

**Entrust Managed Services PKI**

**FOR INTERNAL USE ONLY**

*WARNING: This document is For Internal Use Only (FIUO). It is to be controlled, stored, handled, transmitted, distributed and disposed of in accordance with EMS PKI policy relating to FIUO Information and is not to be released to the public or other personnel who do not have a valid need-to-know with prior approval of the EMS PKI Policy Management Authority.*



Combined X.509 Certification Practices Statement

For the

Entrust Managed Service PKI

Federal Root Certification Authority

&

Federal Shared Service Provider Certification Authority

13 March, 2012

Version 2.4

**Signature Page**

|  |  |  |
| --- | --- | --- |
| Entrust Managed Services PKI Policy Authority |  | Date |

CONTENTS

[1.0 Introduction 1](#_Toc233004134)

[1.1 Overview 2](#_Toc233004135)

[1.1.1 Certificate Policy 2](#_Toc233004136)

[1.1.2 Relationship Between the Common Policy CP and this CPS 2](#_Toc233004137)

[1.1.3 Scope 2](#_Toc233004138)

[1.1.4 Interoperation with CAs issuing under different policies 3](#_Toc233004139)

[1.2 Document Name and Identification 3](#_Toc233004140)

[1.2.1 Federal Root CA 3](#_Toc233004141)

[1.2.2 FSSP CA 3](#_Toc233004142)

[1.3 PKI Participants 4](#_Toc233004143)

[1.3.1 PKI Authorities 4](#_Toc233004144)

[1.3.2 Registration Authority 6](#_Toc233004145)

[1.3.3 Trusted Agents 6](#_Toc233004146)

[1.3.4 Subscribers 6](#_Toc233004147)

[1.3.5 Relying Parties 6](#_Toc233004148)

[1.3.6 Other Participants 6](#_Toc233004149)

[1.4 Certificate Usage 6](#_Toc233004150)

[1.4.1 Appropriate Certificate Uses 6](#_Toc233004151)

[1.4.2 Prohibited Certificate Uses 7](#_Toc233004152)

[1.5 Policy Administration 7](#_Toc233004153)

[1.5.1 Organization Administering the Document 7](#_Toc233004154)

[1.5.2 Contact Information 7](#_Toc233004155)

[1.5.3 Person Determining CPS Suitability for the Policy 8](#_Toc233004156)

[1.5.4 CPS Approval Procedures 8](#_Toc233004157)

[1.6 Definitions and Acronyms 8](#_Toc233004158)

[1.6.1 List of Definitions 8](#_Toc233004159)

[1.6.2 List of Acronyms 11](#_Toc233004160)

[2.0 Publication and REPOSITORY RESPONSIBILITIES 13](#_Toc233004161)

[2.1 Repositories 13](#_Toc233004162)

[2.2 Publication of Certification Information 14](#_Toc233004163)

[2.2.1 Publication of Certificates and Certificate Status 14](#_Toc233004164)

[2.2.2 Publication of CA Information 14](#_Toc233004165)

[2.2.3 Interoperability 15](#_Toc233004166)

[2.3 Time or Frequency of Publication 15](#_Toc233004167)

[2.4 Access Controls on Repositories 15](#_Toc233004168)

[2.4.1 Access Controls on Root CA Repositories 15](#_Toc233004169)

[2.4.2 Access Controls on FSSP CA Repositories 16](#_Toc233004170)

[3.0 IDENTIFICATION AND AUTHENTICATION 17](#_Toc233004171)

[3.1 Naming 17](#_Toc233004172)

[3.1.1 Types of Names 17](#_Toc233004173)

[3.1.2 Need for Names to be Meaningful 22](#_Toc233004174)

[3.1.3 Anonymity or Pseudonymity of Subscribers 23](#_Toc233004175)

[3.1.4 Rules for Interpreting Various Name Forms 23](#_Toc233004176)

[3.1.5 Uniqueness of Names 23](#_Toc233004177)

[3.1.6 Recognition, Authentication, and Role of Trademarks 24](#_Toc233004178)

[3.2 Initial Identity Validation 24](#_Toc233004179)

[3.2.1 Method to Prove Possession of Private Key 24](#_Toc233004180)

[3.2.2 Authentication of Organization Identity 25](#_Toc233004181)

[3.2.3 Authentication of Individual Identity 25](#_Toc233004182)

[3.2.4 Non-verified Subscriber Information 27](#_Toc233004183)

[3.2.5 Validation of Authority 27](#_Toc233004184)

[3.2.6 Criteria for Interoperation 28](#_Toc233004185)

[3.3 Identification and Authentication for Re-Key Requests 28](#_Toc233004186)

[3.3.1 Identification and Authentication for Routine Re-key 28](#_Toc233004187)

[3.3.2 Identification and Authentication for Re-Key After Revocation 28](#_Toc233004188)

[3.3.3 Identification and Authentication for Certificate Recovery 29](#_Toc233004189)

[3.4 Identification and Authentication for Revocation Request 29](#_Toc233004190)

[3.4.1 Root CA 29](#_Toc233004191)

[3.4.2 FSSP CA 29](#_Toc233004192)

[4.0 OPERATIONAL REQUIREMENTS 31](#_Toc233004193)

[4.1 Certificate Application 31](#_Toc233004194)

