CMSs, repositories, remote workstations used to administer the CAs, 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 authentication of the remote workstation 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, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

7.1.1 Version Number(s)

CAs operating under this policy 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].

Certificates issued by CAs operating under this policy shall comply with Federal Public Key Infrastructure X.509 Certificate and CRL Extensions Profile [FPKI-Prof].

CAs operating under this policy that issue PIV-I Certificates shall comply with [PIV-I Profile]. The associated CSS certificates will also comply with [PIV-I Profile].

Certificates issued by CAs operating under this policy shall not include critical private extensions. Subscriber certificates issued by PKIs 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 the CAs operating under this policy shall identify the signature algorithm using one of the following OIDs:

id-dsa-with-sha1	{ iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3 }
sha-1WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }
sha256WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
id-RSASSA-PSS	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10 }
ecdsa-with-SHA1	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) 1 }
ecdsa-with-SHA224	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 1 }
ecdsa-with-SHA256	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2 }

ecdsa-with-SHA384	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }
ecdsa-with-SHA512	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4 }

Where certificates are signed using RSA with PSS padding, the OID is independent of the hash algorithm; the hash algorithm is specified as a parameter. RSA signatures with PSS padding may be used with the hash algorithms and OIDs specified below:

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

Where non-CA certificates issued under this policy contain an elliptic curve public key, the parameters shall be specified as one of the following named curves:

ansip192r1	{ iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 1 }
ansit163k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 1 }
ansit163r2	{ iso(1) identified-organization(3) certicom(132) curve(0) 15 }
ansip224r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 33 }
ansit233k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 26 }
ansit233r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 27 }
ansip256r1	{ iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7 }
ansit283k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 16 }
ansit283r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 17 }
ansip384r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 34 }
ansit409k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 36 }
ansit409r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 37 }

ansip521r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 35 }
ansit571k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 38 }
ansit571r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 39 }

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 [RFC3280].

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

Certificates issued under this CP shall assert the OID appropriate to the type of certificate and level of assurance with which it was issued. See Section 1.2, Document Identification for specific OIDs.

7.1.7 Usage of Policy Constraints Extension

CAs operating under this policy may assert policy constraints in CA certificates.

7.1.8 Policy Qualifiers Syntax and Semantics

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

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Not applicable; Certificates issued under this policy do not contain a critical certificate policies extension.

7.2 CRL PROFILE

7.2.1 Version Number(s)

CAs operating at Basic, Medium, or Medium Hardware Assurance under this policy shall issue X.509 version two (2) CRLs.

7.2.2 CRL and CRL Entry Extensions

CAs operated operating under this policy shall conform to [FPKI-PROF].

7.3 OCSP PROFILE

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

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

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

The Entrust 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.

8.1 *FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT*

The CAs, CMSs, RAs and their subordinate CAs, CMSs, and RAs operating under this policy 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.

As an alternative to a full annual compliance audit against the entire CPS, the compliance audit of CAs and RAs may be carried out in accordance with the requirements as specified in the FPKI Compliance Audit Requirements document [AUDIT].

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

The CAs have 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 Entrust Policy Authority acknowledges that the FPKIPA has the right to require aperiodic compliance audits of CAs (and, when needed, their subordinate CAs) that interoperate with the FBCA under this CP.

8.2 *IDENTITY/QUALIFICATIONS OF ASSESSOR*

The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the requirements that Entrust and this CP impose on the issuance and management of their certificates. The compliance auditor must perform such compliance audits as a regular ongoing business activity. In addition to the previous requirements, the auditor must be a Certified Information System Auditor (CISA), IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

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

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

8.4 TOPICS COVERED BY ASSESSMENT

The purpose of a compliance audit of the Entrust NFI PKI is to verify that Entrust is complying with any MOAs between the Entrust and any other PKI, as well as the requirements of the CPS, and that the CPS is consistent with this CP. 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 Entrust NFI PKI covers all aspects within the scope identified above.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

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

- The compliance auditor shall note the discrepancy;
- The compliance auditor shall notify the parties identified in section 8.6 of the discrepancy;
- The Entrust Policy Authority shall determine what further notifications or actions are necessary to meet the requirements of this CP, the CA's CPS, and any relevant MOA provisions. The Entrust Policy Authority shall proceed to make such notifications and take such actions without delay.

