Combined X.509 Certification Practices Statement
For the
Entrust PKI SSP (ETPKISSP)
Federal Root Certification Authority
&
Federal Shared Service Provider Certification Authorities
(3.22 REDACTED)

Version 3.22

SIGNATURE PAGE

JIM TROVATO

Entrust Federal mPKI Policy Authority (Print Name)

Signed by:
Jim Trovato
89D32B44D9C945B...

28 May, 2026

Entrust Federal mPKI
Policy Authority

ETPKISSP CPS RECORD OF CHANGES

Version	Date	Author(s)	Reason	Description
2.1	22 January 2009	Entrust Cygnacom	Apply corrections / recommendations from Compliance Audit	Changed or added sections and text, including record of changes table.
2.2	17 June 2009	Entrust Cygnacom	Combine Root and Subordinate CPS documents into one document per discussions with external auditor	Combine the Root and Subordinate CPS documents and make changes correction to practice as necessary.
2.3	18 March 2011	Entrust	Updates to address areas of clarification required as a result of Annual Audit	Numerous changes required to provide greater clarification in aligning practices with the CPS document
2.4	13 March 2012	Entrust	Updates to address areas of clarification in regards to background investigation and update to CRL issuance	Section 4.9.3.2 and 5.3.2
2.5	20 July 2015	Entrust MSO Policy Authority	Updates applied to address changes made in the FCPCA Common Policy CP from 1.18 to 1.24	Changed or added sections and text, including record of changes table.
2.6	28 July 2015	Entrust MSO Policy Authority	Additional updates requested by the Federal PKI to bring the CA into compliance with proposed modifications to the Common Policy Framework Certificate Policy 2 April 2015	Section 3.3.1 Added requirements for Derived PIV; Section 6.1.7 to state that only digitalSignature keyUsage are asserted in in Derived PIV certs; 6.2.1 Add FIPS 140 requirements for Derived PIV; Section 6.2.4.2, 6.2.8 Add Derived PIV;
2.7	24 February 2017	Entrust MSO Policy Authority	Common Policy CPS Evaluation Mapping Matrix v2.13 (Based on FCPCA Certificate	1.3.1.5 fleshed out PMA segment 1.3.1.7 Added segment for CSS Update Entrust to

Version	Date	Author(s)	Reason	Description
			Policy v1.25) September 22, 2016	Entrust Datacard for company name. This does not extend to Entrust MSO or EMSPKI naming at this time
2.8	7 February 2018	Entrust mPKI Policy Authority	Bring the CPS into compliance with the Common Policy Framework Version 1.27, June 29, 2017	Internal Review
2.8.1	9 March, 2018	Entrust mPKI Policy Authority	Minor updates after internal review and finalization	Finalize document
2.9	17 October 2022	Entrust mPKI Policy Authority	Updates reflecting changes adopted by the FPKIPA through common-change-proposal-2018-07; incorporated comments from the last version provided by the FPKI	Final
2.91	3 March 2020	Entrust mPKI Policy Authority	Update CPS to reflect comments from FPKI PA review	Final
2.92	17 April 2020	Entrust mPKI Policy Authority	Update CPS to reflect comments from Auditor	Final
2.93	7 October 2021	Entrust mPKI Policy Authority	Update CPS to reflect comments from internal review	Final
3.0	12 October 2022	Entrust mPKI Policy Authority	Update CPS to reflect CP 2.2, auditor and FPKI feedback.	Final
3.1	17 November 2023	Entrust mPKI Policy Authority	Assimilation of *X.509 Certification Practices Statement For Entrust Managed Service PKI Derived PIV Credential Federal Shared Service Provider Certification Authorities(v1.1)* and *Key Recovery Practices Statement*	Draft

Version	Date	Author(s)	Reason	Description
			(KRPS) for the Entrust Managed Service into this consolidated CPS. Added certificate suspension and restoration, updates relative to CP 2.6, Nov 3, 2023	
3.2	October 2, 2025	EMPA	Major update to address previous findings, align with current practices requirements and introduce delegated digital signature.	Final
3.21	November 12, 2025	EPMA	Updates for audit remediation and updates to reflect current practices	Final
3.22	January 16, 2026	EPMA	Updates for audit remediation of all discrepancies and recommended change requests	Final