[4.1.1 Who Can Submit a Certificate Application 32](#_Toc233004195)

[4.1.2 Enrollment Process and Responsibilities 33](#_Toc233004196)

[4.2 Certificate Application Processing 34](#_Toc233004197)

[4.2.1 Performing Identification and Authentication Functions 34](#_Toc233004198)

[4.2.2 Approval or Rejection of Certificate Applications 35](#_Toc233004199)

[4.2.3 Time to Process Certificate Applications 35](#_Toc233004200)

[4.3 Certificate Issuance 35](#_Toc233004201)

[4.3.1 CA Actions During Certificate Issuance 35](#_Toc233004202)

[4.3.2 Notification to Subscriber by the CA of Issuance of Certificate 36](#_Toc233004203)

[4.4 Certificate Acceptance 36](#_Toc233004204)

[4.4.1 Conduct Constituting Certificate Acceptance 37](#_Toc233004205)

[4.4.2 Publication of the Certificate by the CA 37](#_Toc233004206)

[4.4.3 Notification of Certificate Issuance by the CA to Other Entities 37](#_Toc233004207)

[4.5 Key Pair and Certificate Usage 37](#_Toc233004208)

[4.5.1 Subscriber Private Key and Certificate Usage 37](#_Toc233004209)

[4.5.2 Relying Party Public key and Certificate Usage 37](#_Toc233004210)

[4.6 Certificate Renewal 37](#_Toc233004211)

[4.6.1 Circumstance for Certificate Renewal 37](#_Toc233004212)

[4.6.2 Who May Request Renewal 38](#_Toc233004213)

[4.6.3 Processing Certificate Renewal Requests 38](#_Toc233004214)

[4.6.4 Notification of New Certificate Issuance to Subscriber 38](#_Toc233004215)

[4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 38](#_Toc233004216)

[4.6.6 Publication of the Renewal Certificate by the CA 38](#_Toc233004217)

[4.6.7 Notification of Certificate Issuance by the CA to Other Entities 38](#_Toc233004218)

[4.7 Certificate Re-key 38](#_Toc233004219)

[4.7.1 Circumstance for Certificate Re-key 39](#_Toc233004220)

[4.7.2 Who May Request Certification of a New Public Key 39](#_Toc233004221)

[4.7.3 Processing Certificate Re-keying Requests 39](#_Toc233004222)

[4.7.4 Notification of New Certificate Issuance to Subscriber 40](#_Toc233004223)

[4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate 40](#_Toc233004224)

[4.7.6 Publication of the Re-keyed Certificate by the CA 40](#_Toc233004225)

[4.7.7 Notification of Certificate Issuance by the CA to Other Entities 40](#_Toc233004226)

[4.8 Certificate Modification 40](#_Toc233004227)

[4.8.1 Circumstance for Certificate Modification 40](#_Toc233004228)

[4.8.2 Who May Request Certificate Modification 40](#_Toc233004229)

[4.8.3 Processing Certificate Modification Requests 40](#_Toc233004230)

[4.8.4 Notification of New Certificate Issuance to Subscriber 41](#_Toc233004231)

[4.8.5 Conduct Constituting Acceptance of Modified Certificate 41](#_Toc233004232)

[4.8.6 Publication of the Modified Certificate by the CA 41](#_Toc233004233)

[4.8.7 Notification of Certificate Issuance by the CA to Other Entities 41](#_Toc233004234)

[4.9 Certificate Revocation and Suspension 41](#_Toc233004235)

[4.9.1 Circumstances for Revocation 43](#_Toc233004236)

[4.9.2 Who Can Request a Revocation 44](#_Toc233004237)

[4.9.3 Procedure for Revocation Request 46](#_Toc233004238)

[4.9.4 Revocation Grace Period 48](#_Toc233004239)

[4.9.5 Time within which CA must Process the Revocation Request 48](#_Toc233004240)

[4.9.6 Revocation Checking Requirements for Relying Parties 49](#_Toc233004241)

[4.9.7 CRL Issuance Frequency 49](#_Toc233004242)

[4.9.8 Maximum Latency for CRLs 49](#_Toc233004243)

[4.9.9 Online Revocation/Status Checking Availability 50](#_Toc233004244)

[4.9.10 On-line Revocation Checking Requirements 50](#_Toc233004245)

[4.9.11 Other Forms of Revocation Advertisements Available 50](#_Toc233004246)

[4.9.12 Special Requirements Related To Key Compromise 50](#_Toc233004247)

[4.9.13 Circumstances for Suspension 50](#_Toc233004248)

[4.9.14 Who Can Request Suspension 51](#_Toc233004249)

[4.9.15 Procedure for Suspension Request 51](#_Toc233004250)

[4.9.16 Limits on Suspension Period 52](#_Toc233004251)

[4.10 CERTIFICATE STATUS SERVICES 52](#_Toc233004252)

[4.10.1 Operational Characteristics 52](#_Toc233004253)

[4.10.2 Service Availability 52](#_Toc233004254)

[4.10.3 Optional Features 52](#_Toc233004255)

[4.11 End of Subscription 52](#_Toc233004256)

[4.12 Key Escrow and Recovery 52](#_Toc233004257)

[4.12.1 Key Escrow and Recovery Policy and Practices 52](#_Toc233004258)

[4.12.2 Session Key Encapsulation and Recovery Policy and Practices 53](#_Toc233004259)