When the Entrust Policy Authority receives a report of audit deficiency from the NFI PKI, the Entrust Policy Authority may direct the Entrust Operational Authority to take additional actions to protect the level of trust in the infrastructure.

8.6 COMMUNICATION OF RESULTS

On an annual basis, the Entrust Policy Authority shall submit an audit compliance package to the FPKIPA. This package shall be prepared in accordance with the "Compliance Audit Requirements" document and includes an assertion from the Entrust Policy Authority 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.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 Certificate Issuance or Renewal Fees

No Stipulation.

9.1.2 Certificate Access Fees

No Stipulation.

9.1.3 Revocation or Status Information Access Fees

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 of certificates issued by CAs under this policy. Rather, entities, acting as relying parties, shall determine what financial limits, if any, they wish to impose for certificates used to complete a transaction.

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

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

9.3.1 Scope of Confidential Information

No stipulation.

9.3.2 Information not within the Scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

No stipulation.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

No Stipulation.

9.4.2 Information Treated as Private

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

9.4.3 Information not Deemed Private

Information included in certificates is not subject to protections outlined in section 9.4.2.

For CAs operating under this policy, 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.

9.4.5 Notice and Consent to Use Private Information

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

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

9.4.7 Other Information Disclosure Circumstances

None.

9.5 INTELLECTUAL PROPERTY RIGHTS

The Entrust Policy Authority will not knowingly violate intellectual property rights held by others.

9.6 REPRESENTATIONS AND WARRANTIES

The obligations described below to all CAs which either interoperate with the FBCA or are in a trust chain up to a CA that interoperates with the FBCA. The obligations applying to Root or other CAs pertain to their activities as issuers of certificates. Further, the obligations focus on obligations of CAs affecting interoperability with the FBCA. Thus, where the obligations include, for example, a review (or audit) by the FPKIPA or some other body of Entrust's PKI operations, the purpose of that review pertains to interoperability using the FBCA, and whether the Entity is complying with the MOA.

9.6.1 CA Representations and Warranties

The Entrust Policy Authority determines whether that entity's certificate policy meets its legal and policy requirements. Entrust understands that review of Entrust's certificate policy by the FPKIPA is not a substitute for due care and mapping of certificate policies by the non- federal entity.

For PIV-I, Entrust CAs shall maintain an agreement with Affiliated Organizations concerning the obligations pertaining to authorizing affiliation with Subscribers of PIV-I certificates.

9.6.2 RA Representations and Warranties

No stipulation.

9.6.3 Subscriber Representations and Warranties

For Medium and Medium Hardware Assurance levels, a Subscriber shall be required to sign a document 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 CAs 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 appropriate CA upon suspicion of loss or compromise of their private keys. Such notification shall be made directly or indirectly through mechanisms consistent with the CA's 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

None.

9.6.5 Representations and Warranties of Affiliated Organizations

Affiliated Organizations shall authorize the affiliation of subscribers with the organization, and shall inform Entrust of any severance of affiliation with any current subscriber

9.6.6 Representations and Warranties of Other Participants

None

9.7 DISCLAIMERS OF WARRANTIES

None.

9.8 LIMITATIONS OF LIABILITY

No stipulation.

9.9 INDEMNITIES

No stipulation.

9.10 TERM AND TERMINATION

9.10.1 Term

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

9.10.2 Termination

Termination of this CP is at the discretion of the Entrust Policy Authority.

9.10.3 Effect of Termination and Survival

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

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

No stipulation.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

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

9.12.2 Notification Mechanism and Period

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

9.12.3 Circumstances under which OID must be changed

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

9.13 DISPUTE RESOLUTION PROVISIONS

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

9.14 GOVERNING LAW

The construction, validity, performance and effect of certificates issued under this CP for all purposes shall be governed by applicable statutes, laws and regulations..

9.15 COMPLIANCE WITH APPLICABLE LAW

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

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

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

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 OTHER PROVISIONS

No stipulation.

10 BIBLIOGRAPHY

The following documents were used in part to develop this CP:

ABADSG Digital Signature Guidelines, 1996-08-01. http://www.abanet.org/scitech/ec/isc/dsgfree.html.