ETPKISSSP CPS 3.22 TABLE OF CONTENTS

1.0 INTRODUCTION

- 1.1 Overview
  - 1.1.1 Certificate Policy
  - 1.1.2 Relationship between the Common Policy CP and this CPS
  - 1.1.3 Scope
  - 1.1.4 Interoperation with CAs issuing under different policies
  - 1.1.5 Interoperation with CAs issuing under the same policies
- 1.2 Document Name and Identification
  - 1.2.1 Federal Root CA
  - 1.2.2 FSSP CAs
- 1.3 PKI Participants
  - 1.3.1 PKI Authorities
    - 1.3.1.1 Federal Chief Information Officers Council
    - 1.3.1.2 Federal PKI Policy Authority
    - 1.3.1.3 Entrust Policy Management Authority (EPMA)
    - 1.3.1.4 EPMA Policy Authority Program Managers
    - 1.3.1.5 RA Agency/Organization PMA
    - 1.3.1.6 ETPKISSP Operational Authority
  - 1.3.2 ETPKISSP Certification Authorities
    - 1.3.2.1 Certificate Status Services
  - 1.3.3 Registration Authorities (RA)
    - 1.3.3.1 Registration Authority Organizations (RAO)
    - 1.3.3.2 Trusted Agents
  - 1.3.4 Key Recovery Authorities
    - 1.3.4.1 Key Escrow Database (KED)
    - 1.3.4.2 Data Decryption Server
    - 1.3.4.3 Key Recovery Agent (KRA)
    - 1.3.4.4 Key Recovery Official (KRO)
  - 1.3.5 Key Recovery Requestors
    - 1.3.5.1 Internal Third-Party Requestor
    - 1.3.5.2 External Third-Party Requestor
  - 1.3.6 Subscriber
  - 1.3.7 Relying Parties
  - 1.3.8 Other Participants
- 1.4 Certificate Usage
  - 1.4.1 Appropriate Certificate Uses
  - 1.4.2 Prohibited Certificate Uses
- 1.5 Policy Administration
  - 1.5.1 Organization Administering the Document
  - 1.5.2 Contact Information
  - 1.5.3 Person Determining CPS Suitability for the Policy
  - 1.5.4 CPS Approval Procedures
- 1.6 Definitions and Acronyms

2.0 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories
2.2 Publication of Certification Information
2.2.1 Publication of Certificates and Certificate Status
2.2.1.1 HTTP Servers
2.2.1.2 LDAP Directory Infrastructure
2.2.1.3 Certificate Status Service Infrastructure
2.2.2 Publication of CA Information
2.2.3 Interoperability
2.3 Time or Frequency of Publication
2.3.1 Access Controls on Root CA Repositories
2.3.2 Access Controls on the FSSP CA Repositories

3.0 IDENTIFICATION AND AUTHENTICATION

3.1 Naming
3.1.1 Types of Names
3.1.1.1 Types of Names for the Root CA
3.1.1.1.1 ETPKISSP Trusted Role Users (SOMU, SCO, & RA)
3.1.1.1.2 Certificates issued to FSSP CA
3.1.1.1.3 Certificates issued to Federal department subordinate CAs
3.1.1.1.4 Certificates issued to CSS Servers
3.1.1.2 Types of Names for FSSP CAs
3.1.1.2.1 Trusted Role Users (SOMU, SCO, & RA)
3.1.1.2.2 Certificates issued to CSS Servers
3.1.1.2.3 For customer Local Registration Authorities
3.1.1.2.4 Subscribers
3.1.1.2.5 Device Subscriber certificates
3.1.1.2.6 Derived PIV credentials
3.1.1.2.7 Subscriber Credentials for Delegated Digital Signature
3.1.1.2.8 General Subscriber Naming
3.1.2 Need for Names to be Meaningful
3.1.2.1 Need for Root CA Names to be Meaningful
3.1.2.2 Need for FSSP CA Names to be Meaningful
3.1.3 Anonymity or Pseudonymity of Subscribers
3.1.4 Rules for Interpreting Various Name Forms
3.1.5 Uniqueness of Names
3.1.6 Recognition, Authentication, and Role of Trademarks
3.2 Initial Identity Validation
3.2.1 Method to Prove Possession of Private Key
3.2.2 Authentication of Organization Identity
3.2.3 Authentication of Individual Identity
3.2.3.1 Authentication of Human Subscribers
3.2.3.1.1 Security Officer / Master Users (SOMUs)
3.2.3.1.2 Registration Authorities and Security Compliance Officer
3.2.3.1.3 Local Registration Authorities
3.2.3.1.4 Derived Credentials and RA/LRAs

