



X.509 Certificate Policy for the Entrust Managed Services Non-Federal Identity Public Key Infrastructure

(EMS NFI CP)

Version3.0

12 August, 2026

SIGNATURE PAGE

JIM TROVATO

Entrust Federal mPKI Policy Authority (Print Name)

Signed by:
Jim Trovato
89D32B44D9C945B...

12 August, 2026

Entrust Federal mPKI
Policy Authority

TABLE OF CONTENTS

1.0	INTRODUCTION	11
1.1	OVERVIEW	11
1.1.1	Certificate Policy (CP).....	11
1.1.2	Relationship between the CP and the CPS	12
1.1.3	Relationship between the FBCA CP and this CP	12
1.1.4	Scope	13
1.1.5	Interoperation with CAs Issuing under Different Policies	13
1.2	Document Name and Identification	13
1.3	PKI Participants.....	15
1.3.1	PKI Authorities	16
1.3.1.1	Entrust Policy Management Authority (EPMA).....	16
1.3.1.2	EPMA Policy Authority Program Managers.....	17
1.3.1.3	RA Agency/Organization PMA.....	17
1.3.1.4	Operational Authority	17
1.3.2	Certification Authority	17
1.3.2.1	Root Certification Authorities	18
1.3.2.2	Issuing Certification Authorities.....	18
1.3.3	Card Management System.....	18
1.3.4	Registration Authorities.....	18
1.3.4.1	Trusted Agents	19
1.3.5	Certificate Status Servers.....	19
1.3.6	Key Recovery Authorities.....	19
1.3.6.1	Key Escrow Database (KED).....	19
1.3.6.2	Data Decryption Server	19
1.3.6.3	Key Recovery Agent (KRA).....	20
1.3.6.4	Key Recovery Official (KRO)	20
1.3.7	Key Recovery Requestors	21
1.3.7.1	Internal Third-Party Requestor	21
1.3.7.2	External Third-Party Requestor.....	21
1.3.8	Subscribers	21
1.3.9	Affiliated Organizations	22
1.3.10	Relying Parties	22
1.3.11	Other Participants.....	22
1.4	Certificate Usage	22
1.4.1	Appropriate Certificate Uses.....	22
1.4.2	Prohibited Certificate Uses	24
1.5	Policy Administration	24
1.5.1	Organization Administering the Document	24
1.5.2	Contact Person	24
1.5.3	Person Determining CPS Suitability for the Policy	24
1.5.4	CPS Approval Procedures.....	24
1.6	Definitions and Acronyms.....	25
2.0	PUBLICATION AND REPOSITORY RESPONSIBILITIES.....	26

2.1	Repositories.....	26
2.2	Publication of Certification Information	26
2.2.1	Publication of Certificates and Certificate Status.....	26
2.2.2	Publication of CA Information.....	27
2.2.3	Interoperability	27
2.3	Time or Frequency of Publication.....	27
2.4	Access Controls on Repositories	28
3.0	IDENTIFICATION AND AUTHENTICATION	29
3.1	Naming	29
3.1.1	Types of Names	29
3.1.1.1	Subject Names	29
3.1.1.2	Subject Alternative Names.....	30
3.1.2	Need for Names to Be Meaningful	30
3.1.3	Anonymity or Pseudonymity of Subscribers	31
3.1.4	Rules for Interpreting Various Name Forms	31
3.1.5	Uniqueness of Names	31
3.1.6	Recognition, Authentication, and Role of Trademarks	32
3.2	Initial Identity Validation	32
3.2.1	Method to Prove Possession of Private Key.....	32
3.2.2	Authentication of Organization Identity	32
3.2.3	Authentication of Individual Identity	32
3.2.3.1	Authentication of Human Subscribers	33
3.2.3.2	Authentication of Human Subscribers for Role-based Certificates	35
3.2.3.3	Authentication of Human Subscribers for Group Certificates.....	35
3.2.3.4	Authentication of Devices	36
3.2.4	Non-verified Subscriber Information	37
3.2.5	Validation of Authority	37
3.2.6	Criteria for Interoperation	37
3.3	Identification and Authentication for Re-key Requests	38
3.3.1	Identification and Authentication for Routine Re-key	38
3.3.2	Identification and Authentication for Re-key after Revocation	38
3.4	Identification and Authentication for Revocation Request.....	38
3.5	Identification and Authentication for Key Recovery Requests	38
3.5.1	KRA Authentication.....	39
3.5.2	KRO Authentication	39
3.5.3	Subscriber Authentication	39
3.5.4	Third-Party Key Requestor Authentication	39
3.5.5	Authentication of Data Decryption Servers	40
4.0	CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	41
4.1	Certificate Application	41
4.1.1	Who Can Submit a Certificate Application	41
4.1.2	Enrollment Process and Responsibilities.....	41
4.2	Certificate Application Processing	42
4.2.1	Performing Identification and Authentication Functions.....	42
4.2.2	Approval or Rejection of Certificate Applications	42

4.2.3	Time to Process Certificate Applications.....	42
4.3	Issuance.....	42
4.3.1	CA Actions during Certificate Issuance	42
4.3.2	Notification to Subscriber by the CA of Issuance of Certificate.....	43
4.4	Certificate Acceptance.....	43
4.4.1	Conduct Constituting Certificate Acceptance	43
4.4.2	Publication of the Certificate by the CA.....	43
4.4.3	Notification of Certificate Issuance by the CA to Other Entities	44
4.5	Key Pair and Certificate Usage.....	44
4.5.1	Subscriber Private Key and Certificate Usage	44
4.5.2	Relying Party Public key and Certificate Usage	44
4.6	Certificate Renewal	44
4.6.1	Circumstance for Certificate Renewal.....	45
4.6.2	Who May Request Renewal.....	45
4.6.3	Processing Certificate Renewal Requests	45
4.6.4	Notification of New Certificate Issuance to Subscriber.....	45
4.6.5	Conduct Constituting Acceptance of a Renewal Certificate.....	45
4.6.6	Publication of the Renewal Certificate by the CA	45
4.6.7	Notification of Certificate Issuance by the CA to Other Entities	46
4.7	Certificate Re-key	46
4.7.1	Circumstance for Certificate Re-key	46
4.7.2	Who May Request Certification of a New Public Key.....	46
4.7.3	Processing Certificate Re-keying Requests	47
4.7.4	Notification of New Certificate Issuance to Subscriber.....	47
4.7.5	Conduct Constituting Acceptance of a Re-keyed Certificate.....	47
4.7.6	Publication of the Re-keyed Certificate by the CA	47
4.7.7	Notification of Certificate Issuance by the CA to Other Entities	47
4.8	Certificate Modification.....	48
4.8.1	Circumstance for Certificate Modification	48
4.8.2	Who May Request Certificate Modification.....	48
4.8.3	Processing Certificate Modification Requests.....	49
4.8.4	Notification of New Certificate Issuance to Subscriber.....	49
4.8.5	Conduct Constituting Acceptance of Modified Certificate.....	49
4.8.6	Publication of the Modified Certificate by the CA.....	49
4.8.7	Notification of Certificate Issuance by the CA to Other Entities	49
4.9	Certificate Revocation and Suspension	49
4.9.1	Circumstances for Revocation	50
4.9.2	Who Can Request Revocation.....	50
4.9.3	Procedure for Revocation Request	50
4.9.4	Revocation Request Grace Period.....	51
4.9.5	Time within which CA must Process the Revocation Request	51
4.9.6	Revocation Checking Requirements for Relying Parties.....	51
4.9.7	CRL Issuance Frequency.....	52

4.9.8	Maximum Latency for CRLs.....	52
4.9.9	On-line Revocation/Status Checking Availability	52
4.9.10	On-line Revocation Checking Requirements.....	53
4.9.11	Other Forms of Revocation Advertisements Available	53
4.9.12	Special Requirements Related To Key Compromise	53
4.9.13	Circumstances for Suspension	54
4.9.14	Who Can Request Suspension	54
4.9.15	Procedure for Suspension Request.....	55
4.9.16	Limits on Suspension Period	55
4.10	Certificate Status Services	56
4.10.1	Operational Characteristics	56
4.10.2	Service Availability	56
4.10.3	Optional Features	56
4.11	End Of Subscription	56
4.12	Key Escrow and Recovery	56
4.12.1	Key Escrow and Recovery Policy and Practices	57
4.12.1.1	Key Escrow Process and Responsibilities	57
4.12.1.2	Key Recovery Process and Responsibilities	57
4.12.1.2.1	Key Recovery Through KRA	58
4.12.1.2.2	Automated Self-Recovery	58
4.12.1.2.3	Key Recovery During Token Issuance.....	58
4.12.1.2.4	Key Recovery by Data Decryption Server	58
4.12.1.3	Who Can Submit a Key Recovery Application	58
4.12.1.3.1	Key Requestor Authorization Validation	59
4.12.1.3.2	Subscriber Authorization Validation	59
4.12.1.3.3	KRA Authorization Validation.....	59
4.12.1.3.4	KRO Authorization Validation	59
4.12.1.3.5	Data Decryption Server Authorization Validation	59
4.12.2	Session Key Encapsulation and Recovery Policy and Practices	59
5.0	FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS	60
5.1	Physical Controls	60
5.1.1	Site Location and Construction	60
5.1.2	Physical Access	60
5.1.2.1	Physical Access for CA Equipment.....	60
5.1.2.2	Physical Access for RA Equipment	61
5.1.2.3	Physical Access for CSS Equipment	61
5.1.2.4	Physical Access for CMS Equipment.....	61
5.1.2.5	Physical Access for KED Equipment.....	61
5.1.2.6	Physical Access for DDS Equipment	62
5.1.2.7	Physical Access for KRA and KRO Equipment.....	62
5.1.3	Power and Air Conditioning	62
5.1.4	Water Exposures.....	62
5.1.5	Fire Prevention and Protection.....	62
5.1.6	Media Storage	63
5.1.7	Waste Disposal	63
5.1.8	Off-Site Backup	63
5.2	Procedural Controls.....	64
5.2.1	Trusted Roles	64

5.2.1.1	NFI CA Trusted Roles	64
5.2.1.2	Registration Authority Trusted Roles	65
5.2.2	Number of Persons Required per Task	65
5.2.3	Identification and Authentication for Each Role	66
5.2.4	Separation of Roles.....	66
5.3	Personnel Controls	66
5.3.1	Background, Qualifications, Experience, and Security Clearance Requirements	66
5.3.2	Background Check Procedures	67
5.3.3	Training Requirements	67
5.3.4	Retraining Frequency and Requirements.....	68
5.3.5	Job Rotation Frequency and Sequence	68
5.3.6	Sanctions for Unauthorized Actions.....	68
5.3.7	Independent Contractor Requirements.....	68
5.3.8	Documentation Supplied to Personnel	68
5.4	Audit Logging Procedures.....	69
5.4.1	Types of Events Recorded.....	69
5.4.2	Frequency of Processing Log.....	74
5.4.3	Retention Period for Audit Log	75
5.4.4	Protection of Audit Log.....	75
5.4.5	Audit Log Backup Procedures	76
5.4.6	Audit Collection System (Internal vs. External)	76
5.4.7	Notification to Event-Causing Subject	76
5.4.8	Vulnerability Assessments	76
5.5	Records Archival	77
5.5.1	Types of Events Archived	77
5.5.2	Retention Period for Archive	80
5.5.3	Protection of Archive	81
5.5.4	Archive Backup Procedures	81
5.5.5	Requirements for Time-Stamping of Records	82
5.5.6	Archive Collection System (Internal or External)	82
5.5.7	Procedures to Obtain and Verify Archive Information.....	82
5.6	Key Changeover.....	82
5.7	Compromise and Disaster Recovery	83
5.7.1	Incident and Compromise Handling Procedures.....	83
5.7.2	Computing Resources, Software, and/or Data Are Corrupted	84
5.7.3	Entity (CA) Private Key Compromise Procedures	84
5.7.3.1	CA Key Compromise Procedures.....	84
5.7.3.2	KRS Private Key Compromise Procedures	85
5.7.4	Business Continuity Capabilities after a Disaster	85
5.8	CA & RA Termination.....	85
6.0	TECHNICAL SECURITY CONTROLS	87
6.1	Key Pair Generation and Installation	87
6.1.1	Key Pair Generation	87
6.1.1.1	CA Key Pair Generation	87

6.1.1.2	Subscriber Key Pair Generation	87
6.1.1.3	CSS Key Pair Generation.....	88
6.1.1.4	PIV-I Content Signing Key Pair Generation.....	88
6.1.2	Private Key Delivery to Subscriber	88
6.1.3	Public Key Delivery to Certificate Issuer.....	89
6.1.4	CA Public Key Delivery to Relying Parties.....	89
6.1.5	Key Sizes	89
6.1.6	Public Key Parameters Generation and Quality Checking.....	91
6.1.7	Key Usage Purposes (as per X.509 v3 Key Usage Field).....	91
6.2	Private Key Protection and Cryptographic Module Engineering Controls	92
6.2.1	Cryptographic Module Standards and Controls	92
6.2.1.1	Custodial Subscriber Key Stores.....	93
6.2.2	Private Key (n out of m) Multi-Person Control.....	94
6.2.3	Private Key Escrow.....	94
6.2.3.1	Escrow of CA private signature key.....	94
6.2.3.2	Escrow of CA encryption key.....	94
6.2.3.3	Escrow of Subscriber private signature keys.....	94
6.2.3.4	Escrow of Subscriber private encryption and dual use keys Subscriber	95
6.2.4	Private Key Backup	95
6.2.5	Private Key Archival	96
6.2.6	Private Key Transfer into or from a Cryptographic Module	97
6.2.7	Private Key Storage on Cryptographic Module	97
6.2.8	Method of Activating Private Key	97
6.2.9	Method of Deactivating Private Key	98
6.2.10	Method of Destroying Private Key	98
6.2.11	Cryptographic Module Rating.....	98
6.3	Other Aspects of Key Pair Management.....	99
6.3.1	Public Key Archival.....	99
6.3.2	Certificate Operational Periods and Key Usage Periods.....	99
6.4	Activation Data	100
6.4.1	Activation Data Generation and Installation.....	100
6.4.2	Activation Data Protection.....	100
6.4.3	Other Aspects of Activation Data.....	101
6.5	Computer Security Controls	101
6.5.1	Specific Computer Security Technical Requirements.....	101
6.5.2	Computer Security Rating.....	102
6.6	Life Cycle Technical Controls	102
6.6.1	System Development Controls	102
6.6.2	Security Management Controls	103
6.6.3	Life Cycle Security Controls.....	103
6.7	Network Security Controls.....	104
6.8	Time-Stamping	105
7.0	CERTIFICATE, CRL, AND OSCP PROFILES.....	106
7.1	Certificate Profile.....	106
7.1.1	Version Number(s).....	106

7.1.2	Certificate Extensions	106
7.1.3	Algorithm Object Identifiers	107
7.1.4	Name Forms	108
7.1.5	Name Constraints	108
7.1.6	Certificate Policy Object Identifier	108
7.1.7	Usage of Policy Constraints Extension	108
7.1.8	Policy Qualifiers Syntax and Semantics.....	109
7.1.9	Processing Semantics for the Critical Certificate Policies Extension	109
7.1.10	Inhibit Any Policy Extension.....	109
7.2	CRL Profile	109
7.2.1	Version Number(s).....	109
7.2.2	CRL and CRL Entry Extensions.....	109
7.3	OCSP Profile.....	109
7.3.1	Version Number(s).....	109
7.3.2	OCSP Extensions	109
8.0	COMPLIANCE AUDIT AND OTHER ASSESSMENTS.....	110
8.1	Frequency or Circumstances of Assessment.....	110
8.2	Identity/Qualifications of Assessor	110
8.3	Assessor's Relationship to Assessed Entity.....	111
8.4	Topics Covered by Assessment.....	111
8.5	Actions Taken as a Result of Deficiency	111
8.6	Communication of Results.....	111
9.0	OTHER BUSINESS AND LEGAL MATTERS	112
9.1	Fees	112
9.1.1	Certificate Issuance or Renewal Fees.....	112
9.1.2	Certificate Access Fees.....	112
9.1.3	Revocation or Status Information Access Fees	112
9.1.4	Fees for other Services	112
9.1.5	Refund Policy	112
9.2	Financial Responsibility	112
9.2.1	Insurance Coverage	112
9.2.2	Other Assets	113
9.2.3	Insurance or Warranty Coverage for End-Entities	113
9.3	Confidentiality of Business Information	113
9.3.1	Scope of Confidential Information.....	113
9.3.2	Information not within the Scope of Confidential Information	113
9.3.3	Responsibility to Protect Confidential Information.....	113
9.4	Privacy of Personal Information	113
9.4.1	Privacy Plan.....	113
9.4.2	Information Treated as Private	113
9.4.3	Information not Deemed Private	114
9.4.4	Responsibility to Protect Private Information.....	114
9.4.5	Notice and Consent to Use Private Information	114

9.4.6	Disclosure Pursuant to Judicial or Administrative Process.....	114
9.4.7	Other Information Disclosure Circumstances	114
9.5	Intellectual Property Rights	114
9.6	Representations and Warranties.....	115
9.6.1	CA Representations and Warranties.....	115
9.6.2	RA Representations and Warranties.....	115
9.6.3	Subscriber Representations and Warranties	115
9.6.4	Relying Parties Representations and Warranties.....	115
9.6.5	Representations and Warranties of Affiliated Organizations.....	116
9.6.6	Representations and Warranties of Other Participants	116
9.7	Disclaimers of Warranties	117
9.8	Indemnities.....	118
9.9	Term and Termination.....	118
9.9.1	Term	118
9.9.2	Termination	118
9.9.3	Effect of Termination and Survival.....	118
9.10	Individual Notices and Communications with Participants.....	118
9.11	Amendments.....	119
9.11.1	Procedure for Amendment.....	119
9.11.2	Notification Mechanism and Period	119
9.11.3	Circumstances under which OID MUST be changed	119
9.12	Dispute Resolution Provisions	119
9.13	Governing Law.....	119
9.14	Compliance with Applicable Law	119
9.15	Miscellaneous Provisions.....	119
9.15.1	Entire Agreement	119
9.15.2	Assignment	119
9.15.3	Severability	120
9.15.4	Enforcement (Attorneys' Fees and Waiver of Rights)	120
9.15.5	Force Majeure	120
9.16	Other Provisions	120
APPENDIX A: PIV-INTEROPERABLE SMART CARD DEFINITION.....		121
APPENDIX B: CARD MANAGEMENT SYSTEM REQUIREMENTS.....		123
APPENDIX C: IN-PERSON ANTECEDENT		125
APPENDIX D: REFERENCES		127
APPENDIX E: ACRONYMS AND ABBREVIATIONS		128
APPENDIX F: GLOSSARY		130

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.
1.7	June 5, 2018	Review and update to align with FBCA CP Version 2.32, April 2018
1.8	April 17, 2020	Updated with latest EMS NFI PA Chair, FKPI PA changes through 2019-01
1.9	October 7th ,2021	Updated and review document to more closely aligned with FBCA CP
2.1	January 3 rd , 2024	Update of audit, suspension, and restoration requirements to align with FBCA CP version 2.3, November 3 rd , 2023
2.2	November 18, 2025	Update to alignment with updated FBCP together with NFI CPS. X.509 Certificate Policy for the Federal Bridge Certification Authority Version 3.8 August 4, 2025
3.0	July 31, 2026	Major update address structural and audit remediation, adding KRS

1.0 INTRODUCTION

This Certificate Policy (CP) governs the Entrust Managed Services Non-Federal Identity (EMS NFI) Public Key Infrastructure (PKI) and establishes requirements for the issuance and management of X.509 Certificates.

This CP defines distinct Certificate policies to support interoperability between cross-certified PKI domains. Certificates issued under this CP SHALL support interoperability with external PKIs through policy mapping to the Federal Bridge Certification Authority (FBCA) Certificate Policy. Cross-certification trust relationships SHALL be established through the use of the *policyMappings* extension in CA Certificates.

Each Certificate Policy defined in this CP corresponds to a level of assurance reflecting the strength of identity binding, private key protection, and PKI security controls. Where a requirement is not explicitly limited to a specific Certificate Policy, it SHALL apply to all Certificate Policies defined in this CP.

This CP defines the following assurance levels: Rudimentary, Basic, Medium, Medium Hardware, and PIV-I, including PIV-I Card Authentication and PIV-I Content Signing.

For the purposes of this CP, a device SHALL mean a non-person entity, including hardware devices and software applications.

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

Certification Authorities operating under this CP (NFI CAs) SHALL issue, manage, and revoke Certificates in accordance with this CP. NFI CAs SHALL bind Subscriber identities to public keys and SHALL enforce lifecycle controls consistent with the defined assurance levels.

A Key Recovery System (KRS) SHALL be implemented to support recovery of private keys associated with key management Certificates. The KRS SHALL include hardware, software, personnel, and procedures necessary to securely escrow and recover private keys. All key recovery operations SHALL be controlled, auditable, and restricted to authorized roles.

The EMS NFI Certification Practice Statement (NFI CPS) SHALL describe how the requirements of this CP are implemented. No CPS SHALL conflict with or weaken the requirements defined in this CP. Use of this CP outside the intended interoperability framework is at the risk of the relying party.

This CP follows the RFC 3647 framework.

1.1 OVERVIEW

1.1.1 Certificate Policy (CP)

Certificates issued under this CP SHALL contain one or more registered Certificate Policy object identifiers (OIDs). Each OID SHALL correspond to a defined level of assurance established by this CP

and SHALL be used by relying parties to determine whether a Certificate is trusted for a specific purpose.

Each Certificate SHALL assert the applicable policy OID in the *certificatePolicies* extension. Policy OIDs asserted in Certificates SHALL be consistent with applicable cross-certification mappings to the FBCA Certificate Policy.

Each Certificate Policy OID SHALL correspond to a level of assurance reflecting the strength of identity binding, private key protection, and PKI security controls.

Where Certificates are issued using automated signing mechanisms, the Certificate Policy OID SHALL only be asserted where all requirements for identity proofing, authorization, and signing controls are satisfied and auditable.