AUDIT FPKI Compliance Audit Requirements http://www.idmanagement.gov/fpki-documents

CIMC Certificate Issuing and Management Components Family of Protection Profiles, version 1.0, October 31, 2001.

FIPS 140-2 Security Requirements for Cryptographic Modules May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

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 800-73 Interfaces for Personal Identity Verification (4 Parts) http://csrc.nist.gov/publications/PubsSPs.html

NIST SP 800-76 Biometric Data Specification for Personal Identity Verification http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf

PIV-I Prof X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards

11 ACRONYMS AND ABBREVIATIONS

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

GSA	General Services Administration
HTTP	HyperText Transfer Protocol
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector
ITU-TSS	International Telecommunications Union – Telecommunications System Sector
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
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
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)
WWW	World Wide Web
PKIX	Public Key Infrastructure X.509

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.
Applicant	The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]
Archive	Long-term, physically separate storage.
Attribute Authority	An entity, recognized by the FPKIPA or comparable Entity body as having the authority to verify the association of attributes to an identity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]

Backup

Copy of files and programs made to facilitate recovery if necessary. [NS4009]

Binding

Process of associating two related elements of information. [NS4009]

Biometric

A physical or behavioral characteristic of a human being.

Certificate

A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]. As used in this CP, the term "Certificate" refers to certificates that expressly reference the OID of this CP in the "Certificate Policies" field of an X.509 v.3 certificate.

Certification Authority (CA)

An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs.

Certification Authority Revocation List (CARL)

A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates, that have been revoked.

CA Facility

The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.

Certificate

A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies it's Subscriber, (3) contains the Subscriber's public key, (4) identifies it's operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]

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 (FPKIPA)

The FPKIPA is a federal government body responsible for setting, implementing, and administering policy decisions regarding inter Entity PKI interoperability that uses the FBCA.

Firewall

Gateway that limits access between networks in accordance with local security policy. [NS4009]

High Assurance Guard (HAG)

An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.

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.

Local Registration Authority (LRA)

A Registration Authority with responsibility for a local community.

Memorandum of Agreement (MOA)

Agreement between the FPKIPA and an Entity allowing interoperability between the Entity Principal CA and the FBCA.

Mission Support Information

Information that is important to the support of deployed and contingency forces.

Mutual Authentication

Occurs when parties at both ends of a communication activity authenticate each other (see authentication).

Naming Authority

An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.

National Security System

Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]

Non-Repudiation

Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.

Object Identifier (OID)

A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI they are used to uniquely identify each of the seven policies and cryptographic algorithms supported.

Out-of-Band

Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).

Outside Threat

An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.

Physically Isolated Network

A network that is not connected to entities or systems outside a physically controlled space.

PKI Sponsor

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 FBCA, the PMA is the FPKIPA.

Principal CA

The Principal CA is a CA designated by an Entity to interoperate with the FBCA. An Entity may designate multiple Principal CAs to interoperate with the FBCA.

Privacy

Restricting access to subscriber or Relying Party information in accordance with Federal law and Entity policy.

Private Key

(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.

Public Key

(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.

Public Key Infrastructure (PKI)

A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

Registration Authority (RA)

An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).

Re-key (a certificate)
To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.

Relying Party
A person or Entity who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.

Renew (a certificate)
The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.

Repository
A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.

Responsible Individual
A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.

Revoke a Certificate
To prematurely end the operational period of a certificate effective at a specific date and time.

Risk
An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Risk Tolerance
The level of risk an entity is willing to assume in order to achieve a potential desired result.

Root CA
In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.

Server
A system entity that provides a service in response to requests from clients.

Signature Certificate
A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.

Subordinate CA
In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).

Subscriber
A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device.

Superior CA

In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).

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.

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 readers and applications, and that may be trusted for particular purposes through a decision of the relying Federal Agency. 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. 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 CardAuthentication 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 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, Issuing CAs have a responsibility to ensure a certain level of security from the CMSs that manage the token on which their certificates reside, and to which they issue certificates for the purpose of signing PIV-I Cards. This appendix provides additional requirements to those found above that apply to CMSs that are trusted under this Certificate Policy.

The Card Management Master Key shall be maintained in a FIPS 140-2 Level 2

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

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

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

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

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

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

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

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

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.

THIS PAGE INTENTIONALLY LEFT BLANK