3.2.3.1.5 Authentication for Derived PIV Credentials
3.2.3.2 Authentication of Devices
3.2.3.3 Authentication for Role-Based certificates
3.2.3.4 Authentication of Human Subscribers for Group Certificates
3.2.4 Non-verified Subscriber Information
3.2.5 Validation of Authority
3.2.6 Criteria for Interoperation
3.3 Identification and Authentication for Re-Key Requests
3.3.1 Identification and Authentication for Routine Re-key
3.3.1.1 Root CA
3.3.1.2 FSSP CAs
3.3.2 Identification and Authentication for Re-Key After Revocation
3.4 Identification and Authentication for Revocation Request
3.4.1 Revocation of Certificates Issued by the Federal Root CA
3.4.2 Revocation of Certificates Issued by FSSP CAs
3.5 Identification and Authentication for Key Recovery Requestion
3.5.1 Third-party Requestor Authentication
3.5.2 Subscriber Authentication
3.5.3 KRA Authentication
3.5.4 KRO Authentication
3.5.5 Data Decryption Server Authentication

4.0 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS
4.1 Certificate Application
4.1.1 Who Can Submit a Certificate Application
4.1.1.1 CA Certificates
4.1.1.2 Cross-Certification Certificate Applications
4.1.1.3 Subordinate CA Certificate Application
4.1.1.4 User Certificates
4.1.1.5 Device Certificates
4.1.1.6 Code Signing Certificates
4.1.1.7 Delegated Digital Signature Credentials
4.1.2 Enrollment Process and Responsibilities
4.2 Certificate Application Processing
4.2.1 Performing Identification and Authentication Functions
4.2.2 Approval or Rejection of Certificate Applications
4.2.3 Time to Process Certificate Applications
4.3 Certificate Issuance
4.3.1 CA Actions During Certificate Issuance
4.3.1.1 Root CA
4.3.1.2 FSSP CA
4.3.2 Notification to Subscriber by the CA of Issuance of Certificate
4.4 Certificate Acceptance
4.4.1 Conduct Constituting Certificate Acceptance
4.4.2 Publication of the Certificate by the CA
4.4.3 Notification of Certificate Issuance by the CA to Other Entities

4.5 Key Pair and Certificate Usage
4.5.1 Subscriber Private Key and Certificate Usage
4.5.2 Relying Party Public key and Certificate Usage
4.6 Certificate Renewal
4.6.1 Circumstance for Certificate Renewal
4.6.2 Who May Request Renewal
4.6.3 Processing Certificate Renewal Requests
4.6.4 Notification of New Certificate Issuance to Subscriber
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate
4.6.6 Publication of the Renewal Certificate by the CA
4.6.7 Notification of Certificate Issuance by the CA to Other Entities
4.7 Certificate Re-key
4.7.1 Circumstance for Certificate Re-key
4.7.2 Who May Request Certification of a New Public Key
4.7.2.1 Root CA
4.7.2.2 FSSP CA
4.7.3 Processing Certificate Re-keying Requests
4.7.4 Notification of New Certificate Issuance to Subscriber
4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate
4.7.6 Publication of the Re-keyed Certificate by the CA
4.7.7 Notification of Certificate Issuance by the CA to Other Entities
4.8 Certificate Modification
4.8.1 Circumstance for Certificate Modification
4.8.2 Who May Request Certificate Modification
4.8.3 Processing Certificate Modification Requests
4.8.4 Notification of New Certificate Issuance to Subscriber
4.8.5 Conduct Constituting Acceptance of Modified Certificate
4.8.6 Publication of the Modified Certificate by the CA
4.8.7 Notification of Certificate Issuance by the CA to Other Entities
4.9 Certificate Revocation and Suspension
4.9.1Circumstances for Revocation
4.9.2Who Can Request a Revocation
4.9.2.1 Root CA
4.9.2.2 FSSP CA
4.9.3 Procedure for Revocation Request
4.9.3.1 Root C
4.9.3.2 FSSP CA
4.9.4 Revocation Grace Period
4.9.5 Time within which CA must Process the Revocation Request
4.9.5.1 Root CA
4.9.5.2 FSSP CA
4.9.6 Revocation Checking Requirements for Relying Parties
4.9.7 CRL Issuance Frequency
4.9.7.1 Root CA
4.9.7.2 FSSP CA
4.9.8 Maximum Latency for CRLs