[4.12.3 Certificate Update 53](#_Toc233004260)

[5.0 Facility, Management, and Operational CONTROLS 55](#_Toc233004261)

[5.1 Physical Controls 55](#_Toc233004262)

[5.1.1 Site Location and Construction 55](#_Toc233004263)

[5.1.2 Physical Access 55](#_Toc233004264)

[5.1.3 Power and Air Conditioning 57](#_Toc233004265)

[5.1.4 Water Exposures 58](#_Toc233004266)

[5.1.5 Fire Prevention and Protection 58](#_Toc233004267)

[5.1.6 Media Storage 58](#_Toc233004268)

[5.1.7 Waste Disposal 59](#_Toc233004269)

[5.1.8 Off-Site Backup 59](#_Toc233004270)

[5.2 Procedural Controls 59](#_Toc233004271)

[5.2.1 Trusted Roles 59](#_Toc233004272)

[5.2.2 Number of Persons Required per Task 62](#_Toc233004273)

[5.2.3 Identification and Authentication for Each Role 63](#_Toc233004274)

[5.2.4 Roles Requiring Separation of Duties 63](#_Toc233004275)

[5.3 Personnel Controls 72](#_Toc233004276)

[5.3.1 Qualifications, Experience, and Clearance Requirements 72](#_Toc233004277)

[5.3.2 Background Check Procedures 73](#_Toc233004278)

[5.3.3 Training Requirements 74](#_Toc233004279)

[5.3.4 Retraining Frequency and Requirements 74](#_Toc233004280)

[5.3.5 Job Rotation Frequency and Sequence 74](#_Toc233004281)

[5.3.6 Sanctions for Unauthorized Actions 75](#_Toc233004282)

[5.3.7 Independent Contractor Requirements 75](#_Toc233004283)

[5.3.8 Documentation Supplied to Personnel 75](#_Toc233004284)

[5.4 Audit Logging Procedures 76](#_Toc233004285)

[5.4.1 Types of Events Recorded 76](#_Toc233004286)

[5.4.2 Frequency of Processing Log 79](#_Toc233004287)

[5.4.3 Retention Period for Audit Log 80](#_Toc233004288)

[5.4.4 Protection of Audit Log 80](#_Toc233004289)

[5.4.5 Audit Log Backup Procedures 80](#_Toc233004290)

[5.4.6 Audit Collection System (Internal vs. External) 81](#_Toc233004291)

[5.4.7 Notification to Event-Causing Subject 81](#_Toc233004292)

[5.4.8 Vulnerability Assessments 81](#_Toc233004293)

[5.5 Records Archival 81](#_Toc233004294)

[5.5.1 Types of Data Archived 81](#_Toc233004295)

[5.5.2 Retention Period for Archive 82](#_Toc233004296)

[5.5.3 Protection of Archive 83](#_Toc233004297)

[5.5.4 Archive Backup Procedures 83](#_Toc233004298)

[5.5.5 Requirement for Time-Stamping of Archive Records 83](#_Toc233004299)

[5.5.6 Archive Collection System (Internal and External) 83](#_Toc233004300)

[5.5.7 Procedures to Obtain and Verify Archive Information 83](#_Toc233004301)

[5.6 Key Changeover 84](#_Toc233004302)

[5.6.1 Root CA 84](#_Toc233004303)

[5.6.2 FSSP CA 85](#_Toc233004304)

[5.7 Compromise and Disaster Recovery 85](#_Toc233004305)

[5.7.1 Incident and Compromise Handling Procedures 86](#_Toc233004306)

[5.7.2 Computer Resources, Software, and/or Data are Corrupted 86](#_Toc233004307)

[5.7.3 Entity (CA) Private Key Compromise Procedures 87](#_Toc233004308)

[FSSP CA Subscriber Key Compromise 87](#_Toc233004309)

[5.7.4 Business Continuity Capabilities after a Disaster 89](#_Toc233004310)

[5.8 CA or RA Termination 89](#_Toc233004311)

[6.0 TECHNICAL SECURITY CONTROLS 91](#_Toc233004312)

[6.1 Key Pair Generation and Installation 91](#_Toc233004313)

[6.1.1 Key Pair Generation 91](#_Toc233004314)

[6.1.2 Private Key Delivery to Subscriber 92](#_Toc233004315)

[6.1.3 Public Key Delivery to Certificate Issuer 93](#_Toc233004316)

[6.1.4 CA Public Key Delivery to Relying Parties 94](#_Toc233004317)

[6.1.5 Key Sizes 97](#_Toc233004318)

[6.1.6 Public Key Parameters Generation and Quality Checking 97](#_Toc233004319)

[6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field) 97](#_Toc233004320)

[6.2 Private Key Protection and Cryptographic Module Engineering Controls 99](#_Toc233004321)

[6.2.1 Cryptographic Module Standards and Controls 99](#_Toc233004322)

[6.2.2 Private Key (n out of m) Multi-Person Control 99](#_Toc233004323)

[6.2.3 Private Key Escrow 100](#_Toc233004324)

[6.2.4 Private Key Backup 100](#_Toc233004325)

[6.2.5 Private Key Archival 102](#_Toc233004326)

[6.2.6 Private Key Transfer into or from a Cryptographic Module 102](#_Toc233004327)

