

Non-Federal Identity (NFI) Public Key Infrastructure Certification Practices Statement [REDACTED]

Version 2.2

12 November, 2025



Non-Federal Identity (NFI) Public Key Infrastructure Certification
Practices Statement [REDACTED]

Version: 2.2

Signature Page

Jim Trovato

Entrust Federal mPKI Policy Authority (Print Name)

Signed by:
Jim Trovato
89D32B44D9C945B...

Entrust Federal mPKI

Policy Authority

12 November, 2025

Date

CONTENTS

1	Introduction.....	14
1.1	Overview.....	16
1.1.1	Certificate Policy ([CP]).....	16
1.1.2	Relationship between the [CP] and this CPS	16
1.1.3	Scope	16
1.1.4	Interoperation with CAs Issuing under Different Policies.....	16
1.2	Document Name and Identification	17
1.3	PKI Participants	18
1.3.1	PKI Authorities	19
1.3.1.1	Entrust Policy Management Authority (EPMA).....	19
1.3.1.2	EPMA Policy Authority Program Managers	20
1.3.1.3	RA Agency/Organization PMA	20
1.3.1.4	EMS NFI Operational Authority	21
1.3.1.5	EMS NFI Certification Authority	21
1.3.1.6	Root Certification Authorities.....	21
1.3.1.7	Issuing Certification Authorities.....	22
1.3.1.8	Certificate Status Servers.....	22
1.3.2	Registration Authorities	22
1.3.3	Card Management System	24
1.3.4	Trusted Agents	24
1.3.5	Subscribers.....	24
1.3.6	Affiliated Organizations	25
1.3.7	Relying Parties	26
1.3.8	Other Participants	26
1.4	Certificate Usage.....	26
1.4.1	Appropriate Certificate Uses	26
1.4.2	Prohibited Certificate Uses.....	27
1.5	Policy Administration	27
1.5.1	Organization Administering the Document.....	27
1.5.2	Contact Information	27
1.5.3	Person Determining CPS Suitability for the Policy	28
1.5.4	CPS Approval Procedures.....	28
1.6	Definitions and Acronyms.....	28
2	Publication and Repository Responsibilities.....	28
2.1	Repositories	29
2.1.1	Repository Obligations.....	29

2.2	Publication of Certification Information	29
2.2.1	Publication of Certificates and Certificate Status.....	29
2.2.1.1	HTTP Servers	30
2.2.1.2	LDAP Directory Infrastructure	30
2.2.1.3	Certificate Status Infrastructure.....	30
2.2.2	Publication of CA Information.....	31
2.2.3	Interoperability.....	31
2.3	Time or Frequency of Publication	31
2.4	Access Controls on Repositories	31
2.4.1	Access Controls on Root CA Repositories.....	31
2.4.2	Access Controls on Issuing CA Repositories.....	32
3	Identification and Authentication.....	32
3.1	Naming.....	33
3.1.1	Types of Names	33
3.1.1.1	Types of Names for the Root CA.....	34
3.1.1.2	Types of Names for the Issuing CA.....	35
3.1.2	Need for Names to be Meaningful	42
3.1.2.1	Need for Root CA Names to be Meaningful.....	42
3.1.2.2	Need for Issuing CA Names to be Meaningful	43
3.1.3	Anonymity or Pseudonymity of subscribers	43
3.1.4	Rules for Interpreting Various Name Forms	44
3.1.5	Uniqueness of Names	44
3.1.6	Recognition, Authentication, and Role of Trademarks.....	44
3.2	Initial Identity Validation	44
3.2.1	Method to Prove Possession of Private Key	44
3.2.2	Authentication of Organization Identity	45
3.2.3	Authentication of Individual Identity.....	45
3.2.3.1	Authentication of Human subscribers	45
3.2.3.1.1	Basic and Rudimentary Policies.....	47
3.2.3.1.2	PIV-I Policies	48
3.2.3.1.3	All Other (Medium) Policies	51
3.2.3.1.4	Trusted Role Credentials	55
3.2.3.2	Authentication of Human subscribers For Role-based Certificates	59
3.2.3.3	Authentication of Human subscribers for Group Certificates	60
3.2.3.4	Authentication of Devices.....	61
3.2.4	Non-Verified subscriber Information	61
3.2.5	Validation of Authority	62
3.2.6	Criteria for Interoperation	62
3.3	Identification and Authentication for Re-Key Requests.....	62
3.3.1	Identification and Authentication for Routine Re-Key.....	62
3.3.1.1	Root CA	62
3.3.1.2	Issuing CA	62
3.3.2	Identification and Authentication for Re-Key After Revocation	63
3.4	Identification and Authentication for Revocation Request	63