4.9.9 Online Revocation/Status Checking Availability
4.9.10 On-line Revocation Checking Requirements
4.9.11 Other Forms of Revocation Advertisements Available
4.9.12 Special Requirements Related To Key Compromise
4.9.13 Circumstances for Suspension
4.9.13.1 Root CA
4.9.13.2 FSSP CA
4.9.14 Who Can Request Suspension and Restoration
4.9.15 Procedure for Suspension Request
4.9.16 Limits on Suspension Period
4.10 Certificate Status Services
4.10.1 Operational Characteristics
4.10.2 Service Availability
4.10.3 Optional Features
4.11 End of Subscription
4.12 Key Escrow and Recovery
4.12.1 Key Escrow and Recovery Policy and Practices
4.12.1.1 Key Escrow Process and Responsibilities
4.12.1.2 Key Recovery Process and Responsibilities
4.12.1.3 Key Recovery
4.12.1.4 Automated Self-Recovery
4.12.1.5 Key Recovery During Token Issuance
4.12.1.6 Key Recovery by Data Decryption Server
4.12.1.7 Who Can Submit a Key Recovery Application
4.12.1.8 Requestor Authorization Validation
4.12.1.9 Subscriber Authorization Validation
4.12.1.10 KRA Authorization Validation
4.12.1.11 KRO Authorization Validation
4.12.1.12 Data Decryption Server Authorization Validation
4.12.2 Session Key Encapsulation and Recovery Policy and Practices

5.0 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls
5.1.1 Site Location and Construction
5.1.2 Physical Access
5.1.2.1 Physical Access for CA Equipment
5.1.2.2 Physical Access for RA Equipment
5.1.2.3 Physical Access for CSS Equipment
5.1.2.4 Physical Access for KED Equipment
5.1.2.5 Physical Access for DDS Equipment
5.1.2.6 Physical Access for KRA and KRO Equipment
5.1.3 Power and Air Conditioning
5.1.4 Water Exposures
5.1.5 Fire Prevention and Protection
5.1.6 Media Storage
5.1.7 Waste Disposal

5.1.8 Off-Site Backup
5.2 Procedural Controls
5.2.1 Trusted Roles
5.2.1.1 Administrator
5.2.1.2 System Administrator
5.2.1.3 Security Officers / Master Users (SOMUs)
5.2.1.3.1 SA and SOMU Functions
5.2.1.4 Key Recovery Agent (KRA)
5.2.1.5 Issuing Organization Key Recovery Official (KRO)
5.2.1.6 Super Key Recovery Official (Super KRO)
5.2.1.7 Operator
5.2.1.8 Officer
5.2.1.9 Registration Authoritie
5.2.1.10 Local Registration Authorities
5.2.1.11 Auditor
5.2.1.12 Security Compliance Officer
5.2.2 Number of Persons Required per Task
5.2.2.1 Root CA
5.2.2.2 FSSP CA
5.2.2.3 MSO-KRS Key Recovery Service
5.2.3 Identification and Authentication for Each Role
5.2.4 Roles Requiring Separation of Duties
5.2.4.1 Root CA
5.2.4.2 FSSP CA
5.3 Personnel Controls
5.3.1 Qualifications, Experience, and Clearance Requirements
5.3.2 Background Check Procedures
5.3.3 Training Requirements
5.3.4 Retraining Frequency and Requirements
5.3.5 Job Rotation Frequency and Sequence
5.3.6 Sanctions for Unauthorized Actions
5.3.7 Independent Contractor Requirements
5.3.8 Documentation Supplied to Personnel
5.4 Audit Logging Procedures
5.4.1 Types of Events Recorded
5.4.2 Frequency of Processing Log
5.4.2.1 SIEM Alert Event List
5.4.3 Retention Period for Audit Log
5.4.4 Protection of Audit lo
5.4.5 Audit Log Backup Procedures
5.4.6 Audit Collection System (Internal vs. External)
5.4.7 Notification to Event-Causing Subject
5.4.8 Vulnerability Assessments
5.5 Records Archival
5.5.1 Types of Data Archived
5.5.2 Retention Period for Archive