[6.2.7 Private Key Storage on Cryptographic Module 102](#_Toc233004328)

[6.2.8 Method of Activating Private Key 103](#_Toc233004329)

[6.2.9 Method of Deactivating Private Key 103](#_Toc233004330)

[6.2.10 Method of Destroying Private Key 104](#_Toc233004331)

[6.2.11 Cryptographic Module Rating 104](#_Toc233004332)

[6.3 Other Aspects of Key Pair Management 104](#_Toc233004333)

[6.3.1 Public Key Archival 104](#_Toc233004334)

[6.3.2 Certificate Operational Periods and Key Usage Periods 104](#_Toc233004335)

[6.4 Activation Data 105](#_Toc233004336)

[6.4.1 Activation Data Generation and Installation 105](#_Toc233004337)

[6.4.2 Activation Data Protection 105](#_Toc233004338)

[6.4.3 Other Aspects of Activation Data 106](#_Toc233004339)

[6.5 Computer Security Controls 107](#_Toc233004340)

[6.5.1 Specific Computer Security Technical Requirements 107](#_Toc233004341)

[6.5.2 Computer Security Rating 108](#_Toc233004342)

[6.6 Lifecycle Technical Controls 108](#_Toc233004343)

[6.6.1 System Development Controls 108](#_Toc233004344)

[6.6.2 Security Management Controls 110](#_Toc233004345)

[6.6.3 Life Cycle Security Controls 111](#_Toc233004346)

[6.7 Network Security Controls 111](#_Toc233004347)

[6.7.1 Federal Root CA 112](#_Toc233004348)

[6.7.2 FSSP CA 112](#_Toc233004349)

[6.8 Time-Stamping 112](#_Toc233004350)

[7.0 CERTIFICATE, CRL, AND OCSP PROFILES 113](#_Toc233004351)

[7.1 Certificate Profile 113](#_Toc233004352)

[The Federal Root CA and FSSP CA issue X.509 version 3 certificates, all of which include the following fields: 113](#_Toc233004353)

[7.1.1 Version Numbers 113](#_Toc233004354)

[7.1.2 Certificate Extensions 113](#_Toc233004355)

[7.1.3 Algorithm Object Identifiers 116](#_Toc233004356)

[7.1.4 Name Forms 116](#_Toc233004357)

[7.1.5 Name Constraints 117](#_Toc233004358)

[7.1.6 Certificate Policy Object Identifier 117](#_Toc233004359)

[7.1.7 Usage of Policy Constraints Extension 117](#_Toc233004360)

[7.1.8 Policy Qualifiers Syntax and Semantics 117](#_Toc233004361)

[7.1.9 Processing Semantics for the Critical Certificate Policy Extension 117](#_Toc233004362)

[7.2 CRL Profile 117](#_Toc233004363)

[The CAs will issue *partitioned CRLs* that will contain a subset of all end entity certificate revocations, and will contain the following additional information: 118](#_Toc233004364)

[7.2.1 Version Numbers 118](#_Toc233004365)

[7.2.2 CRL and CRL Entry Extensions 118](#_Toc233004366)

[7.3 OCSP Profile 118](#_Toc233004367)

[7.3.1 Version Number(s) 119](#_Toc233004368)

[7.3.2 OCSP Extensions 119](#_Toc233004369)

[8.0 Compliance Audit AND OTHER ASSESSMENTS 120](#_Toc233004370)

[8.1 Frequency or Circumstances of Assessment 120](#_Toc233004371)

[8.2 Identity/Qualifications of Compliance Assessor 120](#_Toc233004372)

[8.3 Assessor’s Relationship to Assessed Entity 120](#_Toc233004373)

[8.4 Topics Covered by Assessment 121](#_Toc233004374)

[8.5 Actions Taken as a Result of Deficiency 121](#_Toc233004375)

[8.6 Communications of Results 123](#_Toc233004376)

[9.0 OTHER BUSINESS AND LEGAL MATTERs 124](#_Toc233004377)

[9.1 Fees 124](#_Toc233004378)

[9.1.1 Certificate Issuance or Renewal Fees 124](#_Toc233004379)

[9.1.2 Certificate Access Fees 124](#_Toc233004380)

[9.1.3 Revocation or Status Information Access Fees 124](#_Toc233004381)

[9.1.4 Fees for Other Services Such as Policy Information 124](#_Toc233004382)

[9.1.5 Refund Policy 124](#_Toc233004383)

[9.2 Financial Responsibility 124](#_Toc233004384)

[9.2.1 Insurance Coverage 124](#_Toc233004385)

[9.2.2 Other Assets 124](#_Toc233004386)

[9.2.3 Insurance or Warranty Coverage for End-Entities 124](#_Toc233004387)

[9.3 Confidentiality of Business Information 124](#_Toc233004388)

[9.3.1 Scope of Confidential Information 125](#_Toc233004389)

[9.3.2 Information not within the Scope of Confidential Information 125](#_Toc233004390)

[9.3.3 Responsibilities to Protect Confidential Information 125](#_Toc233004391)

[9.4 Privacy of Personal Information 125](#_Toc233004392)

[9.4.1 Privacy Plan 125](#_Toc233004393)

[9.4.2 Information Treated as Private 125](#_Toc233004394)

[9.4.3 Information not Deemed Private 126](#_Toc233004395)