Certificates supporting key recovery SHALL be issued under Certificate Policies that enforce approved Key Recovery System (KRS) controls. All key recovery capabilities SHALL be implemented in accordance with this CP and SHALL be auditable and restricted to authorized roles.

1.1.2 Relationship between the CP and the CPS

This CP defines the level of assurance that may be placed in Certificates issued under this policy.

The Certification Practice Statement (CPS) SHALL describe how the Certification Authority (CA) implements the requirements of this CP to establish and maintain the stated level of assurance.

Certification Authorities issuing Certificates under this CP SHALL maintain a corresponding CPS. The CPS SHALL address all applicable requirements of this CP and SHALL not conflict with or weaken any requirement defined herein.

1.1.3 Relationship between the FBCA CP and this CP

This CP supports interoperability with the Federal Bridge Certification Authority (FBCA) Certificate Policy through cross-certification and formal policy mapping.

The FBCA issues a Cross-Certificate to Entrust NFI Certification Authorities (NFI CAs) based on successful policy mapping and compliance with FBCA requirements. This Cross-Certificate establishes a trust relationship that enables interoperability between the NFI PKI and the Federal PKI. Historically, Entrust has issued a corresponding Cross-Certificate to the FBCA to establish a bidirectional trust relationship. Entrust no longer issues a Cross-Certificate to the FBCA; however, Entrust SHALL remain capable of issuing such a Cross-Certificate and SHALL do so where required to support interoperability or as directed by governing policy authorities.

Certificate Policies defined in this CP SHALL be mapped to corresponding FBCA Certificate Policies in accordance with FBCA requirements. Such mappings SHALL establish policy equivalence based on the defined levels of assurance, including the strength of identity binding, private key protection, and PKI security controls.

Where Cross-Certification is established, the *policyMappings* extension in CA Certificates SHALL be used to express the relationships between Certificate Policies defined in this CP and those defined in the FBCA Certificate Policy.

This CP SHALL be no less stringent than the FBCA Certificate Policy for any mapped level of assurance. Where differences exist, this CP SHALL enforce requirements that meet or exceed the corresponding FBCA requirements.

Certificates issued under this CP that are intended to interoperate with the FPKI SHALL conform to all requirements necessary to support FBCA policy mapping and cross-certification.

1.1.4 Scope

This CP applies to all Certificates issued by Entrust Managed Services Non-Federal Identity (EMS NFI) Certification Authorities (CAs), including Certificates issued to CAs, devices, and affiliated personnel, including non-federal employees, contractors, and other authorized individuals.

This CP governs all Certificate types and assurance levels defined herein and SHALL apply to all NFI CAs operating under this CP. All Certificates issued under this CP SHALL conform to the requirements specified for the applicable level of assurance.

1.1.5 Interoperation with CAs Issuing under Different Policies

Interoperation with Certification Authorities (CAs) issuing Certificates under different Certificate Policies SHALL be achieved through cross-certification and policy mapping to the Federal Bridge Certification Authority (FBCA) Certificate Policy. Cross-certification relationships SHALL be established and maintained in accordance with FBCA requirements.

The *policyMappings* extension in CA Certificates SHALL be used to express relationships between Certificate Policies and SHALL ensure that relying parties can accurately determine the equivalence of assurance levels between domains.

1.2 Document Name and Identification

This document is the X.509 Certificate Policy for the Entrust Managed Services Non-Federal Identity Public Key Infrastructure (EMS NFI CP).

Each Certificate Policy defined in this CP SHALL be identified by a unique object identifier (OID) and SHALL be asserted in Certificates issued by NFI CAs.

Certificate policies defined in this CP are mapped to corresponding Federal PKI Certificate policies to support interoperability with the Federal Bridge Certification Authority (FBCA). Policy mappings SHALL establish equivalence between assurance levels in accordance with FBCA requirements. The EMS NFI Certificate policies associated with the Federal PKI Certificate Policies and EMS NFI Policies have been mapped according to the following table:

1 - Policy Object Identifier Mapping Table

Federal PKI policy Object Identifier and Name	EMS NFI policy Object Identifier and Name
2.16.840.1.101.3.2.1.3.1 <i>id-fpki-certpcy-rudimentaryAssurance</i>	2.16.840.1.114027.200.3.10.7.8 <i>id-emspki-nfssp-rudimentary-policy</i>
2.16.840.1.101.3.2.1.3.2 <i>id-fpki-certpcy-basicAssurance</i>	2.16.840.1.114027.200.3.10.7.7 <i>id-emspki-nfssp-basic-policy</i>
2.16.840.1.101.3.2.1.3.3 <i>id-fpki-certpcy-mediumAssurance</i>	2.16.840.1.114027.200.3.10.7.1 <i>id-emspki-nfssp-medium-policy</i>
2.16.840.1.101.3.2.1.3.12 <i>id-fpki-certpcy-mediumHardware</i>	2.16.840.1.114027.200.3.10.7.2 <i>id-emspki-nfssp-medium-hardware</i> 2.16.840.1.114027.200.3.10.7.4 <i>id-emspki-nfssp-medium-authentication</i>
2.16.840.1.101.3.2.1.3.37 <i>id-fpki-certpcy-mediumDevice</i>	2.16.840.1.114027.200.3.10.7.3 <i>id-emspki-nfssp-medium-devices</i>
2.16.840.1.101.3.2.1.3.14 <i>id-fpki-certpcy-medium-CBP</i>	2.16.840.1.114027.200.3.10.7.14 <i>id-emspki-nfssp-medium-CBP</i>
2.16.840.1.101.3.2.1.3.15 <i>id-fpki-certpcy-mediumHW-CBP</i>	2.16.840.1.114027.200.3.10.7.15 <i>id-emspki-nfssp-mediumHW-CBP</i>
2.16.840.1.101.3.2.1.3.19 <i>id-fpki-certpcy-pivi-cardAuth</i>	2.16.840.1.114027.200.3.10.7.13 <i>id-emspki-nfssp-pivi-cardAuth</i>
2.16.840.1.101.3.2.1.3.18 <i>id-fpki-certpcy-pivi-hardware</i>	2.16.840.1.114027.200.3.10.7.6 <i>id-emspki-nfssp-pivi-hardware</i>
2.16.840.1.101.3.2.1.3.20 <i>id-fpki-certpcy-pivi-contentSigning</i>	2.16.840.1.114027.200.3.10.7.9 <i>id-emspki-nfssp-pivi-contentsigning</i>
2.16.840.1.101.3.2.1.3.38 <i>id-fpki-certpcy-mediumDeviceHardware</i>	2.16.840.1.114027.200.3.10.7.16 <i>id-emspki-nfssp-medium-devicesHW</i>

Certificates issued to CAs MAY assert one or more of the Certificate Policy OIDs listed in Table 1, consistent with the scope of the CA and applicable cross-certification mappings.

Requirements for device Certificate policies SHALL be equivalent to the corresponding assurance levels defined in this CP, except where explicitly specified for identity proofing, re-key, or activation data controls.

Requirements for Medium Hardware and Medium Hardware commercial best practice policies SHALL be equivalent to the corresponding Medium Assurance policies, except for identity proofing, re-key, and activation data.

Requirements for PIV-I Hardware and PIV-I Content Signing policies SHALL be equivalent to Medium Hardware policies, except where explicitly modified by PIV-I-specific requirements.

Certificates asserting the PIV-I Content Signing policy SHALL be restricted to use by authorized systems for signing PIV-I card data.

End-entity Certificates issued to devices SHALL assert Certificate policies mapped to FBCA Medium Device, Medium Device Hardware, or PIV-I Content Signing policies, as applicable. Certificate policies intended for human Subscribers SHALL not be asserted for device Certificates unless all applicable requirements are met.

Certificates valid for the following policies are issued to Human Subscribers:

PIV-I Authentication Certificate	<i>id-fpki-certpcy-pivi-hardware</i>
Digital Signature certificate with the private key generated on a PIV-I credential	<i>id-fpki-certpcy-mediumHardware</i>
Key Management Certificate associated with a PIV-I credential	<i>id-fpki-certpcy-mediumAssurance</i> <i>id-fpki-certpcy-mediumHardware</i>
All other hardware-based Certificates	<i>id-fpki-certpcy-mediumHW-CBP</i> <i>id-fpki-certpcy-mediumHardware</i>
All software-based Certificates	<i>id-fpki-certpcy-rudimentaryAssurance</i> <i>id-fpki-certpcy-basicAssurance</i> <i>id-fpki-certpcy-medium-CBP</i> <i>id-fpki-certpcy-mediumAssurance</i>

Personal Identity Verification Interoperable (PIV-I) Device Subscriber Certificates valid for the following policies are issued to Device Subscribers and are limited to use with PIV-I credentials.

Card Authentication Certificate with the private key on a PIV-I credential	<i>id-fpki-certpcy-pivi-cardAuth</i>
Content Signing Certificate used to sign PIV-I data objects	<i>id-fpki-certpcy-pivi-contentSigning</i>

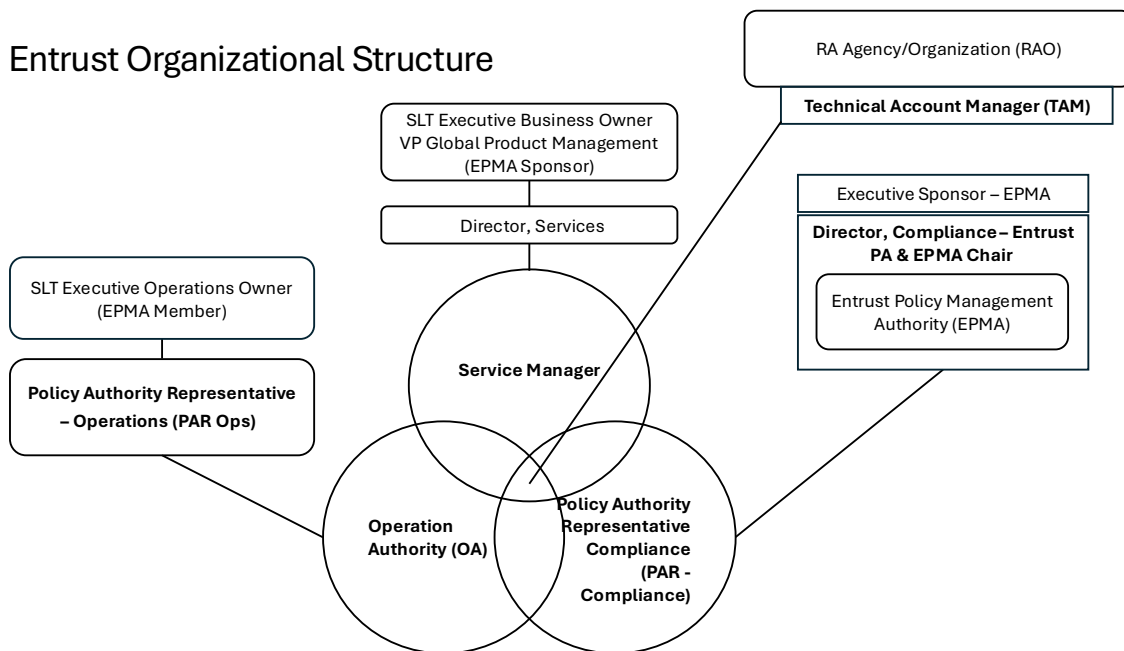
Note that:

- Requirements associated *id-fpki-certpcy-pivi-contentSigning* are identical to *id-fpki-certpcy-mediumHardware* except where specifically noted in the text.
- The *id-fpki-certpcy-pivi-contentSigning* policy is reserved for Certificates used by the Card Management System (CMS) to sign the PIV-I card security objects.

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 Policy Management Authority (EPMA)

The Entrust Policy Management Authority (EPMA) serves as the Policy Management Authority (PMA) for EMS NFI services and is responsible for maintaining this CP and for ensuring that EMS NFI components are operated in accordance with this CP and the NFI CPS.

The EPMA designates a Policy Authority (PA) to administer this CP and associated policy governance activities.

The EPMA is responsible for notifying the Federal PKI Policy Authority (FPKIPA) of any infrastructure change that has the potential to affect the Federal PKI operational environment at least two weeks prior to implementation. Any new artifacts resulting from such changes, including CA certificates, CRL Distribution Point (CRLDP) URLs, Authority Information Access (AIA) URLs, Subject Information Access (SIA) URLs, or similar PKI artifacts, SHALL be provided to the FPKIPA within 24 hours following implementation.

The EPMA is available at mpkipa@entrust.com or by mail or phone:

EPMA Chair
1187 Park Place
Shakopee, MN 55379
Office: 952-933-1223

1.3.1.2 EPMA Policy Authority Program Managers

The Policy Authority (PA) SHALL appoint a Policy Authority Representative - Operations (PAR Ops) and a Policy Authority Representative - Compliance (PAR Compliance) to assist in the administration and compliance oversight of EMS NFI services.

These representatives act on behalf of the PA within the scope of their assigned responsibilities and support operational compliance, audit activities, coordination with Registration Authorities, change management processes, and interactions with the Federal PKI community.

The detailed responsibilities and authorities of these representatives are specified in the NFI CPS and supporting procedures.

1.3.1.3 RA Agency/Organization PMA

Under this CP Each Registration Authority (RA) is required to establish a RA Policy Management Authority (RA PMA) responsible for ensuring that all on-premises EMS NFI components and internal registration processes comply with this CP and are documented in a Registration Practices Statement, reviewed, updated at least annually, and approved by the Entrust PA. The RA PMA SHALL be responsible for collaborating with Entrust to meet the FPKI annual requirements. Members of the RA PMA act as primary points of contact for the Entrust Policy Management Authority (EPMA).

1.3.1.4 Operational Authority

The Entrust PA SHALL appoint an EMS NFI Operational Authority (OA), responsible for the operational personnel, processes, physical and logical environments and change control, providing contact information for the EMS NFI RAs.

1.3.2 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 prescribe a specific PKI architecture. The policy MAY be implemented through a hierarchical PKI or mesh PKI. The CPS SHALL describe the architecture for CAs operated under this CP.

1.3.2.1 Root Certification Authorities

It is the responsibility of the PA to designate which CAs SHALL be subordinated to the Root CA. A CA that is to be designated as a Root CA for this service SHALL:

- Be cross-certified to the Federal Bridge CA.
- Not cross-certify with any other CA.
- Not issue Certificates to Subscribers as defined in Section 1.3.8.

The Root CA MAY issue Certificates for the purpose of administering Root CA or 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.

The OA SHALL ensure that no CA under EMS NFI has more than one trust path to the FBCA.

1.3.2.2 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.

1.3.3 Card Management System

If deployed by the RA, in EMS NFI a 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. The CMS SHALL not be issued any Certificates that express the *PIV-I Hardware* or *PIV-I Card Authentication* policy OIDs. CMS practices SHALL be included in the RPS.

1.3.4 Registration Authorities

The Registration Authorities (RAs) collect and verify each Subscriber’s identity and information that is to be entered into the Subscriber’s public key Certificate. The RA performs its function in accordance with a CPS approved by the Entrust PA. The RA is responsible for:

- Control over the registration process including the generation, storage and archival of audit evidence.
- The identification and authentication process including any CMS hosted by the RA.

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

1.3.4.1 Trusted Agents

A 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 RPS will identify the parties responsible for providing such services to the RA, and the mechanisms for determining their trustworthiness.

1.3.5 Certificate Status Servers

EMS NFI MAY optionally include an authority that provides status information about Certificates on behalf of a CA through on-line transactions. PKIs MAY include OCSP responders to provide on-line status information. Such an authority is termed as a Certificate Status Server (CSS). Where the CSS is identified in Certificates as an authoritative source for revocation information, the operations of that authority are considered within the scope of this CP. Examples include OCSP servers that are identified in the authority information access (AIA) extension. OCSP servers that are locally trusted, as described in RFC 6960, are not covered by this policy. Any CA that issues PIV-I Certificates under this policy MUST provide OCSP status responses.

1.3.6 Key Recovery Authorities

1.3.6.1 Key Escrow Database (KED)

The Key Escrow Database (KED) is defined as the function, system, or subsystem that maintains the key escrow repository and responds to key registration requests. The KED SHALL:

- Maintain escrowed private keys in accordance with this Certificate Policy;
- Respond to key recovery requests initiated by two or more KRAs or by a current Subscriber performing self-recovery;
- Enforce all applicable physical, technical, and procedural protections required under this policy.

1.3.6.2 Data Decryption Server

An optional element of the KRS is a Data Decryption Server (DDS), an automated system that has the capability to obtain Subscriber private keys from the KED or another DDS for data monitoring or other authorized purposes (e.g., email inspection). A DDS SHALL:

- Not provide recovered keys directly to Subscribers or other third-party human Key Requestors;
- Be considered a type of Key Requestor;
- Meet all applicable physical, personnel, procedural, and technical security requirements of the KED.

Implementation of a DDS by an organization is optional. Where implemented, the DDS SHALL be within the scope of applicable RA requirements, and documented in the RPS

1.3.6.3 Key Recovery Agent (KRA)

A Key Recovery Agent (KRA) is an individual who is authorized as specified in the NFI CPS, to approve and facilitate the recovery of escrowed keys. KRAs SHALL:

- Be considered Trusted Roles;
- Operate under multi-party control, requiring at least two KRAs to approve a key recovery request;
- Have controlled and limited access to the KED
- Not have direct access to recovered private keys beyond what is required to perform their authorized functions.

A KRA SHALL perform the following functions:

- Confirm the validity, completeness, and authorization of key recovery requests;
- Collaborate with other KRAs to approve key recovery transactions;
- Ensure that recovery actions are appropriate and in the interest of the Issuing Organization;
- Support the distribution of recovered key material or associated recovery data to the authorized Key Requestor in accordance with this policy and the CPS.

For RAs that do not use KRO, the KRAs MAY:

- Verify the identity and authorization of Key Requestors; and
- Assist Key Requestors in preparing key recovery requests;

1.3.6.4 Key Recovery Official (KRO)

RAs MAY appoint a Key Recovery Official (KRO) to support identity verification and authorization validation for key recovery requests. Note that Key Recovery Officials are referred to as “Key Recovery Officers” in the MSO-KRS system.

A KRO:

- Is not considered a Trusted Role;
- SHALL not have access to the KED or to recovered private keys.

A KRO SHALL perform the following functions:

- Verify the identity and authorization of Key Requestors; and
- Assist Key Requestors in preparing key recovery requests;
- Utilize secure communication for interactions related to key recovery;
- Participate in the distribution of recovered keys or associated recovery data in accordance with the applicable CPS.

Where personnel perform both KRO and Trusted Role functions, the organization SHALL enforce Separation of Duties requirements in accordance with this policy.

EMS NFI also maintains a ‘super’ KRO that is able to configure organizations for deployment and assign KROs as identified by the Issuing Organization. The super KRO position is held by one of the trusted roles maintaining the CA infrastructure.

1.3.7 Key Recovery Requestors

A Key Requestor is an individual or system that requests the recovery of a Subscriber's escrowed private key.

A Key Requestor MAY be:

- The Subscriber; or
- An authorized third party, internal or external, acting on behalf of the Subscriber or the organization.

All Key Requestors SHALL:

- Be authorized by the KRO
- Demonstrate verifiable authority;
- Demonstrate a legitimate need for the requested key recovery.

1.3.7.1 Internal Third-Party Requestor

An Internal Third-Party Requestor is a Key Requestor within the Issuing Organization who is authorized to request recovery of a Subscriber's key. Such authorization SHALL be granted in accordance with organizational policy and NFI CPS requirements.

1.3.7.2 External Third-Party Requestor

An External Third-Party Key Requestor is an individual outside the Issuing Organization who is authorized to request recovery of a Subscriber's private key through a valid legal instrument (e.g., a court order).

External requests SHALL:

- Be subject to validation in accordance with applicable legal and policy requirements;
- Be processed through authorized internal mechanisms as defined in the CPS;
- Comply with all applicable controls governing release of escrowed key material.

1.3.8 Subscribers

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

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

There MAY be a subset of human Subscribers that can be issued role-based Certificates. These Certificates identify a specific role on behalf of which the Subscriber is authorized to act rather than the Subscriber's name and are issued in the interest of supporting accepted business practices. The role-based Certificate can be used in situations where non-repudiation is desired. Normally, role-based Certificates are issued in addition to an individual Subscriber Certificate. A specific role MAY be identified in Certificates issued to multiple Subscribers, however, the key pair will be unique to each individual role-based Certificate (i.e. there may be four individuals carrying a Certificate issued in the role of "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).

1.3.9 Affiliated Organizations

Subscriber Certificates MAY be issued in conjunction with an organization that has a relationship with the Subscriber; this is termed affiliation. The organizational affiliation will be indicated in the Certificate. Affiliated Organizations are responsible for verifying the affiliation at the time of Certificate application and requesting revocation of the Certificate if the affiliation is no longer valid. The RPS SHALL identify any affiliated organizations.

1.3.10 Relying Parties

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

For this CP, the relying party MAY be any entity that wishes to validate the binding of a public key to the name (or role) of a Subscriber.

1.3.11 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 or RPS 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: Appropriate Certificate Uses

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

Certificates that map to *id-fpki-certpcy-pivi-cardAuth* MUST be used only to authenticate the hardware token containing the associated private key and MUST not be interpreted as authenticating the presenter or holder of the token.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The Entrust Policy Management Authority (EPMA) is responsible for all aspects of this CP.

1.5.2 Contact Person

Questions, comments and suggestions regarding this CP may be directed to the EPMA at mpkipa@entrust.com.

1.5.3 Person Determining CPS Suitability for the Policy

The Certification Practices Statement (CPS) MUST conform to this 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 EPMA SHALL make the determination that a CPS complies with this policy. The signature of the Entrust PA SHALL be evidence of such determination. 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. All RAs operating under this policy SHALL maintain an RPS, submitting updates to the EPMA for approval on an annual basis. All RAs SHALL submit the results of their annual RA Compliance Audit (or other approved assessment mechanism). The Entrust PA SHALL make these documents and results available to the FPKIPA. NFI CAs and RAs are not permitted to issue waivers for any CP requirement; if a change is required the Entrust PA will inform the FPKIPA and amend the CP in a mutually agreed manner.