5.5.3 Protection of Archiv
5.5.4 Archive Backup Procedure
5.5.5 Requirement for Time-Stamping of Archive Records
5.5.6 Archive Collection System (Internal and External)
5.5.7 Procedures to Obtain and Verify Archive Information
5.6 Key Changeover
5.6.1 Root CA
5.6.2 FSSP CA
5.6.3 KRS
5.7 Compromise and Disaster Recovery
5.7.1 Incident and Compromise Handling Procedures
5.7.2 Computer Resources, Software, and/or Data are Corrupted
5.7.3 Entity (CA) Private Key Compromise Procedures
5.7.3.1 CA Key or CA Software Compromised, Dates Unknown
5.7.3.2 CA Key Compromised, Date Known
5.7.3.3 CA Software is Compromised, Date Known
5.7.3.4 KRS Private Key Compromise Procedures
5.7.4 Business Continuity Capabilities after a Disaster
5.8 CA and RA Termination
5.8.1 CA Cessation of Operation
5.8.2 PKI Termination
5.8.3 RA Suspension
5.8.4 RA Termination
5.8.5 KRS Authority Termination
5.8.5.1 KED Termination
5.8.5.2 KRA Termination
5.8.5.3 KRO Termination
5.8.5.4 Data Decryption Server Termination

6.0 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation
6.1.1 Key Pair Generation
6.1.1.1 CA Key Pair Generation
6.1.1.2 Subscriber Key Pair Generation
6.1.1.3 CSS Key Pair Generation
6.1.1.4 PIV Content Signing Key Pair Generation
6.1.1.5 Subscriber Derived PIV Credentials Key Pair Generation
6.1.2 Private Key Delivery to Subscriber
6.1.3 Public Key Delivery to Certificate Issuer
6.1.4 CA Public Key Delivery to Relying Parties
6.1.4.1 Federal Root CA
6.1.4.2 FSSP CA
6.1.5 Key Sizes
6.1.6 Public Key Parameters Generation and Quality Checking
6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)
6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls
6.2.2 Private Key (n out of m) Multi-Person Control
6.2.3 Private Key Escrow
6.2.4 Private Key Backup
6.2.4.1 Backup of CA Private Signature Key
6.2.4.1.1 Federal Root CA
6.2.4.1.2 FSSP CA
6.2.4.2 Backup of Subscriber Private Signature Key
6.2.4.3 Backup of Subscriber Private Key Management Key
6.2.4.4 Backup of CSS Private Key
6.2.4.5 Backup of Device Private Keys
6.2.4.6 Backup of Common PIV/PIV-I Content Signing Key
6.2.5 Private Key Archival
6.2.6 Private Key Transfer into or from a Cryptographic Module
6.2.7 Private Key Storage on Cryptographic Module
6.2.8 Method of Activating Private Key
6.2.8.1 Root CA
6.2.8.2 FSSP CA
6.2.9 Method of Deactivating Private Key
6.2.10 Method of Destroying Private Key
6.2.11 Cryptographic Module Rating
6.3 Other Aspects of Key Pair Management
6.3.1 Public Key Archival
6.3.2 Certificate Operational Periods and Key Usage Periods
6.3.2.1 Federal Root CA
6.3.2.2 FSSP CA
6.4 Activation Data
6.4.1 Activation Data Generation and Installation
6.4.2 Activation Data Protection
6.4.3 Other Aspects of Activation Data
6.5 Computer Security Controls
6.5.1 Specific Computer Security Technical Requirements
6.5.1.1 Federal Root CA
6.5.1.2 FSSP CA
6.5.1.3 CSS / OCSP Servers
6.5.1.4 KRA and KRO Workstations
6.5.2 Computer Security Rating
6.6 Lifecycle Technical Controls
6.6.1 System Development Controls
6.6.1.1 Federal Root CA
6.6.1.2 FSSP CA
6.6.2 Security Management Controls
6.6.3 Life Cycle Security Controls
6.7 Network Security Controls
6.7.1 Federal Root CA
6.7.2 FSSP CA