[9.4.4 Responsibilities to Protect Private Information 126](#_Toc233004396)

[9.4.5 Notice and Consent to Use Private Information 126](#_Toc233004397)

[9.4.6 Disclosure Pursuant to Judicial or Administrative Process 126](#_Toc233004398)

[9.4.7 Other Information Disclosure 127](#_Toc233004399)

[9.5 Intellectual Property Rights 127](#_Toc233004400)

[9.6 Representations and Warranties 128](#_Toc233004401)

[9.6.1 CA Representations and Warranties 128](#_Toc233004402)

[9.6.2 RA Representations and Warranties 128](#_Toc233004403)

[9.6.3 Subscriber Representations and Warranties 129](#_Toc233004404)

[9.6.4 Relying Parties Representations and Warranties 129](#_Toc233004405)

[9.6.5 Representations and Warranties of Other Participants 129](#_Toc233004406)

[9.7 DISCLAIMERS OF WARRANTIES 129](#_Toc233004407)

[9.8 LIMITATIONS OF LIABILITY 129](#_Toc233004408)

[9.9 INDEMNITIES 129](#_Toc233004409)

[9.10 TERM AND TERMINATION 129](#_Toc233004410)

[9.10.1 Term 129](#_Toc233004411)

[9.10.2 Termination 130](#_Toc233004412)

[9.10.3 Effect of Termination and Survival 130](#_Toc233004413)

[9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 130](#_Toc233004414)

[9.12 AMENDMENTS 130](#_Toc233004415)

[9.12.1 Procedure for Amendment 130](#_Toc233004416)

[9.12.2 Notification Mechanism and Period 130](#_Toc233004417)

[9.12.3 Circumstances under which OID must be Changed 130](#_Toc233004418)

[9.13 DISPUTE RESOLUTION PROVISIONS 131](#_Toc233004419)

[9.14 GOVERNING LAW 131](#_Toc233004420)

[9.15 COMPLIANCE WITH APPLICABLE LAW 131](#_Toc233004421)

[9.16 MISCELLANEOUS PROVISIONS 131](#_Toc233004422)

[9.16.1 Entire Agreement 131](#_Toc233004423)

[9.16.2 Assignment 131](#_Toc233004424)

[9.16.3 Severability 131](#_Toc233004425)

[9.16.4 Enforcement (Attorneys’ Fees and Waiver of Rights) 131](#_Toc233004426)

[9.16.5 Force Majeure 131](#_Toc233004427)

[9.17 OTHER PROVISIONS 132](#_Toc233004428)

[9.17.1 Waivers 132](#_Toc233004429)

[Appendix B: DElegated Registration Authorities 134](#_Toc233004430)

EXHIBITS

Exhibit 1: Acceptable Identification Credentials 26

Exhibit 2: Revocation Reasons 44

Exhibit 3a: Federal Root CA Authorized Revocation Requestors and Approvers 44

Exhibit 3b: FSSP CA Authorized Revocation Requestors and Approvers ……45

Exhibit 4a: Federal Root CA Trusted Roles and Assigned Privileges.………………………….64

Exhibit 4b: FSSP CA Trusted Roles and Assigned Privileges.…………………………………68

Exhibit 5: Recorded Audit Events 76

Exhibit 6: Retained Archive Records 81

# IDENTIFICATION AND AUTHENTICATION

The EMS PKI employs a delegated registration model. In this model, certain individuals filling Trusted Roles (SOMUs, and Registration Authorities) are employees of, or contractors for, Entrust. These individuals are responsible for the operation and maintenance of the various Certificate Authorities that make up the EMS PKI.

In addition, for the FSSP CA, the Registration Authorities are responsible for performing the identification and authentication for Local Registration Authority for the EMS PKI subscribers. In addition to those individuals filling Trusted Roles, the EMS PKI relies on Local Registration Authorities to perform the identification and authentication for their Subscribers.

This section contains the practices to be followed in identifying and authenticating the SOMUs and Registration Authorities who are responsible for the operation and maintenance of the Federal Root CA. Additional practices are defined for identification and authentication of subordinate CAs and cross-certified CAs.

This section also contains practices to be followed in performing the identification and authentication for all subscribers to the EMS PKI Federal Shared Service Provider CA.

Note: for the FSSP CA, delegated RAs are used to register end user subscribers. The organizations serving as the delegated RAs are listed in Appendix B.

## Naming

### Types of Names

#### Types of Names for the Root CA

The Federal Root CA uses the X.501 DNs for all Subscribers. The DN will consist of a geo-political name consisting of naming elements C, O, OU, and CN as follows:

* **For Trusted Role Users (SOMU, SCO, & RA)** (see Section 5.2.1) – [Note: these certificates will not assert any of the *policy OIDs defined in the Common Policy*. These Subscribers are Entrust employees or contractors and will be responsible for administrative operations of the Federal Root CA.]:

RDN = CN (+ Optional serialNumber: where CN = [Subscriber first and last name] and optional serialNumber = [Entrust employee number]

OU = [Administrators]

O = [Entrust]

C = [US]

Example1:

*subject::=* cn=John Smith, ou=Administrators, o=Entrust, c=US

Example2:

*subject::=* cn=John Smith + serialNumber=2EJAS01, ou=Administrators, o=Entrust, c=US