1.6 Definitions and Acronyms

See Appendix E and Appendix F.

2.0 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

EMS NFI SHALL maintain repositories to support the publication and distribution of information required by this CP. The repository SHALL make available applicable Certificate status information, CP, CPS documents, and other information identified in this CP as publicly available. Entrust repositories SHALL provide access consistent with the availability requirements specified in this CP and the NFI CPS.

Repository information SHALL be protected against unauthorized addition, deletion, modification, or destruction. Entrust SHALL implement appropriate logical, physical, administrative, and procedural controls to protect repository systems and the information contained within them.

Entrust SHALL ensure that repository information is published in a timely manner and remains accurate, complete, and consistent with applicable operational records.

Where Certificate status information is provided through CRLs, OCSP services, delegated OCSP responders, or other approved status mechanisms, such services SHALL operate in accordance with the requirements of this CP and the NFI CPS.

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.
- 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 Subscriber Certificates SHALL contain valid Uniform Resource Identifiers (URIs) that are publicly accessible for the purposes of certification path building and revocation checking.

All NFI CAs that issue CA Certificates SHALL publish all CA Certificates they issue in a file available via a publicly accessible HTTP URI. This URI SHALL be asserted in the Subject Information Access (SIA) extension of all applicable CA Certificates. The file SHALL be a certs-only Cryptographic Message Syntax file with a .p7c extension.

With the exception of self-signed Certificates, all CA Certificates SHALL be published by the subject CA in a file available via a publicly accessible HTTP URI. This URI SHALL be asserted in the Authority Information Access (AIA) extension of all applicable Certificates issued by that CA. The repository SHALL contain either:

- A binary (DER encoded) certs-only Cryptographic Message Syntax file with a .p7c extension and an HTTP response content type of application/pkcs7-mime; or
- A single binary (DER encoded) Certificate with a .cer extension and an HTTP response content type of application/pkix-cert.

The certs-only Cryptographic Message Syntax format is preferred as it permits publication of zero, one, or multiple CA Certificates as needed to support certification path validation.

The publicly accessible repository system mechanisms and procedures SHALL be designed to ensure that CA Certificates and Certificate Revocation Lists (CRLs) are available for retrieval twenty-four (24) hours per day, seven (7) days per week, with a minimum annual availability of 99 percent. Scheduled downtime SHALL not exceed 0.5 percent annually.

A Certificate Status Server (CSS) provides status information about Certificates on behalf of a CA through online transactions.

NFI CAs supporting PIV-I SHALL provide a CSS in the form of a delegated Online Certificate Status Protocol (OCSP) service, as specified in RFC 6960. The OCSP service SHALL provide Certificate status information for Subscriber Certificates through a publicly accessible HTTP URI identified in the Authority Information Access (AIA) extension. Operation of the delegated OCSP service is within the scope of this CP.

Pre-generated OCSP responses MAY be created by the CSS and distributed to OCSP responders. OCSP responses, like CRLs, are publicly distributable information. OCSP responders that do not perform OCSP response signing SHALL be subject to the same security requirements as repositories hosting CRLs.

Locally trusted OCSP services as described in RFC 6960 are outside the scope of this CP.

2.2.2 Publication of CA Information

The Entrust Non-Federal Identities PKI (EMS NFI) CP SHALL be publicly available on the Entrust website. The CPS will not be published; however, a redacted version of the CPS will be publicly available from the Entrust website <https://www.entrust.com/legal-compliance/federal-pki>.

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 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.

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

2.4 Access Controls on Repositories

The Entrust PA SHALL protect repository information not intended for public dissemination or modification. CA Certificates and Certificate status information issued to the EMS NFI 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.

3.0 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

This CP establishes requirements for both subject distinguished names and subject alternative 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

3.1.1.1 Subject Names

Certificates issued to Subscribers MUST include distinguished names that are comprised of a base distinguished name (Base DN) and additional relative distinguished names (RDNs). A Device Subscriber name MUST be a unique name for the device and MUST not take the form of a Human Subscriber name.

For PIV-I Card Authentication Subscriber Certificates, use of the Subscriber's common name is prohibited, instead a serialNumber=UUID is required and MUST be encoded within the serialNumber attribute using the UUID string representation defined in Section 3 of [RFC 4122].

PIV-I Hardware Certificates MAY be issued to individuals external to the entity operating the CA. Such individuals may or may not be affiliated with an organization. In these cases, the PIV-I Hardware Certificates MUST indicate whether or not the Subscriber is associated with an Affiliated Organization by taking one of the following forms:

For PIV-I Hardware Certificates with an Affiliated Organization:

- cn=Subscriber's full name, ou=Affiliated Organization Name, {Base DN}

For PIV-I cardAuth Certificates with an Affiliated Organization:

- serial number=UUID, ou=Affiliated Organization Name, {Base DN}

For PIV-I Hardware Certificates with no Affiliated Organization:

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

For PIV-I cardAuth Certificates with no Affiliated Organization:

- serial number=UUID, ou=Unaffiliated, ou=Entity CA's Name, {Base DN}

This requirement does not apply to CAs that issue PIV-I Certificates only to a single organization, designated in the CA issuer name.

PIV-I Content Signing Certificates MUST clearly indicate the organization administering the CMS.

Role-based and group Certificates MAY be issued under any non-PIV-I human Subscriber policy.

- Role-based Certificates identify a specific role on behalf of which one or more Subscribers are authorized to act rather than the Subscriber's name. Where the organization is implicit in the role, it may be omitted. Where the role alone is ambiguous, the organization MUST be present in the DN.
- The *subjectName* DN in a group Certificate MUST not imply that the subject is a single individual, e.g., by inclusion of a human name form

3.1.1.2 Subject Alternative Names

PIV-I Hardware and PIV-I Card Authentication Certificates MUST include a subject alternate name extension, containing a UUID value encoded as a URI as specified in Section 3 of [RFC 4122].

PIV-I Card Authentication Certificates MUST not include any other name in the subject alternative name extension.

Subscriber Certificates that contain *id-kp-emailProtection* in the EKU MUST include a subject alternative name extension that includes a *rfc822Name*.

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

3.1.2 Need for Names to Be Meaningful

Names used in Certificates issued by Certification Authorities operating under this CP SHALL identify the person, device, system, organization, or other entity to which they are assigned in a meaningful and non-misleading manner.

The subject name in CA Certificates SHALL match the issuer name contained in Certificates issued by that CA, in accordance with RFC 5280.

When Distinguished Names (DNs) are used:

- The directory information tree SHALL accurately reflect organizational structures.
- The Common Name (CN) SHALL identify the Subscriber in a manner that is easily understandable by humans.
- For Certificates issued to human Subscribers, the Common Name SHALL equal the Subscriber's legal name or other verified name authorized under this CP.
- For PIV-I Hardware Certificates and other Certificate types where subject naming requirements are prescribed, the Common Name (CN=) SHALL represent the Subscriber's full verified name.
- The Common Name SHALL comply with namespace uniqueness requirements and SHALL not be misleading.
- Nothing in this section prohibits the use of pseudonymous Certificates as permitted under Section 3.1.3.
- Names assigned to devices SHALL identify the device, system, application, or service in a meaningful manner consistent with the purpose of the Certificate.

When User Principal Names (UPNs) are used, the UPN SHALL:

- Be unique within the applicable namespace.
- Accurately reflect organizational assignments and naming conventions.
- Not be misleading or falsely imply an affiliation, authorization, or identity not possessed by the Subscriber.

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, and limited to, 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.

CAs MAY issue role-based or group Certificates that identify subjects by their organizational roles. Each identified 'role' or 'group' MUST meet name space uniqueness requirements.

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]. Rules for interpreting PIV-I Certificate UUID names are specified in [RFC 4122].

3.1.5 Uniqueness of Names

Name uniqueness MUST be enforced by all NFI CAs under this policy.

The CA is responsible for ensuring name uniqueness in Certificates issued by EMS NFI. 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 EPMA 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 affiliated organization MUST be identified in the RPS.

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

For each Certificate issued under this CP, the Certification Authority (CA), either directly or through an authorized Registration Authority (RA), SHALL authenticate the identity of the individual requestor or authorized representative of the requesting entity.

PIV-I Hardware Certificates SHALL be issued only to human Subscribers whose identity has been authenticated in accordance with the requirements of this CP.

Subscriber Certificates MAY be issued based on an electronically authenticated request using a valid signature Certificate or authentication Certificate and the associated private key, provided that:

- The assurance level of the newly issued Certificate is the same as or lower than the assurance level of the Certificate used to authenticate the request.
- The identity information contained in the newly issued Certificate matches the identity information contained in the Certificate used to authenticate the request.

- The validity period of the newly issued Certificate SHALL NOT extend beyond the next required identity proofing or identity authentication event associated with the Certificate used to authenticate the request.
- Issuance of a Certificate based solely on electronic authentication SHALL NOT modify or extend the Subscriber's required identity proofing or identity authentication schedule.

For Certificates issued to devices, systems, applications, or other non-person entities, the CA or RA SHALL authenticate the identity and authorization of the individual requestor acting on behalf of the sponsoring organization, known as the Human Sponsor, and SHALL verify the association between the Certificate subject and the requesting organization.

3.2.3.1 Authentication of Human Subscribers

For Subscribers, the CA and associated RAs SHALL ensure that the Applicant's identity information is verified in accordance with the process established by this CP and the NFI CPS. Identity proofing processes SHALL depend upon the Certificate level of assurance and SHALL be addressed in the NFI CPS.

For Medium Assurance and Medium Hardware Assurance, identity SHALL be established no more than thirty (30) days before initial Certificate issuance.

For each Certificate issued, the CA or RA SHALL record the following information:

- A signed declaration by that person that the identity of the Applicant was verified as required, using the format set forth at 28 U.S.C. 1746, declaration under penalty of perjury, or a comparable procedure under applicable law; or
- An auditable record linking the authentication of the person performing the identification to that person's verification of the Applicant.
- If in-person identity proofing is performed, a unique identifying number from the Applicant's identity document, or a facsimile of the identity document.
- If electronic authentication is performed, a unique identifying number or other unique identifier from the signature or authentication Certificate used to authenticate the request, such as Certificate serial number, thumbprint, subject key identifier, or public key.
- The date of the verification.
- Either:
 - An auditable record indicating that the Applicant accepted the Certificate; or
 - A declaration of identity signed by the Applicant using a handwritten signature or appropriate digital signature, 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 a comparable procedure under applicable law.

In cases where 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 assurance levels except PIV-I, where an Applicant is unable to appear in person, the Applicant **MAY** be represented by a trusted person already issued a digital Certificate by the Entity. This process **SHALL** be treated as reliance on an in-person antecedent. The trusted person **SHALL** present information sufficient for registration at the assurance level of the Certificate being requested, for both the trusted person and the Applicant represented by the trusted person.

For Basic and Medium Assurance, an entity certified by a State or Federal Entity as authorized to confirm identities **MAY** perform in-person authentication on behalf of the RA and **MAY** be considered a Trusted Agent. The certified entity **SHALL** forward the information collected from the Applicant directly to the RA in a secure manner. Tamper-evident packages or other secure transmission methods **MAY** be used. Such authentication **SHALL NOT** relieve the RA of responsibility to verify the presented data.

For PIV-I Certificates, PIV-I Hardware Certificates **SHALL** be issued only to human Subscribers. PIV-I identity proofing **SHALL** be performed in accordance with the requirements for issuing PIV credentials. The use of an in-person antecedent **SHALL NOT** be permitted for PIV-I Certificates.

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:

- An electronic facial image used for printing the facial image on the card and for performing visual authentication during card usage. A new facial image **SHALL** be collected each time a card is issued.
- 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	<p>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.</p> <p>Address confirmation:</p> <ol style="list-style-type: none"> 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.

Assurance Level	Identification Requirements
Medium (all policies)	<p>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 or supervised remote registration; information provided SHALL be verified to ensure legitimacy. Credentials required are one Federal Government-issued Picture I.D., one REAL ID Act compliant picture ID, or two Non-Federal Government I.D.s, one of which SHALL be a photo I.D. Any credentials presented MUST be unexpired.</p> <p>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.</p>

In the event an applicant is denied a credential based on the results of the identity proofing process, the applicant MAY submit an appeal requesting redress of the decision to the EPMA detailed in Section 1.5.2.

3.2.3.2 Authentication of Human Subscribers for Role-based Certificates

Roles for which role-based Certificates MAY be issued are limited to those that uniquely identify a specific role within an organization (e.g., *Chief Information Officer* is a unique role whereas *Program Analyst* is not). Role-based Certificates:

- MUST not be shared.
- MUST be issued to individual Subscribers and protected in the same manner as individual Certificates.

CAs MUST 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 Entity 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 MUST validate that the individual either holds that role or has been delegated the authority to sign on behalf of the role.

3.2.3.3 Authentication of Human Subscribers for Group Certificates

For each Certificate issued, the CA MUST authenticate the identity of the individual requestor. Normally, a Certificate SHALL be issued to a single Subscriber. Where multiple individuals act in a

common capacity and non-repudiation is not required, a Certificate MAY be issued that corresponds to a private key shared among multiple authorized Subscribers.

Prior to issuance of a group Certificate, the RA SHALL authenticate the identity of a sponsor from the Information Systems Security Office (ISSO), or equivalent authority, and SHALL record the information required by Section 3.2.3.1.

In addition to authentication of the sponsor, the following requirements SHALL apply:

- The Information Systems Security Office, or equivalent authority, SHALL be responsible for controlling the shared private key, maintaining a current list of authorized Subscribers with access to the private key, and maintaining accountability for which Subscriber had custody or use of the private key at any given time.
- The subject distinguished name (DN) SHALL NOT imply that the Certificate represents a single individual, including through the use of an individual human name.
- A current list of individuals authorized to access or use the shared private key SHALL be provided to and retained by the applicable CA or its designated representative.
- Token issuance, key generation, key storage, key recovery, private key protection, Certificate acceptance, and Subscriber obligations associated with group Certificates SHALL comply with all other applicable requirements of this CP.
- Group Certificates SHALL NOT be issued where individual accountability or non-repudiation is required.
- For each Certificate issued, the CA or RA SHALL authenticate the identity of the individual requestor acting on behalf of the group and SHALL verify the requestor's authority to obtain the Certificate.

3.2.3.4 Authentication of Devices

Some computing and communications devices, services, and software applications (e.g., routers, firewalls, servers, applications, and services) MAY be named as Certificate subjects. In such cases, the device, service, or application SHALL have an identified human sponsor. The sponsor SHALL be authenticated in accordance with the requirements of Section 3.2.3.1 and SHALL be responsible for the accuracy of registration information, authorization of Certificate requests, and protection of the associated private keys.

The sponsor SHALL provide the following registration information:

- Equipment identification (e.g., serial number), service name (e.g., DNS name), or unique software application identifier.
- Equipment, service, or software application public keys.
- Applicable authorizations and attributes to be included in the Certificate.
- Contact information sufficient to permit communication with the sponsor when required.

Device Certificates SHALL be issued only to devices, services, or software applications under the control of the sponsoring organization. Issuance SHALL require registration and validation activities

that meet all applicable organizational requirements. Prior to Certificate renewal or re-issuance, the continued authorization and validity of the device registration information SHALL be revalidated.

Where a sponsor changes, the new sponsor SHALL review the status of each device, service, or application under their sponsorship and SHALL confirm that continued Certificate issuance remains authorized.

The CPS and applicable RPS SHALL describe the procedures used to maintain Certificate accountability, sponsor accountability, and authorization records throughout the Certificate lifecycle.

Registration information SHALL be verified to an assurance level commensurate with the assurance level of the Certificate being issued. For Certificates asserting the mediumDevice and mediumDeviceHardware Certificate policies, registration information SHALL be verified commensurate with Medium Assurance requirements.

Acceptable methods for authenticating the sponsor and verifying registration information include, but are not limited to:

- Verification of digitally signed requests submitted by the sponsor using a Certificate of equivalent or greater assurance than the Certificate being requested.
- In-person identity proofing of the sponsor in accordance with Section 3.2.3.1.

The CA or RA SHALL verify both the identity of the sponsor and the sponsor's authority to request Certificates on behalf of the device, service, or software application before issuance.

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.

Under no circumstances SHALL any Certificate have more than one intentional trust path to the FBCA, irrespective of extension processing.

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

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. <i>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.</i>
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.

3.5 Identification and Authentication for Key Recovery Requests

This section applies to CAs that support Key Recovery Services (KRS).

3.5.1 KRA Authentication

KRAs SHALL authenticate to Key Escrow Databases (KEDs), Data Decryption Servers (DDSs), or other KRS components using approved authentication mechanisms.

Where public key Certificates are used for authentication, the Certificate SHALL be issued by the governing organization or an authorized CA and SHALL assert an assurance level equal to or greater than that of the Certificate whose corresponding private key is being recovered.

Authentication credentials and cryptographic modules used to support key recovery operations SHALL comply with the requirements specified in this CP and the EMS NFI CPS.

3.5.2 KRO Authentication

KROs SHALL be authenticated prior to authorizing, approving, or performing key recovery operations.

Authentication SHALL be performed using credentials issued by the governing organization or an authorized CA. The assurance level of the authentication credential SHALL be equal to or greater than that of the Certificate whose corresponding private key is being recovered.

The CPS SHALL describe the controls, approval processes, and role separation requirements applicable to KROs.

3.5.3 Subscriber Authentication

Subscribers requesting recovery of their private keys SHALL be authenticated prior to the initiation of any key recovery operation. Subscriber identity MAY be established using valid public key Certificates issued by the associated PKI at an assurance level equal to or greater than that of the Certificate whose corresponding private key is being recovered. Where Certificate-based authentication cannot be used or adequately verified, identity verification SHALL be performed in accordance with the requirements specified in Section 3.2.3.1.

For automated self-recovery processes, the Subscriber SHALL authenticate using a valid Certificate at an assurance level equal to or greater than that of the Certificate whose corresponding private key is being recovered.

3.5.4 Third-Party Key Requestor Authentication

Third-party Key Requestors SHALL be authenticated and authorized prior to initiating or approving a key recovery request on behalf of a Subscriber. The KRA or KRO SHALL verify both the identity of the Key Requestor and the Key Requestor's authority to request recovery of the private key. Identity authentication SHALL be commensurate with the assurance level of the Certificate associated with the key being recovered and MAY be performed using:

- Identity proofing procedures specified in Section 3.2.3; or

- Certificate-based authentication using current, valid, and unrevoked public key Certificates at an assurance level equal to or greater than that of the Certificate whose corresponding private key is being recovered.

The CPS SHALL describe the circumstances under which third-party key recovery requests are permitted and the applicable authorization requirements.

3.5.5 Authentication of Data Decryption Servers

Data Decryption Servers (DDSs) participating in key recovery operations SHALL authenticate to KRS components using Certificates issued by EMS NFI.

The assurance level of the DDS authentication credential SHALL be equal to or greater than the highest assurance level of encryption Certificates supported by the associated KRS.

The CPS SHALL describe the technical and procedural controls used to authenticate DDS components and protect recovered key material.

4.0 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

The Certificate application process **MUST** be documented in the RPS and provide sufficient information to:

- Establish the Applicant's authorization by the employing or sponsoring agency to obtain a Certificate. See Section 3.2.3 for requirements.
- Establish and record the identity of the Applicant. See Section 3.2.3 for requirements.
- Obtain the Applicant's public key and verify the Applicant's possession of the private key. See Section 3.2.3 for requirements.
- Verify the information included in the Certificate.

These steps may be performed in any order, but all **MUST** be completed before Certificate issuance.

This section specifies requirements for initial application for Certificate issuance.

Subscribers to this PKI **SHALL** be limited to those individuals filling Trusted Roles within EMS NFI and the employees, contractors, business partners and affiliates of EMS NFI PKI customer organizations.

4.1.1 Who Can Submit a Certificate Application

No stipulation beyond 4.1 above.

4.1.2 Enrollment Process and Responsibilities

All communications supporting the Certificate application and issuance process **MUST** be authenticated and protected from modification. Communications **MAY** be electronic or out-of-band.

Any electronic communication of shared secrets **MUST** be protected.

Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair **MUST** be used.

Out-of-band communications **MUST** protect the confidentiality and integrity of the data.

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

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

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

The Entrust OA will ensure that applications for cross-certification are not accepted.

4.2 Certificate Application Processing

Information in Certificate applications SHALL be verified by the RA, or its delegate, before Certificates are issued. Requirements for information verification are defined in the CPS, while RA practices MUST be captured in the RPS.

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 and MUST be documented in the RPS.

RAs and their delegates, LRAs, are responsible for authenticating the Subscriber's identity. The RA PMA 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

The Entrust Policy Authority will reject all requests for Cross-Certificates with any external CA.

For all other Certificates, approval or rejection of Certificate applications is at the discretion of the Entrust Policy Authority and the RAO.

4.2.3 Time to Process Certificate Applications

Certificate applications MUST be processed and a Certificate issued within 90 days of identity verification.

4.3 Issuance

4.3.1 CA Actions during Certificate Issuance

Upon receiving 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 and the RAO RPS.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

For Certificates issued to Subscribers appearing before an RA or LRA, Certificate issuance is immediate. Certificates SHALL be delivered to the Subscriber's token, smart card, or other approved storage mechanism. The system SHALL provide immediate feedback to the Subscriber that Certificate issuance has been completed and that the token, smart card, or other approved storage mechanism may be removed.

For PIV-I Certificates, the CA SHALL inform the Subscriber that the Certificate has been created and SHALL make the Certificate available to the Subscriber.

When issuing device Certificates, the sponsor SHALL provide the activation codes and Certificate Signing Request (CSR) through an approved registration interface. Upon successful validation of the activation codes and acceptance of the CSR, the system SHALL generate the Certificate and SHALL provide notification to the sponsor that Certificate issuance has been completed. Where Certificates are automatically installed or delivered directly to devices, services, or applications, successful installation or Certificate availability MAY constitute notification of issuance.

The CA SHALL notify the applicable Subscriber, sponsor, or authorized representative when Certificate issuance is not an integral component of the issuance process.