6.7.3 KRS
6.8 Time-Stamping

7.0 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile
7.1.1 Version Numbers
7.1.2 Certificate Extensions
7.1.3 Algorithm Object Identifiers
7.1.4 Name Forms
7.1.4.1 Root CA
7.1.4.2 FSSP CA
7.1.5 Name Constraints
7.1.6 Certificate Policy Object Identifier
7.1.7 Usage of Policy Constraints Extension
7.1.8 Policy Qualifiers Syntax and Semantics
7.1.9 Processing Semantics for the Critical Certificate Policy Extension
7.1.10 Inhibit Any Policy Extension
7.2 CRL Profile
7.2.1 Version Numbers
7.2.2 CRL and CRL Entry Extensions
7.3 OCSP Profile
7.3.1 Version Number(s)
7.3.2 OCSP Extensions

8.0 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or Circumstances of Assessment
8.2 Identity/Qualifications of Compliance Assessor
8.3 Assessor's Relationship to Assessed Entity
8.4 Topics Covered by Assessment
8.5 Actions Taken as a Result of Deficiency
8.6 Communications of Results

9.0 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees
9.1.1 Certificate Issuance or Renewal Fees
9.1.2 Certificate Access Fees
9.1.3 Revocation or Status Information Access Fees
9.1.4 Fees for Other Services Such as Policy Information
9.1.5 Refund Policy
9.2 Financial Responsibility
9.2.1 Insurance Coverage
9.2.2 Other Assets
9.2.3 Insurance or Warranty Coverage for End-Entities
9.3 Confidentiality of Business Information
9.3.1 Scope of Confidential Information
9.3.2 Information not within the Scope of Confidential Information

9.3.3 Responsibilities to Protect Confidential Information
9.4 Privacy of Personal Information
9.4.1 Privacy Plan
9.4.2 Information Treated as Private
9.4.3 Information not Deemed Private
9.4.4 Responsibilities to Protect Private Information
9.4.5 Notice and Consent to Use Private Information
9.4.6 Disclosure Pursuant to Judicial or Administrative Process
9.4.6.1 Judicial Processes
9.4.6.2 Administrative Processes
9.4.7Other Information Disclosure Circumstances
9.4.7.1 Release as Part of Civil Discovery
9.4.7.2 Disclosure Upon Owner's Request
9.4.7.3 Other Information Release Circumstances
9.5 Intellectual Property Rights
9.6 Representations and Warranties
9.6.1 CA and KED Representations and Warranties
9.6.2 RA and KRO/KRA Representations and Warranties
9.6.2.1 RA Obligations
9.6.2.2 KRA Obligations
9.6.2.3 KRO Obligations
9.6.2.4 Requestor Representations and Warranties
9.6.3 Subscriber and Data Decryption Server Representations and Warranties
9.6.3.1 Subscriber Representations and Warranties
9.6.3.2 Group Encryption Certificate Sponsor and User Representations and Warranties
9.6.3.3 Data Decryption Server Representations and Warranties
9.6.4 Relying Parties Representations and Warranties
9.6.5 Representations and Warranties of Other Participants
9.7 DISCLAIMERS OF WARRANTIES
9.8 LIMITATIONS OF LIABILITY
9.9 INDEMNITIES
9.10 TERM AND TERMINATION
9.10.1 Term
9.10.2 Termination
9.10.3 Effect of Termination and Survival
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS
9.12 AMENDMENTS
9.12.1 Procedure for Amendment
9.12.2 Notification Mechanism and Period
9.12.3 Circumstances under which OID must be Changed
9.13 DISPUTE RESOLUTION PROVISIONS
9.14 GOVERNING LAW
9.15 COMPLIANCE WITH APPLICABLE LAW
9.16 MISCELLANEOUS PROVISIONS
9.16.1 Entire Agreement

9.16.2 Assignment
9.16.3 Severability
9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)
9.16.5 Force Majeure
9.17 OTHER PROVISIONS
9.17.1 Waivers