The Federal Root CA will not be issuing certificates to federal government departments

* For certificates issued to Entrust Federal Shared Service Provider CA:

OU = [Entrust Managed Services SSP CA]

OU = [Certification Authorities]

O = [Entrust]

C = [US]

* For certificates issued to Federal department subordinate CAs:

OU = [*CA Name*]

OU = [Certification Authorities]

OU = [*Department Name*]

O = [U.S. Government]

C = [US]

* For certificates issued to CSS Servers:

OU = [*CSS Server Name*]

OU = [Administrators]

O = [Entrust]

C = [US]

* For certificates issued to cross-certified CAs:
* As agreed by the EMS PMA

Certificates issued by the Federal Root CA may contain a Subscriber alternate name form in the subjectAltName field. For human Subscribers, the Subscriber alternate name will be the rfc822 e-mail address. For subordinate and cross-certified CAs, the alternate name will be the rfc822 e-mail address for the OA responsible for the CA. If the subjectAltName extension is asserted, it must be marked as non-critical.

CRL distribution points are named with the commonName attribute with a value generated by the CA application and are named subordinate to the Federal Root CA.

#### Types of Names for the FSSP CA

The FSSP CA uses the X.501 DNs for all Subscribers, including those issued under entrust-emspkica-policy-emscp, id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-devices, id-fpki-common-cardAuth and id-fpki-common-authentication.

The DN will consist of a geo-political name consisting of naming elements C, O, OU, and CN as follows:

* **For Trusted Role Users (SO, SCO, & RA)** (see Section 5.2.1) – [Note: these certificates will not assert any of the policy OIDs defined in the Common Policy. These Subscribers are Entrust employees or contractors and will be responsible for administrative operations of the FSSP CA, including management of customer LRAs.]:

RDN = CN (+ optional serialNumber): where CN = [Subscriber first and last name] and optional serialNumber = [Entrust employee number]

OU = [Administrators]

O = [Entrust]

C = [US]

Example1:

*subject::=* cn=John Smith, ou=Administrators, o=Entrust, c=US

Example2:

*subject::=* cn=John Smith + serialNumber=2EJAS01, ou=Administrators, o=Entrust, c=US

* **For certificates issued to CSS Servers:**

CN = [*CSS Server Name*]

OU = [Administrators]

O = [Entrust]

C = [US]

Customers subscribing to the FSSP CA will have their own Local Registration Authorities and End-Entity Subscribers. The End-Entity Subscriber certificates may assert any of the following: id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-devices, id-fpki-common-cardAuth and id-fpki-common-authentication.

All distinguished names assigned to FSSP Subscribers (except for those SOMUs and Registration Authorities as noted above) are placed under the “c=US, o=U.S. Government” branch of the directory information tree.

The organizational units *department* and *agency* appear when applicable and are used to specify the federal entity that employs the subscriber. At least one of these organizational units appears in the DN. As a result, agency is labeled as being Optional. The additional organizational unit *structural\_container* is permitted to support local directory requirements, such as differentiation between human subscribers and devices. This organizational unit may not be employed to further differentiate between subcomponents within an agency.

* **For customer Local Registration Authorities** (see Section 5.2.1) – [Note: Where applicable, these Subscribers will be issued a secure USB token containing their LRA credentials; which are different than their PIV credentials. As an option, LRAs may use a smartcard to store their LRA credentials, pending the approval from the EMS PKI OA.]:

CN = [Subscriber first name middle initial and last name]

OU = [*Structural Container*] – Optional

OU = [*Agency Name*] – Optional

OU = [*Department Name*] – represents the federal entity that employs the Subscriber.

O = [U.S. Government]

C = [US]

Note: The text “LRA” is included in the Role field.

Example:

*subject::=* cn=John A. Smith, ou=Administrators, ou=[*Department Name*], o=U.S. Government, c=US

In most instances, the customer’s Card Management System (CMS) application serves as the LRA responsible for instructing the CA to issue and manage certificates, and as such, will have certificates issued to the application rather than an individual. These certificates do not assert any of the id-fpki policy OIDs. In addition, these certificates do not specify a subjectAltName.

CN = [*CMS Server Name*]

OU = [Infrastructure] (structural\_container)

OU = [*Agency Name*] – Optional

OU = [*Department Name*]

O = [U.S. Government]

C = [US]

Example:

*subject::=* cn=cms1-001-gsa.gov, ou=infrastructure, ou=gsa, o=u.s. government, c=us

**For customer Subscribers**- [Note: These are all Subscribers except for the SOMUs, Registration Authorities and Local Registration Authorities as noted above. These Subscribers may be issued certificates under id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-devices, id-fpki-common-cardAuth and id-fpki-common-authentication.]:

* For federal employee human Subscribers who are issued certificates under id-fpki-common-authentication, the distinguished name takes the form of the following:

CN = [Any one of the following name forms are used: “nickname lastname”, “firstname initial. lastname”, “firstname middlename lastname”] – [Note: nickname may be the subscriber’s first name, a form of the first name, middle name, or pseudonym (e.g., Buck) by which the subscriber is generally known.]