4.4 Certificate Acceptance

Before a Subscriber may make effective use of a private key and associated Certificate, the CA, RA, or LRA, as applicable, SHALL provide the Subscriber with the responsibilities and obligations defined in Section 9.6.3 and SHALL obtain the Subscriber's acceptance of those obligations through a Subscriber Agreement or equivalent documented acknowledgement.

The RA SHALL document the acceptance process in the applicable RPS and SHALL identify the methods used to archive Subscriber Agreements and make them available for audit and compliance purposes.

Use of a Certificate or the associated private key SHALL constitute final acceptance of the Certificate and the Subscriber's obligations under this CP.

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. PIV-I authentication and card authentication Certificates MUST not be distributed via public repositories.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The Entrust Policy Authority (PA) SHALL be notified whenever a Certification Authority (CA) operating under this CP issues a new CA Certificate or issues a new inter-organizational cross-Certificate.

The Entrust PA SHALL notify the Federal PKI Policy Authority (FPKIPA) at least two (2) weeks prior to the issuance of a new CA Certificate or new inter-organizational Cross-Certificate. The notification SHALL assert that the proposed issuance does not introduce multiple certification paths to the Federal Bridge Certification Authority (FBCA).

All artifacts resulting from the issuance, including CA Certificates, CRL Distribution Point (CRL DP) locations, Authority Information Access (AIA) locations, Subject Information Access (SIA) locations, and related repository information, SHALL be provided to the FPKIPA within twenty-four (24) hours of issuance.

The process for notification and artifact submission SHALL be governed by the applicable Memorandum of Understanding (MOU), Memorandum of Agreement (MOA), or other governing agreement 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 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.

PIV-I Certificates MUST not be renewed, except during recovery from CA key compromise (see Section 5.7.3). In such cases, the renewed Certificate MUST expire as specified in the original Subscriber Certificate.

CA Certificates and Delegated OCSP responder Certificates MAY be renewed so long as the aggregated lifetime of the private key does not exceed the requirements specified in Section 6.3.2.

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.

When a CA re-keys, it MAY renew the Certificates it has issued.

When Certificates are renewed as a result of CA key compromise, as described in Section 4.6.1, the CA or RA MUST verify all Certificates issued since the date of compromise were issued appropriately. If the Certificate cannot be verified, then it MUST not be renewed.

4.6.4 Notification of New Certificate Issuance to Subscriber

Refer to 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

The EMS NFI Root CA issues Certificates to EMS NFI Issuing CAs. The OA SHALL notify the FPKIPA at least two weeks prior to the issuance of a CA Certificate, whenever possible. The CAs operating under this policy do not issue Certificates to non-NFI CAs.

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

NFI CAs support Certificate re-key services in accordance with the requirements of this CP and the EMS CPS. Re-key is the process of issuing a new Certificate associated with a newly generated key pair while maintaining the existing Subscriber identity and authorization information. Prior to re-key, the CA or RA SHALL verify that the Subscriber remains authorized to receive the Certificate and that the information associated with the Certificate remains valid. Examples of circumstances that may require Certificate re-key include:

- Expiration of a Certificate or key usage period.
- Suspected or confirmed compromise of a private key.
- Loss, replacement, failure, or upgrade of a cryptographic token or hardware device.
- Cryptographic algorithm or key length transitions.
- Changes to Certificate profiles, policies, or technical requirements requiring issuance of a new key pair.

The CPS SHALL describe the procedures and controls used to support Certificate re-key, including any requirements for identity revalidation, authorization verification, and key generation.

For Certificates asserting *Medium*, *mediumHardware*, *mediumDevice*, *mediumDeviceHardware*, *PIV-I*, or other higher-assurance policies, re-key SHALL be performed in a manner commensurate with the assurance level of the Certificate being re-keyed.

4.7.2 Who May Request Certification of a New Public Key

The OA MAY request Certification of a new public key for a CA operating under this CP, including where required to support Cross-Certification with the Federal Bridge Certification Authority (FBCA).

Subscribers with a currently valid Certificate MAY request certification of a new public key in accordance with the requirements of this CP and the applicable CPS.

Certification Authorities (CAs) and Registration Authorities (RAs) MAY request certification of a new public key on behalf of a Subscriber where authorized to do so.

For device Certificates, the human sponsor of the device, service, or software application MAY request certification of a new public key on behalf of the Certificate subject.

For CA Certificates and Delegated OCSP Responder Certificates, the applicable Operational Authority MAY request certification of a new public key on behalf of the subject Certificate.

Where re-key services are supported, requests SHALL only be accepted from authorized parties and SHALL be subject to the identification, authentication, and authorization requirements defined in Sections 3.2 and 3.3 of this CP.

CAs and RAs MAY initiate re-key of Subscriber Certificates without a corresponding Subscriber request where required to maintain compliance with this CP, support cryptographic transitions, replace compromised or deprecated cryptographic material, respond to operational or security events, or otherwise maintain the integrity and security of the PKI.

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

Subscribers will be notified of new Certificate issuance per the requirements in 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 SHALL be published as specified in Section 2.2.1.

Publication of Subscriber Certificates, where supported, SHALL be performed in accordance with the NFI CPS and applicable privacy requirements.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Notification of Certificate issuance resulting from a re-key operation SHALL be performed in accordance with Section 4.4.3.

Where re-key results in the issuance of a new CA Certificate, Cross-Certificate, Delegated OCSP Responder Certificate, or other Certificate requiring notification under Section 4.4.3, all applicable notification and artifact submission requirements SHALL apply.

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

A Certificate MAY be modified through issuance of a replacement Certificate where the characteristics of the Certificate or Subscriber have changed and continued use of the existing Certificate is no longer appropriate.

Examples of circumstances that MAY require Certificate modification include:

- Changes to Subscriber identity information, such as a legal name change.
- Changes to organizational affiliation, authorizations, or Certificate attributes.
- Changes to Certificate Policy object identifiers (OIDs) or other Certificate extensions.
- Changes to CA Certificate characteristics or Cross-Certification requirements.
- Correction of Certificate information that was inaccurate at the time of issuance.

Certificate modification SHALL be performed in accordance with the applicable identification, authentication, authorization, Certificate issuance, and acceptance requirements defined in this CP.

The CPS SHALL describe the procedures and controls used to support Certificate modification.

4.8.2 Who May Request Certificate Modification

The OA MAY request modification of CA Certificates and Cross-Certificates issued under this CP where changes to Certificate characteristics, policies, extensions, or operational requirements necessitate issuance of a modified Certificate.

For CA Certificates and Delegated OCSP Responder Certificates, the OA MAY request Certificate modification on behalf of the Certificate subject.

Subscribers holding a currently valid Certificate MAY request modification of their Certificates where changes to Subscriber information, authorizations, affiliations, Certificate attributes, or other Certificate characteristics require issuance of a modified Certificate.

Certification Authorities (CAs) and Registration Authorities (RAs) MAY request Certificate modification on behalf of a Subscriber where authorized to do so.

For device Certificates, the human sponsor of the device, service, or software application MAY request modification of the Certificate on behalf of the Certificate subject.

All Certificate modification requests SHALL be subject to the identification, authentication, and authorization requirements specified in Sections 3.2 and 3.3 of this CP.

The CPS SHALL describe the procedures and controls used to support Certificate modification requests.

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

Modified Certificates SHALL be published in accordance with the repository and publication requirements specified in Sections 2.2.1 and 4.4.2, as applicable.

Where a modified Certificate replaces an existing Certificate, the CA SHALL ensure that the replacement Certificate is made available through the appropriate repositories and distribution mechanisms consistent with the Certificate type and applicable CP.

CA Certificates, Delegated OCSP Responder Certificates, Cross-Certificates, and other Certificates required to be publicly available SHALL be published in the applicable repositories following issuance of the modified Certificate.

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.

The Entrust OA SHALL notify the FPKIPA at least two weeks prior to the revocation of a CA Certificate, whenever possible. The process for notification is described in the MOA between

Entrust and the FPKIPA. For emergency revocation, CAs SHALL follow the notification procedures in Section 5.7.

4.9.1 Circumstances for Revocation

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

NFI CAs 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 RA PMA to inform 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

EMS NFI 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 RA or EMS NFI.
- 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 Certificates is mandatory. Even where all the above conditions have been met, revocation of the associated Certificates is recommended.

If it is determined that a private key used to authorize the issuance of one or more Certificates may have been compromised, all Certificates directly or indirectly authorized by that private key since the date of actual or suspected compromise SHALL be revoked or SHALL be verified as appropriately issued.

If it is determined that revocation is required, 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.

An RA 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. RA responsibilities SHALL be documented in the CPS and RPS.

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.

Where key compromise is confirmed, the RAs are required to request revocation within one hour of confirmation of the compromise.

See Section 9.6.3.

4.9.5 Time within which CA must Process the Revocation Request

CAs SHALL 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.

CA Certificates are revoked once all necessary notification periods have elapsed.

4.9.6 Revocation Checking Requirements for Relying Parties

It is the responsibility of the Relying Party to determine the necessity and frequency of revocation status checking based upon the value, sensitivity, and risk associated with the transaction.

Relying Parties SHOULD validate Certificate status in accordance with RFC 5280 and applicable Certificate validation requirements prior to relying upon a Certificate.

Relying Parties MAY obtain Certificate status information through Certificate Revocation Lists (CRLs), Online Certificate Status Protocol (OCSP) services, or other status mechanisms supported by the CA and identified in the Certificate.

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	
	Online CA	Offline CA
Rudimentary	No Stipulation	No Stipulation
Basic	24 Hours	35 Days
Medium (all policies)	24 Hours	35 Days
PIV-Card Authentication	24 Hours	35 Days

CAs MAY be operated in an off-line manner 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 never exceed 35 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

NFI CAs operate as online CAs. CRLs SHALL be published within 4 hours of generation. 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 operating under this CP SHALL support online Certificate status checking through the Online Certificate Status Protocol (OCSP) in accordance with RFC 6960.

For PIV-I Certificates, CAs operating under this CP SHALL provide Certificate status information through OCSP services.

The latency of Certificate status information distributed through OCSP responders or delegated OCSP responders SHALL meet or exceed the CRL issuance and publication requirements specified in Section 4.9.7.

OCSP services and delegated OCSP responders SHALL be designed, implemented, operated, and maintained with sufficient resources to provide a response time of ten (10) seconds or less under normal operating conditions.

OCSP services and delegated OCSP responders SHALL meet the availability requirements specified in Section 2.2.1, including a minimum annual availability of 99 percent and scheduled downtime not exceeding 0.5 percent annually.

Where delegated OCSP responders are used, they SHALL operate in accordance with this CP and the applicable CPS.

4.9.10 On-line Revocation Checking Requirements

Relying Parties are responsible for determining the extent to which Certificate revocation status information is required prior to relying upon a Certificate.

Where online Certificate status checking is available, Relying Parties SHOULD obtain Certificate status information through supported Online Certificate Status Protocol (OCSP) services and/or Certificate Revocation Lists (CRLs) in accordance with RFC 5280 and applicable Certificate validation requirements.

Where online Certificate status checking is unavailable for a Certificate, Relying Parties SHALL use the most current applicable CRL to determine Certificate status.

The availability of CRLs and OCSP services does not relieve the Relying Party of responsibility for performing Certificate validation appropriate to the transaction being conducted.

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:

- Be described in the CA's approved CPS.
- Provide authentication and integrity services commensurate with the assurance level of the Certificate being verified.
- 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 CA Certificate SHALL be revoked and a CRL SHALL be published at the earliest feasible moment 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

Certificate suspension MAY be supported for Subscriber Certificates where permitted by the NFI CPS and Certificate profile.

Certificate suspension SHALL NOT be permitted for CA Certificates, Delegated OCSP Responder Certificates, Cross-Certificates, or Trusted Role Certificates.

Where Certificate suspension is supported, the CPS SHALL define the conditions, approval requirements, duration limits, notification requirements, and processing procedures for suspension and restoration.

A suspended Certificate MAY be restored to valid status when the condition that resulted in suspension has been resolved and the CA has verified that restoration is appropriate. Restoration requests SHALL be subject to authentication and authorization requirements commensurate with the assurance level of the Certificate being restored.

Restoration of a suspended Certificate SHALL be recorded in applicable audit logs and SHALL be reflected in Certificate status information provided through CRLs and OCSP services, as applicable.

Where restoration is not permitted or cannot be performed, the Certificate SHALL be revoked and a replacement Certificate SHALL be issued in accordance with this CP and the CPS.

4.9.14 Who Can Request Suspension

A Subscriber holding a suspended Certificate MAY request restoration of that Certificate.

For device Certificates, the human sponsor of the device, service, or software application MAY request restoration of the Certificate on behalf of the Certificate subject.

Certification Authorities (CAs) and Registration Authorities (RAs) MAY request restoration of a Certificate on behalf of a Subscriber where authorized to do so.

For CA Certificates, Delegated OCSP Responder Certificates, and Cross-Certificates, the applicable Operational Authority (OA) MAY request restoration of a suspended Certificate.

All restoration requests SHALL be subject to the identification, authentication, and authorization requirements specified in Sections 3.2 and 3.3 of this CP.

The CA SHALL verify that the condition that resulted in Certificate suspension has been resolved prior to restoring Certificate status.

The CPS SHALL describe the procedures and controls used to process Certificate restoration requests.

4.9.15 Procedure for Suspension Request

Requests for Certificate suspension SHALL be authenticated and authorized by the CA or RA prior to processing.

A request to suspend a Certificate MAY be submitted by an authorized Subscriber, device sponsor, CA, RA, Operational Authority, or other authorized representative, as applicable to the Certificate type. The CA or RA SHALL verify the identity and authority of the requestor prior to suspending the Certificate. Suspension requests and resulting actions SHALL be recorded in applicable audit records.

Requests to restore a suspended Certificate SHALL be authenticated and authorized prior to processing. Prior to restoring a suspended Certificate, the CA or RA SHALL verify that the condition that resulted in suspension has been resolved and that restoration remains appropriate.

The identity and authority of the restoration requestor SHALL be verified in accordance with the requirements of Sections 3.2 and 3.3 of this CP.

Certificate suspension and restoration actions SHALL be reflected in applicable Certificate status information, including CRLs and OCSP responses, as appropriate.

The CPS SHALL describe the procedures, approval requirements, notification requirements, and operational controls applicable to Certificate suspension and restoration.

4.9.16 Limits on Suspension Period

Where Certificate suspension is supported, the maximum suspension period SHALL be sixty (60) days or the expiration date of the Certificate, whichever occurs first.

The CPS SHALL describe the procedures and controls used to enforce the maximum suspension period.

If a suspended Certificate has not been restored prior to the expiration of the suspension period, the Certificate SHALL be revoked.

Certificates SHALL NOT remain in a suspended state beyond their expiration date and SHALL NOT be published on a CRL with a reason code of *certificateHold* after the Certificate has expired.

Requests to restore a suspended Certificate SHALL be authenticated and authorized at an assurance level commensurate with the assurance level of the Certificate being restored.

4.10 Certificate Status Services

Certificate status services, including Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) services, SHALL be operated in accordance with the requirements specified in Sections 4.7 through 4.9.11, Section 2.2.1, and RFC 6960, as applicable.

Where OCSP services are provided, including Delegated OCSP Responders, such services SHALL comply with all availability, response time, publication, security, re-key, modification, revocation, and status information requirements defined in this CP.

4.10.1 Operational Characteristics

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

4.10.2 Service Availability

Certificate status services SHALL be available in accordance with the requirements specified in Sections 2.2.1 and 4.9.9 of this CP.

The CPS SHALL describe the technical, operational, and monitoring controls used to maintain availability of Certificate status services, including CRLs, OCSP services, and any delegated OCSP responders.

Certificate status services SHALL be operated with sufficient resources to support their intended use and to meet applicable availability requirements defined in this CP.

4.10.3 Optional Features

No stipulation.

4.11 End Of Subscription

No stipulation.

4.12 Key Escrow and Recovery

Key escrow and recovery services MAY be provided for Subscriber key management Certificates where authorized by the applicable Certificate Policy, Subscriber Agreement, the NFI CPS and approved RPS documents.

Where key escrow and recovery services are provided, such services SHALL be performed in accordance with this CP and the NFI CPS.

Subscriber signature keys SHALL NOT be escrowed or recovered.

Identification, authentication, authorization, audit, and operational requirements applicable to key recovery requests SHALL comply with Section 3.5 of this CP.

4.12.1 Key Escrow and Recovery Policy and Practices

CA private keys SHALL NOT be escrowed.

Subscriber key management keys are escrowed to support authorized key recovery operations. EMS NFI supports escrow and recovery of Subscriber key management keys through EMS KRS.

Prior to issuance of a key management Certificate associated with an escrowed key, the CA SHALL verify that the key escrow operation has been successfully completed.

Escrowed keys SHALL be protected during generation, storage, backup, recovery, transmission, and destruction at a level commensurate with the assurance level of the associated Certificate and no less than the level of protection afforded to the key when under Subscriber control.

Under no circumstances SHALL Subscriber signature keys be escrowed or recovered.

The CPS SHALL describe the controls, roles, responsibilities, approval requirements, audit mechanisms, recovery procedures, and technical safeguards governing key escrow and recovery.

4.12.1.1 Key Escrow Process and Responsibilities

Subscriber key management private keys SHALL be securely escrowed within EMS KRS.

The CA SHALL verify successful escrow of key material prior to issuance of the associated key management Certificate. Escrowed keys SHALL be protected during transit and storage using cryptographic mechanisms providing protection commensurate with the assurance level of the escrowed key.

Subscribers SHALL be informed that keys associated with key management Certificates are subject to escrow and recovery.

4.12.1.2 Key Recovery Process and Responsibilities

Key recovery operations SHALL be performed in accordance with EMS KRS procedures as defined in the NFI CPS.

Communications between key recovery participants SHALL be protected against disclosure, modification, replay, substitution, and other relevant threats.

Cryptographic protections used during recovery operations SHALL provide protection commensurate with, or greater than, the protection afforded to the recovered key material.

Escrowed keys SHALL only be released to authenticated and authorized Key Requestors.

The CPS SHALL define recovery procedures applicable to Subscribers, authorized third-party Key Requestors, KRAs, KROs, DDSs, and automated recovery services.

Third-party recovery of key management keys SHALL NOT, by itself, require Certificate revocation.

4.12.1.2.1 Key Recovery Through KRA

A KRA SHALL release escrowed key material only in response to a properly authenticated and authorized key recovery request. Recovery and release of escrowed keys SHALL be subject to approved EMS KRS controls and SHALL be auditable.

The CPS or RPS SHALL describe the procedures, approvals, separation of duties, and technical controls applicable to key recovery performed through a KRA.

4.12.1.2.2 Automated Self-Recovery

Automated self-recovery MAY be supported for authorized Subscribers. Prior to releasing escrowed key material through an automated recovery process, the Subscriber SHALL be authenticated in accordance with Section 3.5.

The CPS or RPS MAY describe the authentication, notification, delivery, and protection mechanisms applicable to automated self-recovery.

4.12.1.2.3 Key Recovery During Token Issuance

Escrowed key management keys MAY be recovered and provisioned during issuance of a replacement token. Recovery and provisioning of escrowed key material during token issuance SHALL be performed using approved cryptographic and operational controls that maintain the confidentiality and integrity of recovered keys.

The CPS or RPS SHALL describe the procedures and safeguards applicable to key recovery during token issuance.

4.12.1.2.4 Key Recovery by Data Decryption Server

Data Decryption Servers (DDSs) MAY recover escrowed keys where authorized by the EMS KRS. DDS recovery requests SHALL be authenticated and authorized in accordance with Section 3.5.

The CPS or RPS MAY describe the controls governing DDS authentication, authorization, operation, auditing, and protection of recovered key material.

4.12.1.3 Who Can Submit a Key Recovery Application

Subscribers MAY request recovery of their own escrowed key material.

Authorized third-party Key Requestors MAY request recovery of escrowed key material on behalf of a Subscriber where permitted by applicable law, policy, contractual agreement, or organizational authorization.

The CPS or RPS SHALL identify authorized Key Requestors and the approval requirements applicable to each request type.

4.12.1.3.1 Key Requestor Authorization Validation

The KRA or KRO SHALL verify the identity and authorization of all Key Requestors prior to processing a key recovery request.

Authorization validation SHALL be performed in accordance with Section 3.5 and the NFI CPS.

4.12.1.3.2 Subscriber Authorization Validation

Subscribers SHALL be authorized to request recovery of their own escrowed key material, subject to successful authentication and authorization verification in accordance with Section 3.5.

4.12.1.3.3 KRA Authorization Validation

The EMS KRS SHALL verify that a KRA possesses appropriate privileges and authority prior to permitting access to escrowed key material.

The CPS SHALL describe the authorization controls applicable to KRAs.

4.12.1.3.4 KRO Authorization Validation

The EMS KRS SHALL verify that a Key Recovery Official (KRO) possesses appropriate authority prior to approving or requesting recovery of escrowed key material.

The CPS SHALL describe the authorization controls applicable to KROs.

4.12.1.3.5 Data Decryption Server Authorization Validation

The EMS KRS SHALL verify that a DDS is authorized to recover escrowed key material within the scope of its approved operational role.

The CPS or RPS SHALL describe the authorization controls and operational restrictions applicable to DDS recovery activities.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No Certification Authorities operating under this CP support session key encapsulation or session key recovery.

Should such services be introduced in the future, the CP and CPS SHALL define the policy, operational controls, and recovery requirements governing those services.

5.0 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

All CA equipment, including CA cryptographic modules, SHALL be protected from unauthorized access. Physical access controls SHALL be implemented to reduce the risk of equipment tampering, including when cryptographic modules are not installed or activated.

CA cryptographic tokens SHALL be protected against theft, loss, and unauthorized use.

All the physical control requirements specified below apply equally to Certification Authorities (CAs), Card Management Systems (CMSs), and remote workstations used to administer CAs, except where specifically noted.

5.1.1 Site Location and Construction

The location and construction of facilities housing NFI CA equipment, EMS KRS, CMS equipment, and remote workstations used to administer CAs SHALL be consistent with facilities used to house high-value, sensitive information.