- 3.4.1 Root CA 63
- 3.4.2 Issuing CA 64
- 4 Certificate Life-Cycle Operational Requirements 64
 - 4.1 Certificate Application 65
 - 4.1.1 Who Can Submit a Certificate Application 65
 - 4.1.1.1 CA Certificates 65
 - 4.1.1.1.1 Cross-Certification Certificate Application..... 66
 - 4.1.1.1.2 Issuing CA Certificate Application 66
 - 4.1.1.2 User Certificates 66
 - 4.1.1.3 Device Certificates 66
 - 4.1.2 Enrollment Process and Responsibilities 66
 - 4.2 Certificate Application Processing 67
 - 4.2.1 Performing Identification and Authentication Functions 67
 - 4.2.1.1 Cross-Certificates 67
 - 4.2.1.2 Issuing CA Certificates 67
 - 4.2.2 Approval or Rejection of Certificate Applications 68
 - 4.2.3 Time to Process Certificate Applications 68
 - 4.3 Certificate Issuance..... 68
 - 4.3.1 CA Actions during Certificate Issuance 68
 - 4.3.1.1 Root CA 68
 - 4.3.1.2 Issuing CA 69
 - 4.3.2 Notification to subscriber by the CA of Issuance of Certificate 69
 - 4.4 Certificate Acceptance..... 70
 - 4.4.1 Conduct Constituting Certificate Acceptance 70
 - 4.4.2 Publication of the Certificate by the CA 70
 - 4.4.3 Notification of Certificate Issuance by the CA to Other Entities 70
 - 4.5 Key Pair and Certificate Usage 70
 - 4.5.1 Subscriber Private Key and Certificate Usage 71
 - 4.5.2 Relying Party Public key and Certificate Usage 71
 - 4.6 Certificate Renewal 71
 - 4.6.1 Circumstance for Certificate Renewal 71
 - 4.6.2 Who May Request Renewal 71
 - 4.6.3 Processing Certificate Renewal Requests 71
 - 4.6.4 Notification of New Certificate Issuance to subscriber 71
 - 4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 72
 - 4.6.6 Publication of the Renewal Certificate by the CA..... 72
 - 4.6.7 Notification of Certificate Issuance by the CA to Other Entities 72
 - 4.7 Certificate Re-key 72
 - 4.7.1 Circumstance for Certificate Re-key 73
 - 4.7.2 Who May Request Certification of a New Public Key 73
 - 4.7.2.1 Root CA 73
 - 4.7.2.2 Issuing CA 74
 - 4.7.3 Processing Certificate Re-keying Requests 74
 - 4.7.4 Notification of New Certificate Issuance to subscriber 74

4.7.5	Conduct Constituting Acceptance of a Re-keyed Certificate	74
4.7.6	Publication of the Re-keyed Certificate by the CA	74
4.7.7	Notification of Certificate Issuance by the CA to Other Entities	74
4.8	Certificate Modification.....	74
4.8.1	Circumstance for Certificate Modification.....	74
4.8.2	Who May Request Certificate Modification	75
4.8.3	Processing Certificate Modification Requests.....	75
4.8.4	Notification of New Certificate Issuance to subscriber	75
4.8.5	Conduct Constituting Acceptance of Modified Certificate.....	75
4.8.6	Publication of the Modified Certificate by the CA.....	75
4.8.7	Notification of Certificate Issuance by the CA to Other Entities	75
4.9	Certificate Revocation and Suspension.....	76
4.9.1	Circumstances for Revocation	78
4.9.2	Who Can Request Revocation	78
4.9.2.1	Root CA	78
4.9.2.2	Issuing CAs.....	79
4.9.3	Procedure for Revocation Request	81
4.9.3.1	Root CA	81
4.9.3.2	Issuing CAs.....	82
4.9.4	Revocation Request Grace Period.....	83
4.9.5	Time within which CA must Process the Revocation Request	83
4.9.5.1	Root CA	83
4.9.5.2	NFI CA	83
4.9.6	Revocation Checking Requirements for Relying Parties	84
4.9.7	CRL Issuance Frequency	84
4.9.7.1	Root CA	84
4.9.7.2	Issuing CA	84
4.9.8	Maximum Latency for CRLs.....	84
4.9.9	On-line Revocation/Status Checking Availability.....	84
4.9.10	On-line Revocation Checking Requirements	85
4.9.11	Other Forms of Revocation Advertisements Available	85
4.9.12	Special Requirements Related to Key Compromise	85
4.9.13	Circumstances for Suspension	85
4.9.13.1	Root CA	85
4.9.13.2	Issuing CA	85
4.9.14	Who Can Request Suspension	86
4.9.15	Procedure for Suspension Request	87
4.9.16	Limits on Suspension Period	88
4.9.17	Procedures for Restoration of a Suspended Certificate	88
4.10	Certificate Status Services	89
4.10.1	Operational Characteristics	89
4.10.2	Service Availability	89
4.10.3	Optional Features.....	89
4.11	End of Subscription	90