OU = [*structural\_ container*] – Optional

OU = [*Agency Name*] – Optional

OU = [*Department Name*]

O = [U.S. Government]

C = [US]

In order to ensure name uniqueness across the domain name space, the certificate subject may contain a multi-value relative distinguished name (RDN) consisting of the common name (cn) plus either a userId or serialNumber. For example:

*subject::=*  uid=123456 + cn=John Q. Doe, ou=[*Department Name*],o=U.S. Government, c=US

Certificates issued under id-fpki-common-authentication include a subject alternative name. At a minimum, the subject alternative name extension includes the pivFASC-N name type [FIPS 201-1]. The value for this name is the FASC-N [PACS] of the subject’s PIV card.

Example:

*subject::=* cn=John Q. Doe, ou=[*Department Name*], o=U.S. Government, c=US

*subjectAltName::=* [pivFASC-N encoded as a 25 byte binary value]; may also include rfc822 email address or other legacy name form.

* For federal employee human Subscribers who are issued certificates under id-fpki-common-cardAuth:

serialNumber = [FASC-N] – encoded as 50 bytes of ASCII HEX

OU = [*Structural Container*] – Optional

OU = [*Agency Name*] – Optional

OU = [*Department Name*]

O = [U.S. Government]

C = [US]

Certificates issued under id-fpki-common-cardAuth will include a subject alternative name extension that includes the pivFASC-N name type. The value for this name will be the FASC-N of the subject’s PIV card. Certificates issued under id-fpki-common-cardAuth will not include any other name in the subject alternative name extension but may include a non-NULL name in the subject field.

Example:

*subject::=* serialNumber= 3019D421085908422D9CE739CD896AD9AD6B5AD6B5ADE08421, ou=[*Department Name*], o=U.S. Government, c=US

*subjectAltName::=* [pivFASC-N encoded as a 25 byte binary value]

* For federal employee human Subscribers who are issued certificates under id-fpki-common-policy or id-fpki-common-hardware:

CN = [Any one of the following name forms may be used: “nickname lastname”, “firstname initial. lastname”, “firstname middlename lastname”] – [Note: nickname may be the subscriber’s first name, a form of the first name, middle name, or pseudonym (e.g., Buck) by which the subscriber is generally known.]

OU = [*Structural Container*] – Optional

OU = [*Agency Name*] – Optional

OU= [*Department Name*]

O = [U.S. Government]

C = [US]

Example:

*subject::=* cn=John Q. Doe, ou=[*Department Name*], o=U.S. Government, c=US

*subjectAltName::=* rfc822 email address or other legacy name form.

In order to ensure name uniqueness across the domain name space, the certificate subject may contain a multi-value relative distinguished name (RDN) consisting of the common name (cn) plus either a userId or serialNumber. For example:

*subject::=*  uid=123456 + cn=John Q. Doe, ou=[*Department Name*],o=U.S. Government, c=US

Distinguished names assigned to federal contractors and other affiliated persons are within the same directory information tree. For federal contractors and affiliated human Subscribers, the name forms will follow as noted above for each of the policies with the exception that the *commonName* field will include the text “(affiliate)” as applicable.

* For device Subscriber certificates issued under id-fpki-common-device:

RDN= [CN]; where CN= a descriptive value for the component

OU = [*Structural Container*] – Optional

OU = [*Agency Name*] – Optional

OU= [*Department Name*]

O = [U.S. Government]

C = [US]

Example:

*subject::=* cn=Cisco ASA, ou=[*Department Name*], o=U.S. Government, c=US

CRL distribution points are named with the commonName attribute with a value generated by the CA application and are named subordinate to the FSSP CA.

### Need for Names to be Meaningful

#### Need for Root CA Names to be Meaningful

The subscriber certificates issued pursuant to this CPS are meaningful. The names that appear in the certificates are understandable and useable by relying parties. The names used in the certificates identify the subscriber of the certificate in a meaningful way (Refer to section 3.1.1).

The common name in the DN represents the subscriber in a way that is easily understandable for humans. For people, this will typically be a legal name, so the preferred common name form is:

cn=*firstname initial. lastname*

Example: cn=John Q. Doe

* For certificates issued to the Entrust Managed Services Root CA:

*subject::=* ou=Entrust Managed Services Federal Root CA, ou=Certification Authorities, o=Entrust, c=US

*issuer::=* ou=Entrust Managed Services Federal Root CA, ou=Certification Authorities, o=Entrust, c=US

* For certificates issued to Entrust Federal Shared Service Provider CA:

*subject::=* ou=Entrust Managed Services SSP CA, ou=Certification Authorities, o=Entrust, c=US

*issuer::=* ou=Entrust Managed Services Federal Root CA, ou=Certification Authorities, o=Entrust, c=US

* For certificates issued to Federal department subordinate CAs:

*subject::=* ou=*CA Name*, ou=Certification Authorities, ou=*Department Name,* o= U.S. Government, c=US

*issuer::=* ou=Entrust Managed Services Federal Root CA, ou=Certification Authorities, o=Entrust, c=US

The subject name as specified in the Federal Root CA certificate matches the issuer name in certificates issued by the Federal Root CA, as required by RFC 3280/5280.

#### Need for FSSP CA Names to be Meaningful

The subscriber certificates issued pursuant to this CPS are meaningful. The names that appear in the certificates are understandable and useable by relying parties. The names used in the certificates identify the subscriber of the certificate in a meaningful way (Refer to section 3.1.1).