Site location and facility construction, when combined with physical security controls such as guards, high-security locks, intrusion detection systems, and other protective measures, SHALL provide robust protection against unauthorized physical access to CA equipment, cryptographic modules, cryptographic tokens, records, and other sensitive information.

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.

5.1.2.5 Physical Access for KED Equipment

Physical access control requirements for Key Escrow Database (KED) equipment storing escrowed private keys SHALL meet the physical access requirements applicable to Certification Authorities as

specified in Section 5.1.2.1. KED equipment SHALL be protected from unauthorized physical access, tampering, theft, loss, and misuse.

5.1.2.6 Physical Access for DDS Equipment

Physical access control requirements for Data Decryption Server (DDS) equipment storing, processing, or recovering escrowed private keys SHALL meet the physical access requirements applicable to Certification Authorities as specified in Section 5.1.2.1.

DDS equipment SHALL be protected from unauthorized physical access, tampering, theft, loss, and misuse.

5.1.2.7 Physical Access for KRA and KRO Equipment

Equipment used by Key Recovery Authorities (KRAs) and Key Recovery Officials (KROs) SHALL be protected from unauthorized physical access while cryptographic modules are installed and activated. KRAs and KROs SHALL implement physical access controls designed to reduce the risk of equipment tampering, theft, loss, or unauthorized use, including when cryptographic modules are not installed or activated.

Physical security controls protecting KRA and KRO equipment SHALL be commensurate with the sensitivity of the equipment and the assurance level of the protected key recovery operations.

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

Facilities housing CA equipment, CMS equipment, EMS KRS equipment, and remote workstations used to administer Certification Authorities SHALL comply with applicable local fire prevention, fire detection, and fire protection requirements.

Fire protection controls SHALL be designed to reduce the risk of damage to personnel, CA equipment, cryptographic modules, records, and other sensitive assets.

The CPS SHALL describe the fire prevention, detection, suppression, disaster recovery, and business continuity controls implemented to protect CA operations.

5.1.6 Media Storage

CA media, including media containing escrowed key material, SHALL be stored in a manner that protects it from accidental damage, including water, fire, electromagnetic interference, and other environmental threats.

Sensitive CA media, EMS KRS media, backup media, and media containing escrowed or recovered key material SHALL be protected against unauthorized physical access, disclosure, modification, theft, and destruction.

Where offline Certification Authorities or offline Key Recovery System components are used, media associated with those systems SHALL be stored in secure facilities with physical protections commensurate with the sensitivity of the information being protected.

The CPS SHALL describe the controls used to protect CA and KRS media throughout its lifecycle, including storage, transport, backup, retention, and destruction.

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 performed on a periodic schedule. Backups SHALL 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 copy need be retained.

Backup media, including media containing CA, KRS, escrowed key material, recovered key material, or other sensitive PKI information, SHALL be protected against unauthorized access, disclosure, modification, theft, destruction, and environmental damage. Off-site storage facilities SHALL employ physical and procedural controls commensurate with those protecting the operational CA.

Where offline Certification Authorities or offline key recovery components are used, associated backup media SHALL be stored in secure facilities providing physical protections commensurate with the sensitivity of the information being protected.

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

5.2 Procedural Controls

Unless otherwise specified, the procedural control requirements in this section apply to all Certification Authorities (CAs) operating under this CP and to all supporting systems and personnel performing trusted functions on behalf of those CAs, including Registration Authorities (RAs), Card Management Systems (CMSs), Key Recovery Authorities (KRAs), Key Recovery Officials (KROs), Key Escrow Databases (KEDs), Data Decryption Servers (DDSs), and other Key Recovery System (KRS) components where applicable.

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, including EMS KRS. 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, EMS KRS, RA, and CSS locations as appropriate.

An auditable record SHALL be created identifying when personnel are assigned to, modified within, or removed from a Trusted Role, including the identity of the individual performing the assignment or removal action. The identity of the individual authorizing the role assignment SHALL be traceable through audit and archive records. Trusted Role appointments SHALL be documented and archived in accordance with Sections 5.4 and 5.5.

5.2.1.1 NFI CA Trusted Roles

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

4. *Administrator* – authorized to install, configure, and maintain the CA; establish and maintain system accounts; configure audit parameters; and generate component keys.
5. *Officer* – authorized to request or approve Certificate issuance and revocations.
6. *Auditor* – authorized to review, maintain, and archive audit logs.
7. *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
Administrator	Security Officer / Master User (SOMU)
Administrator	System Administrator (SA)
Officer	Registration Authority (RA), (and for Issuing CA, Local Registration Authority (LRA))
Auditor	Security Compliance Officer (SCO)

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 identity (SOMU, SA or Auditor).

5.2.1.2 Registration Authority Trusted Roles

An RA may be considered an Officer as defined in Section 5.2.1.1 and is responsible for:

- Verifying initial identity, as described in Section 3.2;
- Entering Subscriber information, and verifying correctness;
- Securely communicating requests to and responses from the CA;
- Receiving and distributing Subscriber Certificates;

The RA role is highly dependent on implementation and local requirements. The responsibilities, controls, and procedures applicable to RAs SHALL be explicitly defined in the NFI CPS and the RPS.

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 themselves 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) PIV-I Card Authentication	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 identity.

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 the following criteria:

- 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

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.

For RA Organizations, in all cases the reinvestigation period for a Trusted Role background check MUST not exceed 10 years and MUST be documented in the RPS. If an RAO Trusted Role's national security eligibility, suitability determination, or PIV eligibility is ever suspended or revoked during their appointment, all CA accesses MUST be revoked until the security eligibility, suitability determination, or PIV eligibility is reinstated or a separate investigation is completed and adjudicated.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of CAs, Key Recovery Services (KRS), and related PKI components 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 CAs, EMS KRS components, and associated trusted functions SHALL receive comprehensive training, or demonstrate competence, in the following areas:

- CA, RA and KRS security principles and mechanisms.
- All PKI software versions in use on the CA system.
- PKI duties they are expected to perform.
- Disaster Recovery and business continuity.

- Stipulations of the NFI CPS.

Documentation SHALL be maintained identifying all personnel who have received training and the level of training completed. Where competence is demonstrated in lieu of formal 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

Personnel performing trusted roles SHALL be subject to appropriate administrative, disciplinary, or other corrective actions for performing actions that are not authorized by this CP, the applicable CPS, RPS, EMS KRS, security procedures, or other documented operational procedures.

Sanctions SHALL be commensurate with the nature, severity, and impact of the unauthorized action and MAY include retraining, suspension of privileges, reassignment of duties, removal from a trusted role, disciplinary action, or termination of employment or contractual relationship, as appropriate.

5.3.7 Independent Contractor Requirements

Contractors fulfilling trusted roles are subject to all personnel requirements stipulated in this policy and practices in the EMS CPS.

5.3.8 Documentation Supplied to Personnel

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

5.4 Audit Logging Procedures

Audit log files SHALL be generated for all events relating to the security of the CA. For CAs operated in a virtual machine environment (VME)¹, audit logs SHALL be generated for all applicable events on both the virtual machine (VM) and isolation kernel (i.e. hypervisor).

Where possible, the security audit logs SHALL be automatically collected. Where this is not possible, a logbook, digital form, or other 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
IDENTIFICATION AND AUTHENTICATION			
Platform or CA application level authentication attempts		X	X

¹ For the purposes of this policy, the definition of a virtual machine environment does not include cloud-based solutions (e.g. platform-as-a-service) or container-type solutions (e.g. Docker), which are not permitted for any CA subordinated to the FBCA.

Auditable Event	Rudimentary	Basic	Medium (all policies) & PIV-I Card Authentication
The value of <i>maximum authentication attempts</i> is changed		X	X
The number of unsuccessful authentication attempts exceeds the <i>maximum authentication attempts</i> during user login		X	X
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
DATA ENTRY AND OUTPUT			
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
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 CA, RA, CSS, CMS, or other keys used by the CA in the lifecycle management of Certificates	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			
Any changes to public keys used by components of the CA to authenticate other components or authorize	X	X	X

Auditable Event	Rudimentary	Basic	Medium (all policies) & PIV-I Card Authentication
Certificate lifecycle requests (e.g., RA or CMS trust stores)			
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 records related to Certificate request authorization, approval and signature, whether generated directly on the CA or generated by a related external system or process	X	X	X
CERTIFICATE STATUS CHANGE APPROVAL			
All records, including request, authorization, approval and execution related to Certificate status changes (e.g., revocation, suspension, or restoration) whether generated directly on the CA or generated by a related external system or process		X	X
CA CONFIGURATION			
Any security-relevant changes to the configuration of the CA. The specific configuration items relevant to the environment in which the CA operates must be identified and documented.		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
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT			

Auditable Event	Rudimentary	Basic	Medium (all policies) & PIV-I Card Authentication
All changes to the Certificate revocation list profile		X	X
EMS KRS			
Key Escrow operations			X
Key Recovery requests			X
Key Recovery approvals and denials			X
Release of escrowed key materials			X
KRA role assignments and removals			X
KRO Role Assignments and removals			X
KED Configuration Changes			X
DDS recovery requests and deliveries			X
Authentication and authorization failures associated with EMS KRS			X
TRUSTED ROLES			
Appointment, modification, or removal of personnel assigned to Trusted Roles	X	X	X
MISCELLANEOUS			
All records of authentication, authorization, recovery, agreement and delivery of key management keys to a Key Requestor.	X	X	X
Record of an individual being added or removed from a trusted role, and who added or removed them from the role	X	X	X
Installation of the Operating System		X	X
Installation of the CA		X	X
Installing hardware cryptographic modules			X
Removing hardware cryptographic modules			X
Destruction of cryptographic modules		X	X
System Startup		X	X
Logon Attempts to CA Applications		X	X
Receipt of Hardware/Software			X

Auditable Event	Rudimentary	Basic	Medium (all policies) & PIV-I Card Authentication
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
Records of manipulation of critical files (e.g., creation, renaming, moving), critical files will vary between installation, and must be identified in the CPS or RPS			X
The date and time any CA artifact is posted to a public repository			X
Access to CA internal database			X
All Certificate compromise notification requests		X	X
Loading tokens with Certificates			X
Shipment and receipt of tokens containing key material, or tokens that allow access to key material (e.g., HSM operator cards)			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

Auditable Event	Rudimentary	Basic	Medium (all policies) & PIV-I Card Authentication
ANOMALIES			
Software Error conditions		X	X
Software check integrity failures		X	X
Equipment failure	X	X	X
Electrical power outages			X
Uninterruptible Power Supply (UPS) failure			X
Network service or access failures that could affect Certificate trust			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

CA, CMS, CSS, and KRS audit logs SHALL be reviewed in accordance with the table below. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the log. Examples of irregularities include discontinuities in the logs and loss of audit data. Actions taken as a result of these reviews SHALL be documented.

Assurance Level	Review Audit Log
Rudimentary	Only required for cause
Basic	At least once per month
Medium (all policies)	At least once per month 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 per month 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 monthly.

5.4.3 Retention Period for Audit Log

For Medium, Medium Hardware, PIV-I Assurance levels, and EMS KRS, audit logs SHALL be retained on-site until reviewed, as well as being retained in the manner described below. Audit records for these assurance levels SHALL not be deleted or destroyed prior to review. Audit records for Basic Assurance environments SHALL not be deleted or destroyed prior to review. For Rudimentary 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

Audit logging systems SHALL be configured to protect audit records against unauthorized modification, deletion, overwriting, and destruction prior to review and archival. The protection requirements of this section apply equally to CA, CMS, CSS, KED, DDS, and other KRS audit records.

The EMS NFI 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.
- 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.

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

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

Procedures MUST be implemented to protect audit records from deletion or destruction before they are reviewed, as described in Section 5.4.2. To protect the integrity of audit records, they MUST be transferred to a backup environment distinct from the environment where the audit records are generated.

5.4.5 Audit Log Backup Procedures

Audit logs generated by CAs, RAs, CMSs, CSSs, and Key Recovery System (KRS) components, including KEDs, KRAs, KROs, and DDSs, SHALL be backed up on a regular basis. Backup copies of audit logs SHALL be protected against unauthorized access, modification, deletion, destruction, and loss for the duration of the applicable retention period.

Audit log backups SHALL be stored separately from the originating system and protected at a level commensurate with the sensitivity of the audit records.

The CPS or RPS (where an RA deploys a DDS) SHALL describe the procedures, frequency, retention, protection, and recovery mechanisms applicable to audit log backups.

5.4.6 Audit Collection System (Internal vs. External)

Audit collection systems, whether internal or external to the CA, SHALL protect audit records from unauthorized access, modification, deletion, destruction, overwriting, or loss prior to review and archival. Audit collection systems SHALL be configured and managed to prevent loss of audit data resulting from audit log overflow, storage exhaustion, or system failures. The requirements of this section apply equally to audit records generated by CAs, RAs, CMSs, CSSs, and EMS KRS components, including KEDs, KRAs, KROs, and DDSs.

If the integrity, availability, or confidentiality of audit information is believed to be at risk, the Entrust Operational Authority (OA) and Policy Authority (PA) SHALL determine whether operations should be suspended until the condition has been investigated and remediated.

The CPS SHALL describe the controls and procedures used to collect, protect, monitor, review, archive, and recover audit records.

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 vulnerability 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.

For RA Organizations operating under this policy, self-assessment of controls and control effectiveness (e.g., FISMA) MUST be performed in accordance with the frequency determined by the risk rating of the CA.

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

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

5.5 Records Archival

Entrust SHALL comply with company records retention policies in accordance with internal requirements and applicable laws and regulations. Entrust SHALL, at a minimum, comply with the retention periods specified in Section 5.5.2 regardless of company records retention policies.

CA archive records SHALL be sufficiently detailed to support verification that the CA was properly operated and to establish the validity of any Certificate, including revoked or expired Certificates, in the event of a dispute regarding use of the Certificate.

Where Key Recovery Services (KRS) are provided, archive records SHALL be maintained for key escrow and key recovery activities. KRS archive records SHALL be sufficiently detailed to permit reconstruction and verification of key recovery operations and to support resolution of disputes involving key recovery activities.

Examples of key recovery disputes MAY include:

- Validation of key recovery requests.
- Validation of the identity of the recipient of recovered key material.
- Verification of authorization to obtain escrowed key material.
- Verification of the transfer of custody of recovered key material to an authorized Key Requestor.
- Establishment of the circumstances under which recovered key material was released.

The CPS SHALL identify the archive records maintained for CA and KRS operations and the controls used to protect archived information from unauthorized modification, deletion, disclosure, or destruction.

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

Data To Be Archived	Rudimentary	Basic	Medium(all policies) & PIV-I Card Authentication
System and equipment configuration	X	X	X
Modifications and updates to system or configuration	X	X	X
All records related to Certificate request authorization, approval and signature, whether generated directly on the CA or generated as part of a related external system or process	X	X	X
All records related to Certificate status changes (e.g., revocation, suspension, or restoration) whether generated directly on the CA or generated as part of a related external system or process		X	X
Suspension requests		X	X
Restoration 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
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
Audit summary reports generated by internal reviews and documentation generated during third party audits		X	X
Any changes to the Audit parameters, e.g., audit frequency, type of event audited		X	X

Data To Be Archived	Rudimentary	Basic	Medium(all policies) & PIV-I Card Authentication
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
Changes to trusted public keys used or published by the CA including Certificates used for trust between the CA and other components such as CMS, RA, etc.	X	X	X
The export of private and secret keys (keys used for a single session or message are excluded)	X	X	X
The approval or rejection of a Certificate status change request		X	X
Appointment to an individual to a Trusted Role	X	X	X
Addition of an individual to a Trusted Role	X	X	X
Removal of an individual from a Trusted Role	X	X	X
Modification of Trusted Role assignments	X	X	X
Identity of the person who assigned the Trusted Role	X	X	X
Identity of the person who removed the Trusted Role	X	X	X
Identity of the person authorizing the role assignment or removal	X	X	X
Record of an individual being added or removed from a trusted role, and who added or removed them from the role	X	X	X
Evidence of qualification for Trusted Agents and the associated validity period(s) for	X	X	X

Data To Be Archived	Rudimentary	Basic	Medium(all policies) & PIV-I Card Authentication
which they are authorized to act as Trusted Agents			
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
EMS-KRS			
Successful key escrow operations	X	X	X
Failed key escrow operations	X	X	X
Verification that key escrow was completed prior to Certificate issuance	X	X	X
Third-party key recovery requests	X	X	X
KRA-initiated recovery actions	X	X	X

5.5.2 Retention Period for Archive

The minimum retention periods for archive data are identified below. In addition, Entrust SHALL comply with internal records retention policies and applicable laws and regulations.

Archive retention periods for CA records SHALL begin at the applicable CA key generation event. Where a CA performs key rollover, a new retention period SHALL begin for each subsequent key generation event. CA archive records SHALL be maintained in an accessible form for the retention periods specified below and SHALL be sufficiently detailed to verify that the CA was properly operated and to establish the validity of any Certificate, including revoked or expired Certificates.

Individual RA records associated with Certificate request authorization, Subscriber authentication, Certificate issuance, Certificate acceptance, Certificate modification, Certificate re-key, Certificate suspension, Certificate restoration, and Certificate revocation SHALL be retained for the period specified below, beginning on the expiration date of the associated Certificate.

Issuance of a replacement Certificate through renewal, re-key, or modification that relies on previously collected Subscriber authentication records SHALL establish a new retention period for those records based upon the expiration date of the replacement Certificate.

Where EMS KRS services are provided, archive retention periods for key escrow and key recovery records SHALL begin when the corresponding escrow or recovery event occurs. KRS records SHALL be retained for the period specified below and SHALL be sufficient to reconstruct and validate key recovery activities.

RA system operational audit records, including systems supporting RA and KRS functions, SHALL be retained for a minimum of three (3) years following system replacement or termination.

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, modify, or delete archive records.

The contents of the archive SHALL NOT be released except in accordance with Sections 9.3 and 9.4. Records of individual transactions MAY be released upon request of the Subscribers involved in the transaction or their legally authorized representatives.

Archive media SHALL be stored in a secure facility separate from the CA and protected against unauthorized access, modification, disclosure, destruction, and loss. Alternatively, Entrust MAY retain archived records using retention and storage procedures approved by NARA or other applicable regulatory authorities for the relevant record category.

Applications, systems, and tools required to process, access, or read archive records SHALL be maintained for a period sufficient to comply with the archive retention requirements specified in Section 5.5.2. Where archived records are transferred to new media, formats, or storage environments, documented procedures SHALL be used to protect the records during transfer in accordance with 5.4.5.

If the original media cannot retain data for the required retention period, procedures SHALL be established to periodically migrate archived records to new media or formats while maintaining record integrity, accessibility, and evidentiary value.

The requirements of this section apply to both CA archive records and EMS KRS archive records, where applicable.

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 and RPS.

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 the risk of compromise of a CA private signing key, the key MAY be periodically changed. Following key changeover, only the new private key SHALL be used to issue CA and Subscriber Certificates. The corresponding older public key SHALL remain available to validate signatures associated with Certificates issued under the previous key pair until all such Certificates have expired or been revoked.

If the previous CA private key continues to be used to sign Certificate Revocation Lists (CRLs) or OCSP Responder certificates that support Certificates issued under that key, the previous private key SHALL be retained and protected in accordance with the requirements of this CP and the NFI CPS.

After all Certificates issued under the previous key have expired or been revoked, the CA MAY issue a final long-term CRL using the previous private key, with a nextUpdate value extending beyond the validity period of all Certificates issued under that key. The final CRL SHALL remain available until all Certificates issued under the previous key have expired.

Once all Certificates associated with the previous key have expired and all required CRLs and OCSP-related activities have concluded, the previous CA private signing key MAY be destroyed in accordance with the key destruction requirements of this CP.

Entrust performs periodic key rollover operations as described above. Detailed key rollover procedures SHALL be described in the NFI CPS.

When EMS NFI performs a key changeover and generates a new public key, EMS NFI SHALL notify affected RAs. RAs are responsible for notifying Subscribers who rely upon the affected CA Certificate.

The CA SHALL do one of the following:

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

5.7 Compromise and Disaster Recovery

Entrust SHALL maintain and follow documented incident handling, compromise response, disaster recovery, and business continuity procedures applicable to Certification Authorities (CAs), Registration Authorities (RAs), Card Management Systems (CMSs), Certificate Status Services (CSSs), and Key Recovery System (KRS) components.

The NFI CPS SHALL describe the incident handling, reporting, escalation, disaster recovery, business continuity, and service restoration procedures applicable to EMS NFI operations.

5.7.1 Incident and Compromise Handling Procedures

The Entrust Policy Authority SHALL notify the FPKIPA within 24 hours as required by the applicable MOA if any of the following cases occur:

- Suspected or detected compromise of the CA systems.
- Physical or electronic attempts to penetrate any CA system.
- Successful denial of service attacks on CA components.
- Any incident preventing the CA from issuing a prior to the nextUpdate time of the previous CRL.
- Suspected or detected compromise of a CSS including OCSP services and Delegated OCSP Responders.
- Suspected or detected compromise of an RA.
- Suspected or detected compromise of Key Recovery System (KRS) components, including KEDs, KRAs, KROs, DDSs, or escrowed key material.

The notification SHALL include a preliminary analysis of the incident and proposed remediation activities.

Once the incident has been resolved, EMS NFI SHALL provide prompt notification to the FPKIPA describing the actions taken to remediate the incident. The notification SHALL include:

- i. Identification of the affected CA, CSS, RA, KRS, or other PKI components.
- ii. EMS NFI's assessment and interpretation of the incident.
- iii. Identification of affected parties.
- iv. The date and time the incident was discovered.
- v. A list of any Certificates that MAY have been issued improperly or that MAY no longer conform to the CP, CPS, or applicable requirements as a result of the incident.
- vi. A statement confirming that the incident has been fully remediated.

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

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

- Before returning to operation, ensure that the system's integrity has been restored.
- If the CA signature keys are not destroyed, CA operation 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.

In the event of an incident as described above, the CA SHALL post a notice on its web page identifying the incident and provide notification to the FPKIPA. See Section 5.7.1 for contents of the notice.