4.12	Key Escrow and Recovery	90
4.12.1	Key Escrow and Recovery Policy and Practices.....	90
4.12.2	Session Key Encapsulation and Recovery Policy and Practices	90
5	Facility, Management, and Operational Controls.....	90
5.1	Physical Controls	91
5.1.1	Site Location and Construction	91
5.1.2	Physical Access.....	91
5.1.2.1	Physical Access for CA Equipment.....	91
5.1.2.2	Physical Access for RA Equipment.....	95
5.1.2.3	Physical Access for CSS Equipment	96
5.1.2.4	Physical Access for CMS Equipment	96
5.1.3	Power and Air Conditioning.....	96
5.1.4	Water Exposures.....	97
5.1.5	Fire Prevention and Protection.....	97
5.1.6	Media Storage.....	97
5.1.7	Waste Disposal.....	97
5.1.8	Off-Site Backup.....	97
5.2	Procedural Controls	97
5.2.1	Trusted Roles	97
5.2.1.1	Administrator.....	98
5.2.1.1.1	Security Officers / Master Users (SOMUs).....	99
5.2.1.1.2	System Administrator	100
5.2.1.1.3	System Administrator and SOMU Functions	100
5.2.1.2	Officer	101
5.2.1.2.1	Registration Authorities	101
5.2.1.2.2	Local Registration Authorities	101
5.2.1.3	Auditor.....	102
5.2.2	Number of Persons Required per Task	102
5.2.2.1	Root CA	102
5.2.2.2	Issuing CAs.....	103
5.2.3	Identification and Authentication for Each Role.....	103
5.2.4	Separation of Roles	103
5.3	Personnel Controls	103
5.3.1	Background, Qualifications, Experience, and Security Clearance Require- ments	103
5.3.2	Background Check Procedures	104
5.3.3	Training Requirements.....	105
5.3.4	Retraining Frequency and Requirements.....	105
5.3.5	Job Rotation Frequency and Sequence.....	106
5.3.6	Sanctions for Unauthorized Actions	106
5.3.7	Independent Contractor Requirements	106
5.3.8	Documentation Supplied to Personnel	106
5.4	Audit Logging Procedures.....	107
5.4.1	Types of Events Recorded.....	107