10.0 BIBLIOGRAPHY

11.0 ACRONYMS AND ABBREVIATIONS

12.0 GLOSSARY

13.0 ACKNOWLEDGMENTS

APPENDIX A: EXTERNAL SERVICE PROVIDERS

APPENDIX B: REGISTRATION AUTHORITY ORGANIZATIONS

APPENDIX C: DERIVED CREDENTIAL ISSUANCE SERVICE

C.1 Derived Credential Issuance Architecture
C.1.1 Entrust Identity Guard Enterprise Server
C.1.2 Derived Credential Revocation Server
C.2 Roles
C.2.1 MSO IDE Administrator
C.2.2 MSO System Administrator
C.2.3 Customer Identity Guard Enterprise Administrator
C.2.4 Customer DCRS Administrator

APPENDIX D: EXAMPLE DEVICE CERTIFICATE REQUEST FORM

1.0 INTRODUCTION

Entrust has implemented a comprehensive, outsourced Public Key Infrastructure (PKI) to provide the services necessary to support Homeland Security Presidential Directive #12 (HSPD-12) and Federal Information Processing Standard Publication 201 (FIPS 201). This PKI, referred to as the Entrust Public Key Infrastructure Shared Service Provider (ETPKISSP), is designed to provide shared service provider (SSP) PKI services to Federal government employees, contractors, and affiliates for the purposes of authentication, digital signature, and confidentiality. This system has not been designed to support national security systems.

The ETPKISSP is compliant with the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework (Common Policy CP) [Common Policy CP], and consists of products and services that provide and manage X.509 certificates for public key cryptography. This PKI includes Certification Authorities (CA) that generate and revoke X.509 public key certificates. The CA binds Subscribers to their public/private key pairs through the issuance of X.509 certificates.

The ETPKISSP shall consist of a Federal Root Certification Authority (Federal Root CA) and one or more Subordinate CAs (SCAs), referred to as the Federal Shared Service Provider CAs (FSSP CAs). To meet Common Policy CP requirements, the ETPKISSP shall also host:

- The Entrust Managed Service Key Recovery Service (MSO-KRS)
- Derived Credential Management Service (DCMS) – this optional service allows designated Subscribers with valid PIV credentials to apply for and receive Common Derived Personal Identity Verification (PIV) certificates. And dedicated ancillary services, including:
- LDAP Repositories – used to publish certificates and revocation information.
- Administration Services – web-based user administration for RA/LRAs.
- Online Certificate Status Protocol (OCSP) Service – this optional OCSP Responder provides relying parties with an alternative method for validating the revocation status of a certificate.
- Digital Autopen Service – an optional service which allows a specific Subscriber to designate another specific Subscriber to digitally sign on their behalf.

Security management services provided by the Federal Root CA and FSSP CAs include the following:

- Key generation and storage.
- Key escrow and recovery.
- Certificate, Derived Credential, and Certificate Revocation List (CRL) Generation and Distribution.
- Repository publishing, providing access to certificates and CRLs.
- Certificate token initialization and management.
- Certificate Update, Modification, Renewal, Suspension/Restoration, and Re-key.
- Certificate token initialization/programming/management.
- System Management Functions (e.g., security audit, certificate tracking, configuration management, archive, etc.).

Specifically excluded are code-signing certificates. ETPKISSP, the Federal Root CA, FSSP CAs, and Ancillary Services do not issue code-signing certificates.

Key Recovery is the ability to escrow and recover private keys from public/private key pairs associated with public key certificates used for key or data encipherment. The Entrust Managed Service Key Recovery Service (MSO-KRS) accesses securely stored end user private keys and provides secure key recovery in accordance with the Common Policy CP.

The Derived Credential Management Service (DCMS) addresses the requirement to issue Derived PIV Credentials that PIV-enable mobile devices in accordance with the Common Policy CP and guidance provided by NIST SP800-157.

The security and trustworthiness of the Federal Root CA, FSSP CAs, MSO-KRS, DCMS, and Ancillary Services depend on the security of the hardware, software, facilities, personnel, and procedures used in the operation of the Federal Root CA, FSSP CAs, DCMS, and MSO-KRS.

The remaining sections of this document have been redacted and are not included in this version. For additional information regarding the Federal 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