5.7.3 Entity (CA) Private Key Compromise Procedures

5.7.3.1 CA Key Compromise Procedures

In the event of an actual or suspected compromise of an Entrust NFI CA private signing key, the following actions SHALL be performed:

- Entrust SHALL immediately notify the FPKIPA and any entities known to distribute or rely upon the affected CA Certificate.
- Entrust SHALL request revocation of any Certificates issued to the compromised CA, as appropriate.
- The affected Entrust NFI CA SHALL generate a new key pair in accordance with Section 6.1.1.1 and the NFI CPS.
- New CA Certificates SHALL be obtained and issued in accordance with the applicable CPS.

If the affected Entrust NFI CA distributes its public key through a self-signed Certificate or trusted Certificate, Entrust SHALL:

- Generate a new trusted Certificate;
- Distribute the new trusted Certificate in accordance with Section 6.1.4; and
- Initiate procedures to notify affected RAs and Subscribers of the compromise.

Subscriber Certificates issued prior to compromise of the CA private key MAY be renewed under the replacement CA key pair or Entrust MAY require Subscribers to complete a new Certificate application process, as determined by the NFI CPS and operational requirements.

Entrust SHALL investigate the cause of the compromise or suspected compromise and SHALL provide the FPKIPA with details regarding the root cause, operational impact, corrective actions taken, and measures implemented to prevent recurrence.

Entrust SHALL publish a notice describing the compromise in accordance with Section 5.7.1 and the applicable CPS.

5.7.3.2 KRS Private Key Compromise Procedures

In the event of an actual or suspected compromise of an EMS Key Recovery System (KRS) component, including a Key Escrow Database (KED), Data Decryption Server (DDS), Key Recovery Authority (KRA), Key Recovery Official (KRO), or escrowed key material, Entrust SHALL perform the following actions:

- Notify the FPKIPA of the compromise or suspected compromise.
- Provide details regarding the root cause, operational impact, affected systems, and initial remediation actions.
- Determine the scope and extent of the compromise.
- Develop and implement corrective actions, including any Certificate revocation, key recovery suspension, or system recovery activities deemed necessary.
- Obtain FPKIPA concurrence where required for planned remediation activities affecting cross-certified operations.

If a KRA or KRO Certificate is revoked due to compromise, Entrust SHALL:

Review audit records to identify any escrowed key material that may have been exposed.

- Determine whether affected Subscriber key management Certificates require revocation or replacement.
- Notify affected Subscribers, where appropriate.
- Reissue replacement KRA or KRO credentials as necessary.

The NFI CPS SHALL define KRS compromise response, investigation, notification, audit review, and remediation procedures.

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 an Entrust NFI CA, all Certificates issued by the terminating CA that have not expired SHALL be revoked. Prior to termination, the Entrust Policy Authority (PA) SHALL ensure that all archive records are transferred to an approved archival facility in accordance with Section 5.5.

A final long-term CRL SHALL be generated with a *nextUpdate* value extending beyond the validity period of all Certificates issued by the terminating CA. This final CRL SHALL remain available to relying parties until the validity period of all Certificates issued by the terminating CA has passed.

Once all required CRLs have been issued and all Certificate validation obligations have been satisfied, the private signing keys associated with the terminating CA SHALL be destroyed in accordance with this CP and the applicable CPS.

Entrust SHALL provide notification of the CA termination to all organizations, subordinate entities, Registration Authorities, and other affected parties that rely upon Certificates issued by the terminating CA. Notification SHALL be provided as far in advance as circumstances permit.

Where the terminating Entrust NFI CA is cross-certified with the Federal Bridge Certification Authority (FBCA), the Entrust Policy Authority SHALL notify the FPKIPA prior to termination.

Whenever practical, the Entrust Policy Authority SHALL notify the FPKIPA at least two (2) weeks prior to the termination of any Entrust NFI CA cross-certified with the FBCA. In emergency termination situations, Entrust SHALL follow the incident notification requirements specified in Section 5.7.

6.0 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

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

6.1.1.1 CA Key Pair Generation

Cryptographic keying material used by CAs to sign Certificates, CRLs, or Certificate status information **SHALL** be generated within FIPS 140 validated cryptographic modules, or cryptographic modules validated under equivalent international standards.

The cryptographic modules **SHALL** meet or exceed Security Level 1 for Rudimentary Assurance and Security Level 2 for Basic, Medium, Medium Hardware, and PIV-I Card Authentication Assurance.

Multiparty control **SHALL** be required for Entrust NFI CA key pair generation and for all CAs operating at the Medium, Medium Hardware, and PIV-I Card Authentication Assurance Levels, in accordance with Section 5.2.2.

CA key pair generation **SHALL** create a verifiable audit trail demonstrating that all applicable security and procedural requirements were followed. For all assurance levels, the documentation of the key generation process **SHALL** be sufficiently detailed to demonstrate that appropriate role separation and multiparty controls were enforced.

For Medium, Medium Hardware, and PIV-I Card Authentication Assurance Levels, an independent third party **SHALL** validate the execution of the CA key generation procedures either by directly witnessing the key generation ceremony or by reviewing the signed documentation and audit records produced during the key generation process.

The detailed key generation procedures, evidence collection requirements, and validation activities **SHALL** be described in the NFI CPS.

6.1.1.2 Subscriber Key Pair Generation

Subscriber key pair generation **MAY** be performed by the Subscriber, CA, or RA.

Where the CA or RA generates Subscriber key pairs, the key delivery requirements specified in Section 6.1.2 **SHALL** be met.

Key generation **SHALL** be performed using FIPS 140 validated cryptographic modules or modules validated under equivalent international standards, as specified in Section 6.2.1.

For PIV-I Certificates, all Subscriber private keys, except key management keys, SHALL be generated on the PIV-I credential in accordance with Appendix A.

For Certificates issued at the Medium Hardware assurance level, Subscriber key generation SHALL be performed using a validated hardware cryptographic module as specified in Section 6.2.1.

For Certificates issued at the Medium and Basic assurance levels, Subscriber key generation SHALL be performed using either a validated software cryptographic module or a validated hardware cryptographic module as specified in Section 6.2.1.

6.1.1.3 CSS Key Pair Generation

Cryptographic keying material used by Certificate Status Services (CSSs), including OCSP Responders and Delegated OCSP Responders, to sign Certificate status information SHALL be generated in FIPS 140 validated cryptographic modules as specified in Section 6.2.1.

6.1.1.4 PIV-I Content Signing Key Pair Generation

Cryptographic keying material used by Card Management Systems (CMSs) or devices for PIV-I Content Signing SHALL be generated in FIPS 140 validated cryptographic modules as specified in Section 6.2.1.

For PIV-I Content Signing Certificates, key generation SHALL be performed using hardware cryptographic modules meeting the requirements specified in Appendix A.

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 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, a key rollover Certificate, or a new CA Certificate issued by the issuer of the current CA Certificate.

Self-signed Root CA Certificates SHALL be conveyed to relying parties in a secure fashion to preclude substitution attacks. Acceptable methods include:

- Secure distribution of the Certificate through authenticated out-of-band mechanisms;
- Download of the Certificate from a trusted web site secured with a currently valid Certificate, followed by comparison of the Certificate hash against a hash value obtained through an authenticated out-of-band source. Hashes posted in-band with the Certificate SHALL NOT be relied upon as an authentication mechanism.

Other methods that preclude substitution attacks MAY be used.

Key rollover Certificates are signed using the CA's current private key; therefore, secure distribution is not required.

CA Certificates signed by an issuing CA's current private key do not require separate secure distribution.

6.1.5 Key Sizes

This CP requires the use of RSA PKCS #1, RSASSA-PSS, or ECDSA signatures. Additional restrictions on key sizes and hash algorithms are specified below.

Certificates SHALL contain 2048-, 3072-, or 4096-bit RSA keys, or 256- or 384-bit elliptic curve keys.

CA Certificates		
	CA Certificates that expire on or before December 31, 2030	CA Certificates that expire after December 31, 2030
Minimum Key Size	RSA: 2048 Elliptic Curve: 256	RSA: 3072 Elliptic Curve: 256
Hash Algorithm	SHA-256, SHA-384, or SHA-512	SHA-256, SHA-384, or SHA-512

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

All Subscriber Certificates associated with PIV-I SHALL contain public keys and algorithms conforming to NIST SP 800-78.

Use of TLS, or another protocol providing equivalent security, SHALL require a minimum of AES-128 (or equivalent) for symmetric encryption and a minimum of RSA-2048 (or equivalent) for asymmetric keys.

After December 31, 2030, TLS, or another protocol providing equivalent security, SHALL require a minimum of AES-128 (or equivalent) for symmetric encryption and a minimum of RSA-3072 (or equivalent) for asymmetric keys.

For CAs that distribute self-signed Certificates to relying parties, subject public keys SHALL be at least:

- RSA 2048 bits or ECC 256 bits for Certificates expiring on or before December 31, 2030.
- RSA 3072 bits or ECC 256 bits for Certificates expiring after December 31, 2030.

Where implemented, Certificate Status Services (CSSs), including OCSP Responders and Delegated OCSP Responders, SHALL use signature algorithms, key sizes, and hash algorithms that meet the requirements of this section.

Key Escrow Databases (KEDs) and Data Decryption Servers (DDSs) SHALL utilize cryptographic keys that are equal to or stronger than the strongest key material being protected, escrowed, or recovered.

6.1.6 Public Key Parameters Generation and Quality Checking

For RSA, the CA SHALL perform partial public key validation as specified in NIST SP 800-89 (section 5.3.3).

For ECC, public keys MUST fall within curves defined in Section 7.1.3. Additionally, the CA should confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine as specified in NIST SP 800-56A (Sections 5.6.2.3.3, or 5.6.2.3.4).

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

Public keys bound into Certificates SHALL be certified for signing, encryption, or key agreement purposes as specified by the associated Certificate profile. Except where expressly permitted by this CP, Certificates SHALL NOT be issued for both signing and encryption purposes.

All Certificates SHALL contain a critical Key Usage extension and SHALL conform to the applicable Certificate profile and associated key usage requirements.

CA Certificates

- CA Certificates SHALL assert only the *keyCertSign* and *cRLSign* Key Usage bits.
- Keys associated with CA Certificates SHALL be used only for signing Certificates and CRLs.
- Where a Certificate is issued for an OCSP Responder or Delegated OCSP Responder, the Key Usage and Extended Key Usage extensions SHALL conform to the applicable Certificate profile.

Subscriber Certificates

- Subscriber Certificates intended solely for authentication SHALL assert only the *digitalSignature* Key Usage bit.
- Subscriber Certificates intended for human digital signatures SHALL assert the *digitalSignature* and *nonRepudiation* Key Usage bits.
- Certificates asserting the *nonRepudiation* Key Usage bit SHALL NOT assert the *keyEncipherment* or *keyAgreement* Key Usage bits.
- Certificates intended for encryption using RSA SHALL assert the *keyEncipherment* Key Usage bit.
- Certificates intended for key agreement using elliptic curve cryptography SHALL assert the *keyAgreement* Key Usage bit.
- Keys associated with Device Subscriber Certificates MAY be used for authentication, digital signature, encryption, or a combination thereof. Except for OCSP Responder Certificates, Device Subscriber Certificates SHALL NOT assert the *nonRepudiation* Key Usage bit.

Dual-Use Certificates

- Rudimentary, Basic, and Medium Assurance Certificates MAY support a single key used for both encryption and digital signature operations for legacy applications.
- Such Certificates:
- SHALL be generated and managed in accordance with signature Certificate requirements;
- SHALL NOT assert the *nonRepudiation* Key Usage bit; and
- SHALL NOT be used to authenticate data that will be validated at a future time based upon the same dual-use Certificate.
- Entrust encourages the use of separate key pairs for key management and digital signature/authentication functions.

Extended Key Usage

- For all Subscriber Certificates issued after June 30, 2019, the Extended Key Usage (EKU) extension SHALL be present.
- Extended Key Usage OIDs SHALL be consistent with the asserted Key Usage bits.
- The EKU extension SHALL NOT contain *anyExtendedKeyUsage* (2.5.29.37.0).

PIV-I Certificates

- All PIV-I Certificates SHALL comply with NIST SP 800-78 and the applicable PIV-I Certificate profile requirements.
- PIV-I Content Signing Certificates SHALL contain a critical Extended Key Usage extension asserting only: *id-fpki-pivi-content-signing* (2.16.840.1.101.3.8.7).
- PIV-I Card Authentication Certificates SHALL contain a critical Extended Key Usage extension asserting *id-piv-cardAuth* (2.16.840.1.101.3.6.8).

The specific Key Usage and Extended Key Usage requirements for Certificates issued under this CP SHALL conform to the applicable Certificate profile worksheets and related profile specifications.

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*.

A FIPS 140 Level 1 or higher validated cryptographic module SHALL be used for all cryptographic operations. Cryptographic modules SHALL be validated to the FIPS 140 level identified in this section or an equivalent internationally recognized standard approved for the applicable use.

The table below summarizes the minimum cryptographic module requirements; higher levels MAY be used.

Assurance Level	CA	CMS & CSS	Subscriber	RA
Rudimentary	Level 1	Level 1	N/A	Level 1 (Hardware or Software)
Basic	Level 2	Level 2	Level 1	Level 1 (Hardware or Software)
Medium	Level 3 (Hardware)	Level 2 (Hardware)	Level 1	Level 2 (Hardware)
PIV-I Card Authentication	Level 3 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)
Medium Hardware	Level 3 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)

Where authorized key recovery services are provided, Key Escrow Databases (KEDs) and Data Decryption Servers (DDSs) SHALL utilize cryptographic modules providing protection equal to or greater than that required for the keys being escrowed, stored, or recovered.

Hardware Subscriber key management keys MAY be recovered into a lower assurance cryptographic module only when necessary to fulfill an authenticated and authorized key recovery request and where such recovery is permitted by the applicable policy, the NFI CPS, and organizational authorization.

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

PIV-I Cards SHALL only be issued using card stock approved by the FIPS 201 Evaluation Program and listed on the GSA Approved Products List (APL). Deprecated card stock MAY continue to be issued for no more than one year after approved replacement card stock becomes available.

For hardware tokens associated with PIV-I, additional requirements are specified in Appendix A.

6.2.1.1 Custodial Subscriber Key Stores

Custodial Subscriber Key Stores are repositories that maintain Subscriber private keys on behalf of multiple Subscribers.

Where custodial Subscriber key stores are used, cryptographic modules protecting escrowed or custodially stored Subscriber keys SHALL meet at least the following requirements:

Assurance Level	Minimum Cryptographic Module Requirement
Rudimentary	FIPS 140 Level 1 (Hardware or Software)
Basic	FIPS 140 Level 2 (Hardware)
Medium	FIPS 140 Level 2 (Hardware)
Medium Hardware	FIPS 140 Level 2 (Hardware)

Authentication to a custodial key store for activation, use, recovery, or release of Subscriber private keys SHALL be commensurate with the assurance level of the associated Certificate.

Where custodial key stores support key escrow or recovery services, access to Subscriber private keys SHALL be restricted to authenticated and authorized parties and SHALL comply with the identification, authentication, authorization, audit, and operational requirements established elsewhere in this CP and the NFI CPS.

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

Use of the private signing key for any Entrust NFI CA operating under this policy SHALL require action by multiple persons as specified in Section 5.2.2 of this CP.

Use of Certificate Status Service (CSS) private signing keys, including OCSP Responders and Delegated OCSP Responders, SHALL require multiparty control at the Medium, Medium Hardware, and PIV-I Card Authentication assurance levels, as specified in Section 5.2.2.

Activation of PIV-I Content Signing private keys SHALL require the same multiparty control requirements established for Entrust NFI CA private signing keys as specified in Section 5.2.2.

6.2.3 Private Key Escrow

CA private signing keys SHALL NOT be escrowed.

Subscriber key management keys MAY be escrowed to support authorized key recovery operations as described in Section 4.12. Subscriber signature keys SHALL NOT be escrowed. Subscriber dual-use keys SHALL NOT be escrowed.

Where a device is issued a separate key management Certificate, the associated key management private key MAY be escrowed in accordance with Section 4.12.

6.2.3.1 Escrow of CA private signature key

CA private signing keys SHALL NOT be escrowed under any circumstances.

6.2.3.2 Escrow of CA encryption key

Entrust NFI CAs do not utilize CA encryption keys for Certificate management operations. Accordingly, escrow of CA encryption keys is not supported.

6.2.3.3 Escrow of Subscriber private signature keys

Subscriber private signature keys SHALL NOT be escrowed.

Private signature keys used for digital signature, authentication, non-repudiation, or PIV-I signing functions SHALL remain under the control of the Subscriber and SHALL NOT be recoverable through key escrow or key recovery services.

6.2.3.4 Escrow of Subscriber private encryption and dual use keys Subscriber

Subscriber key management and encryption private keys MAY be escrowed to support authorized key recovery operations as described in Section 4.12.

Subscriber dual-use private keys SHALL NOT be escrowed.

Where a device has a separate key management Certificate, the associated key management private key MAY be escrowed in accordance with the applicable CPS and approved key recovery procedures.

Escrowed key material SHALL be protected in accordance with the requirements specified in Sections 4.12 and 6.2.

6.2.4 Private Key Backup

Backup of private keys SHALL be performed only where permitted by this CP.

All backups of CA, CSS, and PIV-I Content Signing private signature keys SHALL be protected under the same multiparty control and security protections as the original private key.

At least one backup copy of each CA private signing key SHALL be stored offsite.

Private signature key backups SHALL NOT be exported or stored in plaintext form outside the cryptographic module.

Where backup is permitted, backup copies SHALL provide security protections commensurate with those provided by the original cryptographic module.

The following private key backup requirements apply:

Private Key	Backup
CA <ul style="list-style-type: none"> all applicable policies 	Required
CSS <ul style="list-style-type: none"> all applicable policies 	Optional
PIV-I Content Signing <ul style="list-style-type: none"> <i>id-fpki-certpcy-pivi-contentSigning</i> 	Optional
Hardware Signature and Authentication <ul style="list-style-type: none"> <i>As, RAs, KEDs, CSS, DDS</i> <i>id-fpki-certpcy-pivi-cardAuth</i> <i>id-fpki-certpcy-pivi-hardware</i> 	Not Permitted
Hardware Subscriber Key Management <ul style="list-style-type: none"> <i>id-fpki-certpcy-mediumHardware</i> <i>id-fpki-certpcy-mediumHW-CBP</i> 	Optional

Private Key	Backup
Hardware Device <ul style="list-style-type: none"> <i>id-fpki-certpcy-mediumDeviceHardware</i> 	Optional
Software Signature and Authentication <ul style="list-style-type: none"> <i>id-fpki-certpcy-rudimentaryAssurance</i> <i>id-fpki-certpcy-basicAssurance</i> <i>id-fpki-certpcy-mediumAssurance</i> <i>id-fpki-certpcy-medium-CBP</i> 	Optional *
Software Subscriber Key Management <ul style="list-style-type: none"> <i>id-fpki-certpcy-rudimentaryAssurance</i> <i>id-fpki-certpcy-basicAssurance</i> <i>id-fpki-certpcy-mediumAssurance</i> <i>id-fpki-certpcy-medium-CBP</i> 	Optional
Software Device <ul style="list-style-type: none"> <i>id-fpki-certpcy-mediumDevice</i> 	Optional
* Software Subscriber private signature keys MAY be backed up or copied, but must be held in the Subscriber's control.	

Subscriber private signature keys associated with Medium Hardware Assurance or PIV-I Certificates SHALL NOT be backed up or copied.

Subscriber private signature keys associated with Rudimentary, Basic, or Medium Assurance Certificates MAY be backed up or copied, provided they remain under the Subscriber's control.

Subscriber key management private keys MAY be backed up where permitted by this CP, the NFI CPS, and the applicable RPS.

Device private keys MAY be backed up or copied where permitted by the applicable Certificate profile and CPS.

All backed-up Subscriber, Device, CSS, and Content Signing private keys SHALL be protected at a level commensurate with the protection provided by the original cryptographic module and SHALL NOT be stored in plaintext form outside the cryptographic module.

6.2.5 Private Key Archival

CA private signature keys SHALL NOT be archived.

Subscriber private signature keys SHALL NOT be archived.

Subscriber private encryption keys (key management keys) are archived as part EMS KRS in accordance with Section 4.12.

Subscriber dual-use private keys SHALL NOT be archived.

Where a device is issued a separate key management Certificate, the corresponding device key management private key MAY be archived in support of authorized key recovery operations.

CAs MAY maintain archives of escrowed Subscriber key management keys. Such archives SHALL be protected in accordance with Sections 4.12, 5.1, 5.2, and 6.2.1 of this CP.

Archived key material SHALL be protected against unauthorized disclosure, modification, destruction, and use, and SHALL be accessible only to authenticated and authorized EMS KRS personnel.

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.

CA, CSS and PIV-I Content Signing private signature keys MAY be exported from the cryptographic module only to perform CA key backup procedures as described in Section 6.2.4.

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). Cryptographic modules MUST be protected from unauthorized access.

Subscriber private key activation requirements are detailed in the following table:

Mapped Policy	Activation Requirements
<i>id-fpki-certpcy-basicAssurance</i> <i>id-fpki-certpcy-mediumAssurance</i> <i>id-fpki-certpcy-medium-CBP</i> <i>id-fpki-certpcy-mediumHardware</i> <i>id-fpki-certpcy-mediumHW-CBP</i> <i>id-fpki-certpcy-pivi-hardware</i>	Passphrases, PINs, or biometrics. When passphrases or PINs are used, they MUST be a minimum of six (6) characters. Entry of activation data MUST be protected from disclosure (i.e., the data should not be displayed while it is entered).

Mapped Policy	Activation Requirements
<i>id-fpki-certpcy-mediumDevice</i> <i>id-fpki-certpcy-mediumDeviceHardware</i>	<p>MAY be configured to activate the private key without requiring a human sponsor or authorized administrator to authenticate to the cryptographic token.</p> <p>The appropriate physical and logical access controls MUST be implemented for the device and its cryptographic token.</p>
<i>id-fpki-certpcy-pivi-contentSigning</i>	<p>MAY be configured to activate the private key without requiring a human sponsor or authorized administrator to authenticate to the cryptographic token.</p> <p>The appropriate physical and logical access controls MUST be implemented for content signing operations conformant with PIV issuance requirements (see [FIPS 201]).</p> <p>The strength of the security controls MUST be commensurate with the level of threat in the PIV-I credential issuance system's environment, and MUST protect the hardware, software, and the cryptographic token and its activation data from compromise.</p>
<i>id-fpki-certpcy-pivi-cardAuth</i>	None.