5.4.2	Frequency of Processing Log.....	111
5.4.2.1	SIEM Alert Event List	112
5.4.3	Retention Period for Audit Log	113
5.4.4	Protection of Audit Log.....	113
5.4.5	Audit Log Backup Procedures	114
5.4.6	Audit Collection System (Internal vs. External)	114
5.4.7	Notification to Event-Causing Subject	114
5.4.8	Vulnerability Assessments	114
5.5	Records Archival	115
5.5.1	Types of Events Archived	115
5.5.2	Retention Period for Archive	117
5.5.3	Protection of Archive.....	117
5.5.4	Archive Backup Procedures	118
5.5.5	Requirements for Time-Stamping of Records	118
5.5.6	Archive Collection System (Internal or External)	118
5.5.7	Procedures to Obtain and Verify Archive Information	118
5.6	Key Changeover	119
5.6.1	Root CA	119
5.6.2	Issuing CA	119
5.7	Compromise and Disaster Recovery	120
5.7.1	Incident and Compromise Handling Procedures.....	120
5.7.2	Computing Resources, Software, and/or Data Are Corrupted.....	121
5.7.3	Entity (CA) Private Key Compromise Procedures	122
5.7.3.1	CA Key or CA Software is Compromised with Unknown Date of Compromise....	123
5.7.3.2	CA Key is Compromised with Known Date of Compromise	123
5.7.3.3	CA Software is Compromised with Known Date of Compromise	123
5.7.3.4	Subscriber Key Compromise	124
5.7.4	Business Continuity Capabilities after a Disaster	124
5.8	CA & RA Termination	124
5.8.1	RAO Suspension	125
5.8.2	RAO Termination	125
6	Technical Security Controls	126
6.1	Key Pair Generation and Installation	127
6.1.1	Key Pair Generation	127
6.1.1.1	CA Key Pair Generation.....	127
6.1.1.2	Subscriber Key Pair Generation	127
6.1.2	Private Key Delivery to subscriber.....	128
6.1.3	Public Key Delivery to Certificate Issuer	129
6.1.4	CA Public Key Delivery to Relying Parties	130
6.1.5	Key Sizes	131
6.1.6	Public Key Parameters Generation and Quality Checking	132
6.1.7	Key Usage Purposes (as per X.509 v3 Key Usage Field)	132
6.1.7.1	Root CA	132
6.1.7.2	Issuing CA	133

- 6.2 Private Key Protection and Cryptographic Module Engineering Controls 134
 - 6.2.1 Cryptographic Module Standards and Controls..... 134
 - 6.2.2 Private Key (n out of m) Multi-Person Control 136
 - 6.2.3 Private Key Escrow 136
 - 6.2.3.1 Escrow of CA private signature key 136
 - 6.2.3.2 Escrow of CA encryption key 136
 - 6.2.3.3 Escrow of subscriber private signature keys..... 136
 - 6.2.3.4 Escrow of subscriber private encryption and dual use keys subscriber 136
 - 6.2.4 Private Key Backup..... 137
 - 6.2.4.1 Backup of CA Private Signature Key 137
 - 6.2.4.1.1 Root CA 137
 - 6.2.4.1.2 Issuing CA 137
 - 6.2.4.2 Backup of subscriber private signature key 137
 - 6.2.4.3 Backup of subscriber Private Key Management Key..... 138
 - 6.2.4.4 Backup of CSS Private Key 138
 - 6.2.4.5 Backup of Content Signing Private Key 138
 - 6.2.4.6 Backup of Device Signing Private Keys..... 138
 - 6.2.5 Private Key Archival 139
 - 6.2.6 Private Key Transfer into or from a Cryptographic Module 139
 - 6.2.7 Private Key Storage on Cryptographic Module 139
 - 6.2.8 Method of Activating Private Key 139
 - 6.2.8.1 Root CA 140
 - 6.2.8.2 Issuing CA 140
 - 6.2.9 Method of Deactivating Private Key 140
 - 6.2.10 Method of Destroying Private Key..... 141
 - 6.2.11 Cryptographic Module Rating..... 141
- 6.3 Other Aspects of Key Pair Management 141
 - 6.3.1 Public Key Archival 141
 - 6.3.2 Certificate Operational Periods and Key Usage Periods 141
 - 6.3.2.1 Root CA 141
 - 6.3.2.2 Issuing CA 142
- 6.4 Activation Data..... 142
 - 6.4.1 Activation Data Generation and Installation..... 142
 - 6.4.2 Activation Data Protection 143
 - 6.4.3 Other Aspects of Activation Data 144
- 6.5 Computer Security Controls..... 144
 - 6.5.1 Specific Computer Security Technical Requirements 144
 - 6.5.1.1 Root CA 145
 - 6.5.1.2 Issuing CA 145
 - 6.5.2 Computer Security Rating..... 146
- 6.6 Life Cycle Technical Controls 146
 - 6.6.1 System Development Controls..... 146
 - 6.6.1.1 Root CA 146
 - 6.6.1.2 Issuing CA 147

6.6.2	Security Management Controls	148
6.6.3	Life Cycle Security Controls	149
6.7	Network Security Controls	149
6.7.1	Root CA	149
6.7.2	Issuing CA	150
6.8	Time-Stamping	150
7	Certificate, CRL, and OCSP Profiles	150
7.1	Certificate Profile	151
7.1.1	Version Number(s)	151
7.1.2	Certificate Extensions	151
7.1.3	Algorithm Object Identifiers.....	151
7.1.4	Name Forms	153
7.1.4.1	Root CA	153
7.1.4.2	Issuing CA	153
7.1.5	Name Constraints	153
7.1.6	Certificate Policy Object Identifier	154
7.1.7	Usage of Policy Constraints Extension	154
7.1.8	Policy Qualifiers Syntax and Semantics	154
7.1.9	Processing Semantics for the Critical Certificate Policies Extension.....	154
7.1.10	Inhibit Any Policy Extension.....	154
7.2	CRL Profile	154
7.2.1	Version Number(s)	155
7.2.2	CRL and CRL Entry Extensions.....	155
7.3	OCSP Profile.....	155
8	Compliance Audit and Other Assessments.....	155
8.1	Frequency or Circumstances of Assessment	156
8.2	Identity/Qualifications of Assessor	156
8.3	Assessor’s Relationship to Assessed Entity	156
8.4	Topics Covered by Assessment	157
8.5	Actions Taken as a Result of Deficiency	157
8.6	Communication of Results	159
9	Other Business and Legal Matters	159
9.1	Fees	160
9.1.1	Certificate Issuance or Renewal Fees	160
9.1.2	Certificate Access Fees	160
9.1.3	Revocation or Status Information Access Fees	160
9.1.4	Fees for other Services	160
9.1.5	Refund Policy	160
9.2	Financial Responsibility.....	160
9.2.1	Insurance Coverage	160
9.2.2	Other Assets	160
9.2.3	Insurance or Warranty Coverage for End-Entities.....	160
9.3	Confidentiality of Business Information	160
9.3.1	Scope of Confidential Information.....	160

9.3.2	Information not within the Scope of Confidential Information	161
9.3.3	Responsibility to Protect Confidential Information	161
9.4	Privacy of Personal Information	161
9.4.1	Privacy Plan	161
9.4.2	Information Treated as Private	161
9.4.3	Information not Deemed Private.....	162
9.4.4	Responsibility to Protect Private Information	162
9.4.5	Notice and Consent to Use Private Information	162
9.4.6	Disclosure Pursuant to Judicial or Administrative Process.....	162
9.4.6.1	Judicial Processes	162
9.4.6.2	Administrative Processes.....	163
9.4.7	Other Information Disclosure Circumstances	163
9.4.7.1	Release as Part of Civil Discovery	163
9.4.7.2	Disclosure Upon Owner's Request.....	163
9.4.7.3	Other Information Release Circumstances	163
9.5	Intellectual Property Rights	163
9.6	Representations and Warranties	163
9.6.1	CA Representations and Warranties	164
9.6.2	RA Representations and Warranties	164
9.6.3	Subscriber Representations and Warranties.....	164
9.6.4	Relying Parties Representations and Warranties.....	164
9.6.5	Representations and Warranties of Affiliated Organizations	164
9.6.6	Representations and Warranties of Other Participants.....	164
9.7	Disclaimers of Warranties	164
9.8	Limitations of Liability.....	165
9.9	Indemnities	165
9.10	Term and Termination	165
9.10.1	Term	165
9.10.2	Termination	165
9.10.3	Effect of Termination and Survival	165
9.11	Individual Notices and Communications with Participants.....	165
9.12	Amendments	165
9.12.1	Procedure for Amendment	165
9.12.2	Notification Mechanism and Period	165
9.12.3	Circumstances under which OID must be changed	166
9.13	Dispute Resolution Provisions.....	166
9.14	Governing Law.....	166
9.15	Compliance with Applicable Law	166
9.16	Miscellaneous Provisions	166
9.16.1	Entire Agreement.....	166
9.16.2	Assignment	166
9.16.3	Severability	166
9.16.4	Enforcement (Attorneys' Fees and Waiver of Rights).....	166
9.16.5	Force Majeure.....	167

9.17	Other Provisions	167
9.17.1	Waivers	167
10	Bibliography.....	167
11	Acronyms and Abbreviations	169
12	Glossary	171
	Appendix A: Piv-Interoperable Smart Card Definition.....	181
	Appendix B: Card Management System Requirements	183
13	Appendix C: External Service Providers	184
14	Appendix D: Delegated Registration Authorities.....	185