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

Public key archival SHALL be performed in accordance with the archive requirements specified in Section 5.5 of this CP.

Public keys associated with Certificates issued under this CP SHALL be archived as part of the Certificate archival process and retained for the period specified in Section 5.5.2.

Public key archival records SHALL be protected, maintained, and made available in accordance with the archive protection, retention, recovery, and access requirements applicable to CA and KRS archive records.

6.3.2 Certificate Operational Periods and Key Usage Periods

Key	Private Key	Certificate
Root CA Certificate (self-signed)	30 years	30 years
Federal Bridge CA Certificate	10 years	10 years
Intermediate/Signing CA Certificate	10 years	10 years
Subscriber Authentication	3 years	3 years
Subscriber Signature	3 years	3 years
Subscriber Encryption	Unrestricted	3 years
PIV-I Card Authentication	3 years	3 years
PIV-I Content Signing	3 years	9 years*
Code Signing	3 years	8 years
OCSP Responder	3 years	120 days
Device	3 years	3 years
<i>*Expiration of a PIV-I Content Signing Certificate SHALL be later than the expiration of all active Subscriber Certificates residing on the same PIV-I credential.</i>		

Subscriber Certificates residing on a PIV-I credential SHALL expire no later than the expiration date of the PIV-I hardware token on which they reside.

The validity period of a Subscriber Certificate SHALL NOT exceed the routine re-key identity requirements specified in Section 3.3.1.

CA private signing keys MAY be used to sign CRLs and OCSP Responder Certificates throughout their authorized usage period. All Certificates issued under a specific CA key pair SHALL expire prior to the end of the usage period of that CA key pair.

Where OCSP Responder Certificates are issued, their validity periods SHALL comply with the applicable Certificate profile and CPS requirements.

CAs SHALL NOT issue Subscriber Certificates with validity periods extending beyond the expiration date of the issuing CA Certificate or the operational validity period of the associated CA public key.

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; and,
- Upon appointment of a new Administrator or Operator Trusted Role personnel.

For Medium Assurance and above, RA and Subscriber activation data MAY be user-selected. The strength of the activation data MUST meet or exceed the requirements for authentication mechanisms stipulated for Level 2 in FIPS 140, see Section 6.2.1.

For PIV-I credentials, in the event activation data can be reset by an issuer after a card is locked, authentication of the Subscriber is required. This authentication MUST be conducted in accordance with FIPS 201, Section 2.9.3.

6.4.2 Activation Data Protection

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

- Memorized;
- Biometric in nature;
- Contained within an organizationally approved device or software tool (e.g., password manager) that leverages encryption commensurate with the bit-strength of the key it activates, or
- 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 MS NFI CPS.

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

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 SHALL be conducted by a trusted agent of the issuer.

Additional requirements governing activation data generation, distribution, reset, recovery, protection, storage, management, and destruction SHALL be defined in the NFI CPS.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

For CAs, KEDs, and DDSs 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 CAs and 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;
- Require use of cryptography for session communication and database security;
- Require self-test security-related CA services;
- Require a trusted path for identification of all users;
- Provide residual information protection; and
- Support recovery from key or system failure.

For CSSs and ancillary components operating in a VME, the following security functions also pertain to the hypervisor:

- Require authenticated logins
- Provide discretionary access control
- Provide a security audit capability (see Section 5.4)
- Enforce domain integrity boundaries for security critical processes
- Prohibit object reuse or require separation for CA random access memory
- Require use of cryptography for session communication and database security
- Archive system history and audit data
- Require self-test functionality for security-related CA services
- Require a trusted path for identification of all users
- Provide residual information protection; and
- Require recovery from key or system failure.

The Certificate Status Server 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 (in a VME, these functions are applicable to both the VM and hypervisor):

- Authenticate the identity of users before permitting access to the system or applications;
- Manage privileges of users to limit users to their assigned roles;
- Generate and archive audit records for all transactions; (see Section 5.4)
- Enforce domain integrity boundaries for security critical processes; and
- Support recovery from key or system failure.

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

- Authenticate the identity of users before permitting access to the system or applications;
- Manage privileges of users to limit users to their assigned roles;
- Generate and archive audit records for all transactions; (see Section 5.4)
- Enforce domain integrity boundaries for security critical processes
- provide residual information protection, and;
- Support recovery from key or system failure.

All communications between any PKI trusted role and the CAs SHALL be authenticated and protected from modification.

6.5.2 Computer Security Rating

Computer systems, applications, and components supporting CAs, RAs, CMSs, CSSs, and KRS functions SHALL meet the security requirements specified throughout this CP, the NFI CPS, and supporting security documentation. Where computer security ratings, certifications, evaluations, validations, or assessments are required by applicable laws, regulations, contracts, accreditation requirements, or governing authorities, Entrust SHALL ensure that affected systems comply with those requirements.

The NFI CPS SHALL identify any additional computer security rating, certification, validation, or assessment requirements applicable to systems operating under this CP.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The system development controls for NFI CAs (including any remote workstations used to administer the CA), RAs, and supporting Operating Systems 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, including the VME hypervisor, SHALL be dedicated to operating and supporting the CA (i.e., the systems and services dedicated to the issuance and management of Certificates) 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. In a VME, a single hypervisor MAY support multiple CAs and their supporting systems, provided all systems have comparable security controls and are dedicated to the support of the CA.
- In a VME, all VM systems MUST operate in the same security zone as the CA.
- 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 supplied from the vendor with no modifications and as the version intended for use. The CA SHALL periodically verify the integrity of the software.

6.6.3 Life Cycle Security Controls

Life cycle security controls SHALL be applied to CA, RA, CSS, CMS, and KRS software, hardware, and supporting infrastructure.

Such controls SHALL include:

- Security requirements definition and documentation;
- Controlled development, testing, implementation, and change management processes;
- Verification and validation of software, firmware, hardware, and configuration changes prior to deployment;

- Procedures to detect unauthorized modifications to software, firmware, configuration, and operational environments;
- Protection against malicious software through approved software sources, integrity verification, and periodic malware scanning; and
- Configuration management controls throughout the system life cycle.

The NFI CPS SHALL describe the life cycle security controls, procedures, and technical safeguards implemented to protect CA, RA, CSS, CMS, and KRS components throughout their operational life cycle.

6.7 Network Security Controls

CAs, RAs, CMSs, repositories, CSSs, KEDs, DDSs, and remote workstations used to administer CAs or KRS components SHALL employ appropriate network security controls.

Network guards, firewalls, filtering routers, or equivalent boundary protection devices SHALL protect CA and KRS equipment. Such devices SHALL limit inbound and outbound network services to those necessary to perform authorized CA and KRS functions.

Protection SHALL be provided against known network attacks. Unused network ports and services SHALL be disabled. Network software present on CA, CSS, KED, DDS, RA, CMS, repository, and administrative workstation systems SHALL be limited to that necessary to support authorized PKI or KRS functions.

Any boundary control devices protecting networks hosting PKI or KRS equipment SHALL deny all services except those explicitly required for operation of the applicable systems.

The CA SHALL establish communications with remote workstations used to administer CA or KRS functions only after successful mutual authentication of the remote workstation at an assurance level commensurate with that of the system being administered.

Remote workstation communications with CA, KRS, CSS, and associated boundary control devices SHALL provide data integrity and confidentiality protections.

Remote administration communications SHALL be encrypted and SHALL be protected against replay attacks, machine-in-the-middle attacks, and unauthorized modification.

Where mutual authentication relies upon a shared secret, the shared secret SHALL:

- Be randomly generated.
- Possess entropy commensurate with the cryptographic strength of the Certificates issued by the PKI being administered.
- Be changed at least annually.

Following establishment of the remote connection, remote administration SHALL only be permitted after successful multi-factor authentication of the Trusted Role personnel at an assurance level commensurate with that of the system being administered.

All communications between PKI and KRS trusted roles and CA, CSS, KED, DDS, RA, CMS, repository, or other supporting systems SHALL be authenticated and protected against unauthorized modification.

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.

7.0 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

Certificates and Certificate status services operating under this CP SHALL conform to the applicable certificate profiles defined in the Federal Bridge Certificate and CRL Profile (FBCA-PROF).

PIV-I Authentication, PIV-I Card Authentication, and PIV-I Content Signing Certificates SHALL conform to the applicable profile worksheets specified in FBCA-PROF.

All other Certificates issued under this CP SHALL conform to the X.509 Certificate and CRL Extensions Profile requirements specified in FBCA-PROF.

The NFI CPS and associated Certificate profile documentation MAY define additional requirements provided such requirements do not conflict with the applicable FBCA-PROF requirements.

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 Entrust NFI CAs operating under this policy SHALL comply with the applicable Certificate and CRL profile requirements defined in [FBCA-PROF].

Entrust NFI CAs issuing PIV-I Authentication, PIV-I Card Authentication, or PIV-I Content Signing Certificates SHALL comply with the applicable profile worksheets defined in [FBCA-PROF].

Certificate Status Service (CSS) Certificates, including OCSP Responder and Delegated OCSP Responder Certificates associated with PIV-I Certificate issuance, SHALL comply with the applicable requirements defined in [FBCA-PROF].

CA Certificates SHALL NOT include critical private extensions.

Subscriber Certificates MAY include critical private extensions provided such extensions are interoperable within their intended community of use and do not interfere with Certificate path validation or Certificate interoperability.

CA and Subscriber Certificates MAY include any extensions permitted by RFC 5280, but SHALL include all extensions required by this CP and the applicable Certificate profiles.

Optional or additional extensions SHALL NOT conflict with the Certificate and CRL profile requirements identified in Section 7.1.

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:

<i>sha-1WithRSAEncryption</i>	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }
<i>sha256WithRSAEncryption</i>	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
<i>sha512WithRSAEncryption</i>	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13 } (1.2.840.113549.1.1.13)
<i>id-RSASSA-PSS</i>	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10 }
<i>ecdsa-with-SHA256</i>	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2 }
<i>ecdsa-with-SHA384</i>	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }
<i>ecdsa-with-SHA512</i>	{ 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:

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

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

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

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

<i>ansip256r1</i>	{ iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7 }
<i>ansip384r1</i>	{ iso(1) identified-organization(3) certicom(132) curve(0) 34 }

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

7.1.4 Name Forms

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

7.1.5 Name Constraints

NFI CA Certificates do not assert Name Constraints extensions.

Should Name Constraints be implemented in the future, the constraints SHALL be defined in the applicable Certificate profile and CPS and SHALL comply with RFC 5280 and the applicable requirements of FBCA-PROF.

7.1.6 Certificate Policy Object Identifier

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

Certificates SHALL assert at least one Certificate Policy OID as specified in Section 1.2 of the CP in the Certificate policies extension.

Entrust NFI CAs SHALL NOT assert Federal Bridge Certificate Authority (FBCA) Certificate Policy OIDs in Certificates they issue, except within the subjectDomain field of the policyMappings extension in Certificates issued to the FBCA for the purpose of establishing policy equivalence mappings between FBCA policy OIDs and Entrust NFI policy OIDs.

Certificates issued for PIV-I card authentication or PIV-I content signing SHALL NOT express any policy OIDs other than the applicable PIV-I policy OID.

Delegated OCSP Responder Certificates SHALL assert all policy OIDs for which they are authoritative.

All asserted Certificate Policy OIDs SHALL be consistent with the applicable Certificate profile requirements defined in Section 7.1 and FBCA-PROF.

7.1.7 Usage of Policy Constraints Extension

CAs operating under this policy MAY assert policy constraints in CA Certificates. When this extension appears, at least one of *requireExplicitPolicy* or *inhibitPolicyMapping* SHALL be present. When present, this extension MAY be marked critical. For Subordinate CA Certificates, *inhibitPolicyMapping* skip certs SHALL be set to 0. For Cross-Certificates, *inhibitPolicyMapping* skip certs SHALL be set appropriately. When *requireExplicitPolicy* is included, skip certs SHALL be set to 0. Additional constraints and configuration values SHALL comply with RFC 5280, FBCA-PROF, and applicable Certification Practice Statements (CPSs).

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates MAY contain policy qualifiers identified in RFC 5280.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Certificates issued under this policy SHALL contain a non-critical Certificate Policies extension.

The Certificate Policies extension SHALL include the Certificate Policy OID(s) appropriate to the Certificate type and assurance level as specified in this CP and the applicable Certificate profile requirements.

7.1.10 Inhibit Any Policy Extension

CAs operating under this policy MAY assert *InhibitAnyPolicy* in CA Certificates. When present, this extension MAY be marked as critical. The *skipCerts* value SHALL be set to zero. Use of the *InhibitAnyPolicy* extension SHALL comply with RFC 5280, FBCA-PROF, and the applicable NFI CPS.

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 operating under this policy SHALL conform to FBCA-PROF,

7.3 OCSP Profile

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

All CSSs MUST accept and return SHA-1 hashes in the CertID and responderID fields. CSS MAY accept and return additional hash algorithms within the CertID fields. CSSs MUST not return any response containing a hash algorithm in the CertID that differs from the CertID in the request.

7.3.1 Version Number(s)

CSSs MUST use OCSP version 1.

7.3.2 OCSP Extensions

Critical OCSP extensions MUST not be used.

8.0 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

All entities operating under this policy are subject to an annual review by the FPKIPA to ensure their policies and operations remain consistent with the policy mappings in the Certificate issued to the Entity by the FBCA.

The EPMA SHALL have a compliance audit mechanism in place to ensure that the requirements of their CPS are being implemented and enforced.

The EPMA 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.

The compliance audit of CAs and RAs SHALL be carried out in accordance with the requirements as specified in *the FPKI Annual Review Requirements* document [AUDIT].

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

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

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 or the RPS. 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 EPMA 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 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 annual review package to the FPKIPA. This package SHALL be prepared in accordance with the *FPKI Annual Review 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.

9.0 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

No Stipulation.

9.1.1 Certificate Issuance or Renewal Fees

Entrust MAY enter fees into contracts for the services governed by this CP and MAY charge fees for Certificate issuance and renewal in accordance with such contracts.

9.1.2 Certificate Access Fees

Entrust SHALL make CA Certificates available in accordance with Sections 2 of this CP. No separate fee is charged for access to publicly available CA Certificates. Entrust MAY charge access fees for Subscriber Certificates, in accordance with its contracts.

9.1.3 Revocation or Status Information Access Fees

Entrust SHALL NOT charge additional fees for:

- Revocation of Certificates issued under this CP;
- Access to Certificate Revocation Lists (CRLs); or
- Access to Online Certificate Status Protocol (OCSP) status information.

9.1.4 Fees for other Services

No Stipulation.

9.1.5 Refund Policy

Entrust MAY provide refunds in accordance with contractual requirements.

9.2 Financial Responsibility

This CP contains no financial 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

Entrust SHALL maintain what it determines to be appropriate insurance coverage with respect to services governed by this CP. Insurance requirements MAY be documented in contracts with customers.

9.2.2 Other Assets

Entrust SHALL have access to such other resources as it determines reasonable to support operations and fulfill its obligations with respect to services governed by this CP.

9.2.3 Insurance or Warranty Coverage for End-Entities

Insurance and/or warranty coverage for end entities MAY be documented in contracts with customers.

9.3 Confidentiality of Business Information

CA information identified in Section 2 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

The scope of confidential business information exchanged between Entrust and other entities SHALL be set out in contracts between Entrust and such other entities.

9.3.2 Information not within the Scope of Confidential Information

Information that is not marked or labeled as confidential, and that is not otherwise defined as confidential under a contract, is not within the scope of confidential information under this CP.

9.3.3 Responsibility to Protect Confidential Information

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

Entrust SHALL maintain the confidentiality of information clearly marked or labeled as confidential that is shared with it.

Entrust SHALL treat such information with at least the same degree of care and security as it treats its own confidential information of a similar nature.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Entrust follows the policies, statements and practices available at <https://www.entrust.com/legal-compliance/privacy> ("Privacy Plan") when handling personal information.

9.4.2 Information Treated as Private

For CAs operating under this CP, collection of PII SHALL be limited to the minimum necessary to validate the identity of the Subscriber. This MAY include attributes that correlate identity evidence

to authoritative sources. The RA SHALL provide explicit notice to the Subscriber regarding the purpose for collecting and maintaining a record of the PII necessary for identity proofing and the consequences for not providing the information. PII collected for identity proofing purposes SHALL NOT be used for any other purpose.

9.4.3 Information not Deemed Private

Information included in Certificates is not subject to protections outlined in Section 9.4.2, but SHALL NOT be sold to any party.

9.4.4 Responsibility to Protect Private Information

Sensitive information MUST be stored securely, and MAY be released only in accordance with other stipulations in Section 9.4.

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

9.4.5 Notice and Consent to Use Private Information

Subscribers are hereby notified and consent to the release of their personal information as permitted or required in this 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 or an applicable contract, 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

Entrust retains all rights, title, and interest (including all intellectual property rights), in, to and under this CP, its CPS and all Certificates, except for any information that is supplied by a Subscriber and that is included in a Certificate, which information SHALL remain the property of the Subscriber. No right is or SHALL be deemed to be granted under this CP, whether by implication, estoppel, inference or otherwise.

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

9.6 Representations and Warranties

The representations and warranties described in this section apply to Entrust NFI CAs, RAs, EMS-KRS, Subscribers, Affiliated Organizations, Relying Parties, and other participants operating or receiving the benefit of services governed by this CP.

These obligations apply to such entities as they pertain to such entities' activities governed by this CP.

9.6.1 CA Representations and Warranties

The Entrust Policy Authority determines whether this CP meets Entrust's legal and policy requirements. Entrust understands that review of Entrust's CP by the FPKIPA is not a substitute for due care and mapping of Certificate policies by Entrust.

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

An RA that performs registration functions MUST comply with the stipulations of the applicable policy and CPS.

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

This CP does not prescribe how a Relying Party determines whether to rely upon a Certificate.

Relying Parties SHALL be responsible for making their own determination regarding Certificate reliance, including Certificate path validation, Certificate status verification, and evaluation of Certificate suitability for the intended transaction.

9.6.5 Representations and Warranties of Affiliated Organizations

Affiliated Organizations SHALL be responsible for authorizing 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

Internal Third-Party Requestors and External Third-Party Requestors (collectively, Third-Party Key Requestors) SHALL formally acknowledge and agree to the applicable obligations described in this section prior to receiving recovered key material.

Third-Party Key Requestors SHALL:

- Protect recovered Subscriber key material from unauthorized access, disclosure, modification, loss, or compromise using administrative, physical, technical, personnel, and procedural security controls appropriate to the sensitivity of the recovered key material.
- Destroy or surrender Subscribers' keys when no longer required (i.e., when the data has been recovered).
- Request and use recovered Subscriber key material only to recover Subscriber data that they are authorized to access and only for the documented and authorized recovery purpose.
- Accurately represent their identity, authority, and purpose during all key recovery operations.
- Provide accurate identification and authentication information sufficient to verify their identity and authority (and at least to the same level required for issuing new PKI Certificates at the level of the key being requested) prior to the release of recovered key material.
- Protect information associated with each key recovery operation from unauthorized disclosure or modification.
- Acknowledge receipt of recovered key material and agree to comply with all applicable laws, regulations, Subscriber organizational policies, and agreements governing the protection, use, disclosure, and handling of recovered keys and recovered data.
- Attest that:
 - Their identity has been truthfully and accurately represented;
 - The reason for the recovery request has been truthfully described;
 - They have a legitimate and authorized need to obtain the requested key material;
 - The recovered key material will be used only for the stated and authorized purpose;

- The recovered key material will be protected from unauthorized access, use, disclosure, modification, or loss; and
- When no longer required, the recovered key material will be destroyed or returned in accordance with applicable procedures and organizational requirements.

9.7 Disclaimers of Warranties

Entrust SHALL NOT disclaim warranties that it is required to give under this CP.

Except for such required warranties and any warranties Entrust MAY give under contract to a particular entity, Entrust disclaims any and all representations, conditions or warranties of any kind, express or implied, including warranties of non-infringement, title, merchantability or fitness for a purpose, satisfactory quality, or any representations, conditions or warranties implied by statute, course of dealing, course of performance, or usage or trade.

Limitations of Liability

Where Entrust is a party to a contract with another entity, limitations of liability are governed by such contract.

SUBJECT TO THE FOREGOING AND IF THE ABOVE DOES NOT APPLY:

IN NO EVENT WILL ENTRUST, ITS AFFILIATES AND THEIR RESPECTIVE SUPPLIERS, LICENSORS, SUBCONTRACTORS, DIRECTORS, OFFICERS AND PERSONNEL (“ENTRUST GROUP”) BE LIABLE FOR ANY CONSEQUENTIAL, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR EXEMPLARY DAMAGES OR FOR ANY LOSS OF BUSINESS, OPPORTUNITIES, CONTRACTS, REVENUES, PROFITS, SAVINGS, GOODWILL, REPUTATION, USE, OR DATA, OR COSTS OF REPROCUREMENT OR BUSINESS INTERRUPTION, OR ANY LOSS OR DAMAGE THAT IS NOT DIRECTLY ATTRIBUTABLE TO ENTRUST’S SERVICES PROVIDED UNDER THIS CP INCLUDING ANY LOSS OR DAMAGE RESULTING FROM THE COMBINATION OR INTEGRATION OF THE CERTIFICATE OR SERVICES WITH ANY SOFTWARE OR HARDWARE NOT PROVIDED BY ENTRUST IF THE LOSS OR DAMAGE WOULD NOT HAVE OCCURRED AS A RESULT OF USE OF THE CERTIFICATE OR CERTIFICATE SERVICES ALONE.

IN NO EVENT WILL ENTRUST GROUP’S TOTAL AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS CP AND THE USE AND PERFORMANCE OF ANY PRODUCTS AND SERVICES PROVIDED HEREUNDER EXCEED ONE THOUSAND UNITED STATES DOLLARS (\$1,000.00 U.S.).