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]
1.1.1	May 26, 2009	Align Section 5.3.1 with the FBCA [CP] and other minor corrections
1.1.2	June 09, 2009	Updates based upon comments from the FBCA CPWG mapping review.
1.2	March 5, 2010	Revised to incorporate requirements for SAFE and align with version 1.2 of the EMS NF PKI X.509 [CP]
1.3	September 30, 2010	Revised to incorporate requirements for PIV-I for the US Federal Government
1.4	March 20, 2011	Revised to clarify sections that were identified as unclear during annual audit
1.5	August 15, 2011	Revised Section 6.1.4.2 to clarify key update certificate issuance for Issuing CAs
1.6	June 10, 2016	Update for current policy and practices
1.7	July 20, 2018	Updated to reflect the changes to Version 1.7 of the Certificate Policy.
1.8	April 17, 2020	Updated to reflect the changes to Version 1.8 of the Certificate Policy and mapping comments from the audit
1.9	October 7 th , 2021	Updated to align document more closely with FBCA [CP]
2.0	October 27 th , 2022	Updated to align with NFI CP 2.0 updates
2.1	January 3 rd , 2024	Updated to align with NFI CP 2.1 updates
2.2	November 12 th , 2025	Major update to address service updates and compliance requirements

1 INTRODUCTION

Entrust Corporation (Entrust)) has implemented a comprehensive, outsourced Public Key Infrastructure (PKI) to provide the services necessary to support Non-Federal entities. The Entrust Non-Federal Identity (NFI) PKI, referred to as EMS NFI, is a Shared Service Provider (SSP) PKI.

The EMS NFI is compliant with the *Entrust Managed Services Non-Federal Identity Public Key Infrastructure Certificate Policy Version 2.2*, [CP]. The EMS NFI consists of products and services that provide and manage X.509 public key certificates. Certification Authorities (CAs) are part of this PKI and generate and manage (revoke, suspend, restore) X.509 public key certificates, and bind the subscribers to their public/private key pairs through the issuance of these X.509 certificates. These CAs are hereafter referred to as NFI CAs.

The EMS NFI consists of multiple CAs; a self-signed Root Certification Authority, hereafter referred to as the Root CA, and one or more Subordinate CAs, hereafter referred to as Issuing CAs. The EMS NFI was instantiated for interoperation with Federal PKIs, through cross certification with the Federal Bridge Certificate Authority (FBCA). The EMS NFI consists of the NFI Root CA and NFI Subordinate/Issuing CA(s) known as the as the NFI Shared Service Provider (SSP) CA(s).

This CPS covers sixteen (16) policies defined in the [CP]. The policies represent five different assurance levels (Rudimentary, Basic, Medium, PIV-I Card Authentication, and Medium Hardware) for public key certificates. The level of assurance refers to the strength of the binding between the public key and the individual whose subject name is cited in the certificate, the mechanisms used to control the use of the private key, and the security provided by the PKI itself.

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

This Certification Practices Statement CPS is applicable for NFI CA issued certificates, to support access to systems that have not been designated as national security systems. Certificates are issued to state and local governments, commercial employees, contractors, and other affiliated personnel for the purposes of authentication, signature, and confidentiality.

This CPS defines the practices under which the NFI CAs operate. This CPS is subject to review and approval by the Entrust Managed Services Policy Authority (Entrust PA).

This CPS is applicable to all entities with relationships with the NFI CAs, including Trusted Role users. No end user certificates are issued from the Root CA. All individual certificates issued from the NFI Root CA are to those entities filling Trusted Roles. This CPS provides these entities with a clear statement of the practices and responsibilities of the NFI CAs, as well as the responsibilities of each entity in dealing with the NFI CAs.

Security management services provided by the NFI CAs include the following:

- Key Generation/Storage/Recovery
- Certificate and Certificate Revocation List (CRL) generation and distribution
- Certificate Update, Renewal, and Re-key

- Certificate token initialization/programming/management
- System Management Functions (e.g., security audit, certificate tracking, archive, etc.)

The security and trustworthiness of the EMS NFI depends on the security of the hardware, software, facilities, personnel, and procedures used in the operation of the NFI CAs.

This CPS is consistent with Internet Engineering Task Force (IETF) Request for Comment (RFC) 3647: *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework*.

The remaining sections of this document have been redacted and are not included in this version. For additional information regarding the NFI PKI and related Certification Authorities, please refer to:

<https://www.entrust.com/legal-compliance/federal-pki>

Please contact your representative for any further information regarding this document.