THE EXCLUSIONS AND LIMITS IN THIS SECTION (LIMITATIONS OF LIABILITY) APPLY: (A) REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT (INCLUDING FUNDAMENTAL BREACH), TORT (INCLUDING NEGLIGENCE), WARRANTY, BREACH OF STATUTORY DUTY, MISREPRESENTATION, STRICT LIABILITY, STRICT PRODUCT LIABILITY, OR OTHERWISE; (B) ON AN AGGREGATE BASIS, REGARDLESS OF THE NUMBER OF CLAIMS, TRANSACTIONS, DIGITAL SIGNATURES OR CERTIFICATES; (C) EVEN IF THE POSSIBILITY OF THE DAMAGES IN QUESTION WAS KNOWN OR COMMUNICATED IN ADVANCE AND EVEN IF SUCH DAMAGES WERE FORESEEABLE;

AND (D) EVEN IF THE REMEDIES FAIL OF THEIR ESSENTIAL PURPOSE. ENTRUST HAS SET ITS PRICES AND PROVIDES CERTIFICATES IN RELIANCE ON THE EXCLUSIONS AND LIMITS IN THIS SECTION (LIMITATIONS OF LIABILITY), WHICH FORM AN ESSENTIAL BASIS OF THE PROVISION OF THE SERVICES DESCRIBED IN THIS CP.

Notwithstanding anything to the contrary in this Section (Limitation of Liability), to the extent required by applicable law Entrust neither excludes nor limits its liability for: (i) death or bodily injury caused by its own negligence; (ii) its own fraud or fraudulent misrepresentation; or (iii) other matters for which liability cannot be excluded or limited under applicable law.

9.8 Indemnities

No stipulation.

9.9 Term and Termination

Requirements for the CP term and termination are set out below.

9.9.1 Term

This CP becomes effective when approved by the Entrust Policy Authority. This CP has no specified term. It remains in effect until replaced or terminated by the Entrust PA.

9.9.2 Termination

Termination of this CP is at the discretion of the Entrust Policy Authority, acting in accordance with applicable EPMA governance and change management procedures.

9.9.3 Effect of Termination and Survival

If this CP is terminated, the requirements of the last version of this CP remain in effect through the end of the archive period for the last Certificate issued.

Entrust SHALL determine and implement any transition, archival, notification, and operational requirements necessary to support continuing compliance and trust services following termination of the CP.

9.10 Individual Notices and Communications with Participants

Any planned change to the infrastructure that have the potential to affect the FPKI operational environment SHALL be communicated to the FPKIPA by the Entrust Policy Authority at least two weeks prior to implementation. All new artifacts (CA Certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the change SHALL be provided to the FPKIPA within 24 hours following implementation.

For all other communications, no stipulation

9.11 Amendments

9.11.1 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.

9.11.2 Notification Mechanism and Period

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

9.11.3 Circumstances under which OID MUST be changed

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

9.12 Dispute Resolution Provisions

Any disputes arising with respect to this CP or Certificates issued under this policy SHALL be resolved in accordance with the applicable contract between the relevant parties.

9.13 Governing Law

The construction, validity, performance and effect of Certificates issued under this CP for all purposes SHALL be governed by the law (statutes, case law and regulations) under which Entrust operates.

9.14 Compliance with Applicable Law

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

9.15 Miscellaneous Provisions

9.15.1 Entire Agreement

Entrust MAY enter into contracts that incorporate this CP and/or the CPS. Where no contract exists between Entrust and another participant in the EMS NFI PKI, this CP and the CPS form the entire agreement between Entrust and such participant.

9.15.2 Assignment

Entrust MAY assign, sell, transfer, or otherwise dispose of this CP, together with all of its rights and obligations under this CP (i) to an Affiliate, or (ii) as part of a sale, merger, or other transfer of all or substantially all the assets or stock of the business of Entrust to which the CP relates.

9.15.3 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.

9.15.4 Enforcement (Attorneys' Fees and Waiver of Rights)

No failure to exercise, no delay in exercising, and no statement or representation other than by any authorized representative in an explicit written waiver, of any right, remedy, or power will operate as a waiver thereof, nor will single or partial exercise of any right, remedy, or power under this CP preclude any other or further exercise thereof or the exercise of any other right, remedy, or power provided in this CP, in law, or in equity. The waiver of the time for performance of any act or condition under this CP does not constitute a waiver of the act or condition itself.

9.15.5 Force Majeure

“Force Majeure Event” means any event or circumstance beyond Entrust’s reasonable control, including floods, fires, hurricanes, earthquakes, tornados, epidemics, pandemics, other acts of God or nature, strikes and other labor disputes, failure of utility, transportation or communications infrastructures, riots or other acts of civil disorder, acts of war, terrorism (including cyber terrorism), malicious damage, judicial action, lack of or inability to obtain export permits or approvals, acts of government such as expropriation, condemnation, embargo, designation as a restricted country, changes in applicable laws or regulations, and shelter-in-place or similar orders, and acts or defaults of third party suppliers or service providers. In the event that a Force Majeure Event directly or indirectly causes a failure or delay in Entrust’s performance of its obligations under this CP, Entrust shall not be in default or liable for any loss or damages where performance is impossible or commercially impracticable.

9.16 Other Provisions

None.

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 and relies on specifications published by the National Institute of Standards and Technology (NIST).

The following requirements SHALL apply to PIV-I Cards:

1. **Interoperability Requirements**

To ensure interoperability with Federal systems, PIV-I Cards SHALL use a smart card platform that appears on the GSA FIPS 201 Evaluation Program Approved Product List (APL) and SHALL use the PIV Application Identifier (AID).

2. **PIV Card Interface Requirements**

PIV-I Cards SHALL conform to **NIST SP 800-73-4**.

3. **PIV-I Authentication Certificates**

Only PIV-I Authentication Certificates MAY assert a policy OID mapped to the FBCA PIV-I Hardware policy OID and SHALL conform to the applicable profile requirements defined in **FBCA-PROF**.

4. **Digital Signature and Key Management Certificates**

Digital Signature Certificates on a PIV-I credential SHOULD assert a policy mapped to **mediumHardware**. Key Management Certificates on a PIV-I credential SHOULD assert a policy mapped to either **mediumAssurance** or **mediumHardware**.

5. **Card Authentication Certificate**

PIV-I Cards SHALL contain an asymmetric X.509 Certificate for Card Authentication that:

- a. Conforms to **FBCA-PROF**;
- b. Conforms to **NIST SP 800-73-4**; and
- c. Is issued under the PIV-I Card Authentication policy.

6. **Cardholder Facial Image**

PIV-I Cards SHALL contain an electronic representation of the Cardholder Facial Image printed on the card, as specified in **NIST SP 800-73-4** and **NIST SP 800-76-2**.

7. **Optional Certificates**

The X.509 Certificates for Digital Signature and Key Management described in **NIST SP 800-73-4** are optional for PIV-I Cards.

8. **Visual Distinction Requirements**

Visual distinction of a PIV-I Card from a Federal PIV Card SHALL ensure that the card cannot reasonably be mistaken for a Federal PIV credential. Examples of acceptable visual distinction include, but are not limited to:

- a. Printing a phrase such as *PIV-Interoperable, Company Credential, Organization Credential, Local Access Only*, or similar wording indicating the card is not a Federal PIV Card;

- b. Printing the card in a horizontal (landscape) format rather than a vertical (portrait) format; and
- c. Using a distinctive color scheme or background.

For non-Federally issued PIV-I credentials, images or logos SHALL NOT be placed entirely within Zone 11F (Agency Seal) as defined by **FIPS 201**.

9. **Required Front-of-Card Elements**

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 applicable; otherwise the issuer of the card; and
- d. Card expiration date.

10. **Card Lifetime**

PIV-I Cards SHALL have an expiration date not to exceed six (6) years from issuance.

11. **Relationship to Content Signing Certificate**

Expiration of the PIV-I Card SHOULD NOT be later than the expiration date of the PIV-I Content Signing Certificate residing on the card.

12. **PIV-I Content Signing Certificate**

The digital signature Certificate used to sign objects on the PIV-I Card (e.g., CHUID and Security Object) SHALL contain a policy OID mapped to the FBCA PIV-I Content Signing policy OID. The PIV-I Content Signing Certificate SHALL conform to **FBCA-PROF**.

13. **Card Management System Requirements**

The PIV-I Content Signing Certificate and corresponding private key SHALL be managed within a trusted Card Management System as defined in Appendix B.

14. **Activation and Release of PIV-I Cards**

At issuance, the RA SHALL activate and release the PIV-I Card to the Subscriber only after a successful one-to-one (1:1) biometric match of the applicant against the biometrics collected in Section 3.2.3.1.

15. **Card Personalization and Post-Issuance Updates**

PIV-I Cards MAY support activation by the Card Management System to facilitate card personalization and post-issuance updates. To activate a 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 **NIST SP 800-73-4**. When cards are personalized, card management keys SHALL be unique to each PIV-I Card. Card management keys SHALL meet the algorithm and key size requirements specified in **NIST SP 800-78-4, Cryptographic Algorithms and Key Sizes for Personal Identity Verification**.

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.

APPENDIX C: IN-PERSON ANTECEDENT

This Appendix describes the baseline requirements for an in-person antecedent identity proofing event. An Antecedent event is an in-person proofing event that occurred previously and may suffice as meeting the in-person identity proofing requirements for a new Certificate. The requirement for antecedent is identical to in-person identity proofing in Section 3.2 with the exception of using an historical in-person ID proofing event, and reliance on an on-going relationship. Hence, a proposed antecedent process MUST:

1. meet the thoroughness (rigor) of the in-person event,
2. provide supporting ID proofing artifacts or substantiate the applicant through an existing relationship, and
3. bind the individual to the asserted identity.

The Antecedent process may be appropriate when the applicant has no reasonable access to a Registration Authority or other Enrollment facility.

The Antecedent process requires that the applicant – an employee, member, or associate – has an on-going relationship with the Sponsor and that an equivalent in-person identity proofing event was conducted with the Sponsor on some previous date. The Sponsor MUST attest to the validity of the individual's claimed identity through this existing relationship and provide details concerning the antecedent identity proofing event, including the date of the event, unique applicant identity information and existing artifacts from the event, if any, to the RA.

The following outlines specific requirements for the antecedent identity proofing and credential issuance process.

1. Identity Proofing Relationships
 - The Sponsor of the applicant MUST have a contractual relationship with the Entity PKI.
 - The Sponsor MUST have an established relationship with the applicant. The relationship MUST be sufficient to enable the RA to, with a high degree of certainty, verify that the person seeking the PKI Certificate is the same person that was identity proofed.
 - The Sponsor's application MUST contain a description of the relationship with the applicant describing the initial identity proofing or qualifications and the on-going relationship.
2. Antecedent in-person identity proofing event
 - The Applicant MUST have provided a National Government-issued Picture I.D., or two Non- National Government I.D.s, one of which was a photo I.D. (e.g., Driver's License) during the antecedent identity proofing event. The identity of the entity providing confirmation of the antecedent identity proofing process MUST be captured in an auditable record.
3. Registration Authority (RA) The RA MUST base its decision concerning the validity of the applicant's claimed identity on the information provided via the Antecedent identity proofing process and verification that the applicant is the same individual.
 - The RA MUST record the date of the antecedent in-person identity proofing event as provided by the Sponsor.

- The RA MUST obtain the historical artifacts from the Antecedent event, if any.
 - The RA MUST be able to verify the applicant matches the individual who participated in the Antecedent proofing process.
4. Information source requirements.
- The Antecedent process MUST ensure that all data received by the RA from the Sponsor is validated, protected, and securely exchanged.
 - All participants MUST store and exchange private information in a confidential and tamper evident manner protected from unauthorized access.
5. Binding the Certificate request to the identity.

The process to bind the claimed identity to the specific Certificate request MUST provide commensurate levels of assurance with the Certificate being issued.

- A Sponsor for the applicant MUST provide the Entity PKI with initial contact information, (e.g., name, email address, phone number, sponsoring organization).
- The PKI MUST use the Sponsor provided information to contact the applicant.

APPENDIX D: REFERENCES

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

Reference	Title
FBCA-CP	<i>X.509 Certificate Policy for the U.S. Federal Bridge Certification Authority</i> , current approved version
FBCA-PROF	<i>Federal Bridge Certificate and CRL Profile (FBCA-PROF)</i> , current approved version
FIPS 140-3	<i>Security Requirements for Cryptographic Modules</i> , NIST, March 2019
FIPS 186-5	<i>Digital Signature Standard (DSS)</i> , NIST, February 2023
FIPS 201-3	<i>Personal Identity Verification (PIV) of Federal Employees and Contractors</i> , NIST, January 2022
NIST SP 800-53 Rev. 5	<i>Security and Privacy Controls for Information Systems and Organizations</i> , NIST, September 2020
NIST SP 800-57 Part 1 Rev. 5	<i>Recommendation for Key Management, Part 1: General</i> , NIST, May 2020
NIST SP 800-63-4	<i>Digital Identity Guidelines</i> , NIST, current approved revision
NIST SP 800-73-4	<i>Interfaces for Personal Identity Verification (PIV)</i> , NIST
NIST SP 800-76-2	<i>Biometric Data Specification for Personal Identity Verification</i> , NIST
NIST SP 800-78-4	<i>Cryptographic Algorithms and Key Sizes for Personal Identity Verification</i> , NIST
NIST SP 800-79-2	<i>Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)</i> , NIST
NIST SP 800-85A-4	<i>PIV Card Application and Middleware Interface Test Guidelines</i> , NIST
RFC 3647	<i>Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework</i> , November 2003
RFC 5280	<i>Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile</i> , May 2008
RFC 6960	<i>X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP)</i>
RFC 8017	<i>PKCS #1: RSA Cryptography Specifications Version 2.2</i>
Privacy Act	<i>Privacy Act of 1974, as amended</i>
FOIA	<i>Freedom of Information Act (5 U.S.C. §552)</i>
OMB A-130	<i>Managing Information as a Strategic Resource</i>

APPENDIX E: 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
OA	Operational Authority
PA	Policy Authority
EMPA	Entrust Management Policy Authority
ERC	Enhanced Reliability Check
EMS NFI	Entrust Managed Services Non-Federal Identities
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 interoperability 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)
VME	Virtual Machine Environment
WWW	World Wide Web
PKIX	Public Key Infrastructure X.509

APPENDIX F: GLOSSARY

Term	Definition
Access	Ability to make use of any Information System (IS) resource.
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems.
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using prescribed safeguards at an acceptable level of risk.
Activation Data	Private data, other than cryptographic keys, required to access cryptographic modules or activate private keys.
Affiliated Organization	Organization that authorizes affiliation with Subscribers of PIV-I Certificates.
Applicant	Entity that has applied for a Certificate but has not yet completed the Certificate issuance process.
Archive	Collection of documents and records preserved as evidence of CA, RA, CSS, CMS, or KRS activities.
Audit	Independent review and examination of records and activities to assess compliance with applicable policies, procedures, and controls.
Audit Log	Chronological record of system activities.
Audit Record	Individual entry in an audit log.
Authenticate	To verify the identity of an entity.
Authentication	Security measure used to establish the validity of an identity, transmission, message, or originator.
Backup	Copy of data, software, configuration, or key material retained to facilitate recovery.
Binding	Process of associating two or more related elements of information.

Term	Definition
Biometric	Measurable physical or behavioral characteristic used to verify identity.
Certificate	Digitally signed data structure binding a public key to a named or identified subject.
Certification Authority (CA)	Trusted entity that issues and manages X.509 Certificates and Certificate Revocation Lists (CRLs).
CA Facility	Personnel, equipment, software, procedures, and facilities used to perform CA operations.
Certificate Management Authority (CMA)	A Certification Authority (CA) or Registration Authority (RA).
Certification Authority Software	Software used to manage Certificate issuance, revocation, publication, and related cryptographic operations.
Certificate Policy (CP)	Administrative policy governing Certificate issuance and management.
Certification Practice Statement (CPS)	Statement describing the practices employed by a CA in issuing, managing, revoking, suspending, and renewing Certificates.
Certificate Revocation List (CRL)	List of revoked Certificates published by a CA.
Certificate Status Server (CSS)	Trusted entity that provides online Certificate status information.
Client	System entity that requests services from a server.
Compromise	Unauthorized disclosure, modification, destruction, loss, or use of information or cryptographic material.
Computer Security Objects Registry (CSOR)	NIST registry of security-related object identifiers (OIDs).
Confidentiality	Assurance that information is disclosed only to authorized entities.

Term	Definition
Containerization	Operating system virtualization technology in which applications execute within isolated containers sharing a common operating system.
Cross-Certificate	Certificate used to establish trust between two Certification Authorities.
Cryptographic Module	Hardware, software, firmware, or combination thereof implementing cryptographic functions within a defined security boundary.
Custodial Subscriber Key Store	Repository that stores private keys for multiple Subscribers in a centralized location.
Data Decryption Server (DDS)	System that retrieves escrowed Subscriber key management keys to facilitate authorized data decryption and recovery.
Data Integrity	Assurance that information has not been altered without authorization.
Device	Non-person entity, including hardware, software, applications, systems, or services.
Digital Signature	Cryptographic transformation used to validate origin, authenticity, and integrity of information.
Encryption Certificate	Certificate containing a public key used for encryption or key establishment.
Entity	Organization, corporation, agency, or community having operational control of a CA.
Entity CA	CA operated under the authority of an Entity.
Firewall	Boundary protection mechanism controlling network traffic in accordance with security policy.
Hypervisor	Software, firmware, or hardware used to create and manage virtual machines.
In-Person Antecedent	Previously completed in-person identity proofing event that may satisfy current proofing requirements.

Term	Definition
Integrity	Protection against unauthorized modification or destruction of information.
Intermediate CA	CA subordinate to another CA and superior to one or more subordinate CAs.
Key Escrow	Storage of Subscriber key management private keys for authorized recovery purposes.
Key Escrow Database (KED)	System that stores escrowed private keys and supports key recovery operations.
Key Exchange	Process of exchanging public keys to establish secure communications.
Key Generation Material	Random values, pseudo-random values, and cryptographic parameters used during key generation.
Key Pair	Mathematically related public and private keys used in asymmetric cryptography.
Key Recovery	Authorized retrieval and delivery of escrowed key material.
Key Recovery Agent (KRA)	Individual authorized to perform key recovery operations in conjunction with other authorized personnel.
Key Recovery Official (KRO)	Individual authorized to validate and submit key recovery requests.
Key Recovery Policy (KRP)	Administrative policy governing escrow, storage, recovery, and protection of key management private keys.
Key Recovery Practices Statement (KRPS)	Statement describing the practices employed by a Key Recovery System in protecting and recovering escrowed keys.
Key Recovery System (KRS)	Collection of personnel, systems, procedures, and controls supporting key escrow, storage, recovery, and delivery of Subscriber key management keys.

Term	Definition
Modification (Certificate)	Replacement of a Certificate with another Certificate containing changed information.
Mutual Authentication	Process by which communicating parties authenticate one another.
Network Guard	High-assurance boundary protection device controlling access between protected and external networks.
Non-Repudiation	Assurance that an entity cannot successfully deny having performed an action.
Object Identifier (OID)	Globally unique identifier used to identify Certificate policies, algorithms, and other PKI objects.
Offline CA	CA isolated from network connectivity and typically maintained in a powered-off state except during ceremony operations.
Out-of-Band	Communication using a channel different from the primary communication path.
Physically Isolated Network	Network not connected to systems outside a physically controlled environment.
PKI Sponsor	Individual authorized to act on behalf of a Device Subscriber or group during Certificate lifecycle activities.
Policy Management Authority (PMA)	Authority responsible for creating, maintaining, and approving Certificate policies and practice statements.
Privacy	Protection of Subscriber and Relying Party information in accordance with applicable laws and regulations.
Private Key	Secret cryptographic key used for signing or decryption.
Public Key	Cryptographic key used for signature verification or encryption.
Public Key Infrastructure (PKI)	Collection of policies, procedures, personnel, systems, and technologies used to manage Certificates and cryptographic keys.

Term	Definition
Registration Authority (RA)	Entity responsible for identity proofing and registration of Subscribers on behalf of a CA.
Re-key	Replacement of a cryptographic key and issuance of a corresponding Certificate.
Relying Party	Entity that relies upon a Certificate or digital signature.
Remote Workstation	Secure workstation used to administer CA, CMS, CSS, KRS, KED, DDS, or HSM systems from outside the protected operating environment.
Renew	Issuance of a replacement Certificate that continues an existing binding.
Repository	System storing Certificates, CRLs, OCSP responses, or related information.
Revoke	Prematurely terminate the validity of a Certificate.
Risk	Probability that a threat will successfully exploit a vulnerability and cause harm.
Root CA	Trust anchor at the top of a certification hierarchy.
Server	System entity providing services to clients.
Signature Certificate	Certificate containing a public key intended primarily for digital signature operations.
Structural Container	Distinguished Name attribute used solely to support directory structure requirements.
Subordinate CA	CA whose signing key is certified by another CA.
Subscriber	Entity that is the subject of a Certificate and possesses the corresponding private key.
Superior CA	CA that certifies the Certificate signing key of another CA.

Term	Definition
Supervised Remote Identity Proofing	Remote identity proofing process providing assurance equivalent to in-person identity proofing and conforming to NIST SP 800-63A requirements.
System Software Layer	Software layer providing services to higher-level software, including operating systems, hypervisors, virtual machines, and container platforms.
Third-Party Key Recovery Requestor	Individual or organization authorized to request recovery of escrowed key material on behalf of a Subscriber or organization.
Threat	Circumstance or event capable of causing harm to information systems or information.
Trust List	Collection of trusted Certificates used as trust anchors.
Trusted Agent	Individual authorized to act on behalf of a CA in verifying Subscriber identity information.
Trusted Certificate	Certificate accepted as a trust anchor.
Two-Person Control	Procedure requiring two authorized individuals to jointly supervise and perform a security-sensitive operation.
Zeroize	Process of irreversibly erasing information from storage media to prevent recovery.

End of document, this page left intentionally blank.