The common name in the DN represents the subscriber in a way that is easily understandable for humans. For people, this will typically be a legal name, so the preferred common name form is:

cn=*firstname initial. lastname*

Example: cn=John Q. Doe

For the FSSP CA:

*subject::=* ou=Entrust Managed Services SSP CA, ou=Certification Authorities, o=Entrust, c=US

*issuer::=* ou=Entrust Managed Services Root CA, ou=Certification Authorities, o=Entrust, c=US

For all certificates issued by the FSSP CA:

*issuer::=* ou=Entrust Managed Services SSP CA, ou=Certification Authorities, o=Entrust, c=US

The subject name as specified in the FSSP CA certificate matches the issuer name in certificates issued by the FSSP CA, as required by RFC 3280/5280.

### Anonymity or Pseudonymity of Subscribers

The Federal Root CA does not issue anonymous certificates. Pseudonymous certificates may be issued by the Federal Root CA to support internal operations. As noted in Section 3.1.2, the CA does not issue anonymous certificates to CAs.

The FSSP CA does not issue anonymous certificates. Pseudonymous certificates may be issued by the FSSP CA to support internal operations. As noted in Section 3.1.2, the CA does not issue anonymous certificates to CAs.

### Rules for Interpreting Various Name Forms

As described in Section 3.1.1, the EMS PKI only uses the DN name form as the certificate subject where applicable. This name form is interpreted in accordance with the applicable ISO and Internet standards (i.e. X.501, RFC 2882, PACS), as defined in the certificate profile.

### Uniqueness of Names

Name uniqueness for certificates issued by the Federal Root CA is enforced as described in section 3.1.1. The Federal Root CA and its associated RAs enforce name uniqueness within the X.500 name space. When other name forms are used, they too are allocated such that name uniqueness is ensured for certificates issued by the Federal Root CA.

Variations in the cn and serialNumber are used to ensure name uniqueness. The directory is managed in such a way as to ensure that no two individuals are assigned the same DN and, therefore, the same electronic identity.

Name uniqueness for certificates issued by the FSSP CA is enforced. The FSSP CA and its associated RAs enforce name uniqueness within the X.500 name space. When other name forms are used, they too are allocated such that name uniqueness is ensured for certificates issued by the FSSP CA.

Names are unambiguously defined as set forth in Section 3.1.1. Variations in the cn and serialNumber or uid will be used to ensure name uniqueness.

The directory is managed in such a way as to ensure that no two individuals are assigned the same DN and, therefore, the same electronic identity.

### Recognition, Authentication, and Role of Trademarks

The Federal Root CA only issues certificates to the EMS PKI Federal SubCA, EMS PKI Trusted Roles and the EMS PKI OCSP server. As such, it is not likely that there will be any name or trademark conflict disputes; however, should any arise, such disputes will be passed on to the FPKIPA for resolution.

For the FSSP CA, subscriber registration is under the auspices of the delegated RAs listed in Appendix B. As such, it is the responsibility of the contractors operating the delegated RAs registration processes to pass any disputes arising from a name or trademark conflict on to the FPKIPA for resolution.

## Initial Identity Validation

### Method to Prove Possession of Private Key

In all cases where the party named in a certificate generates its own keys, that party is required to prove possession of the private key, which corresponds to the public key in the certificate request. Proof of possession of a private key is handled automatically by the Federal Root CA or FSSP CA to Subscriber with messages protected by PKIX-Certificate Management Protocol (CMP). Refer to Section 3.2.3 for details concerning Identification and Authentication of Federal Root CA and FSSP CA subscribers and to Section 4.1 for more information regarding the Subscriber application process, including distribution of shared secrets and PIV card.

For the Subscriber’s signature private key, a PKIX-CMP operation initiated by the Subscriber is digitally signed using the signature private key itself.

In the case where key generation is performed under the CA or RA’s direct control, proof of possession is not required. For the Subscriber’s decryption private key, both the public and private keys are generated by the Federal Root CA or the FSSP CA. A PKIX-CMP operation transfers the private key to the Subscriber, together with the corresponding certificate, using digitally signed data from the Federal Root CA or FSSP CA to provide integrity during the transport.

In the case of cross-certificates, the PKIX-CMP initiated by the subject CA, provides the proof of possession.

### Authentication of Organization Identity

The Federal Root CA will not be issuing organization certificates (certificates in which the Subject of the certificate represents an organization, or group, rather than a specific individual), except to other subordinate CAs. The certificates issued by the Federal Root CA to other CAs will be issued according to the requirements defined in the CP and this CPS. All certificate requests for other CAs will include identity information of the requesting representative which will be forwarded to the EMS PMA for approval.

The FSSP CA does not issue CA certificates, including cross-certified CA certificates or subordinate CA certificates.

### Authentication of Individual Identity

This practice statement allows a certificate to be issued only to a single entity. Certificates are not issued that contain a public key whose associated private key is shared.

#### Authentication of Human Subscribers

Procedures used by agencies to issue identification to their own personnel and affiliates may be more stringent than that set forth below (in Sections 3.2.3.1.1, 3.2.3.1.2, and 3.2.3.1.3) for EMS PKI Trusted Roles, including customer LRAs. The registration process for Federal employees and Federal contractors is under the auspices of (and documented by) the delegated RAs listed in Appendix B.

During an in-person proofing process, all individuals filling Trusted Roles for the Federal Root CA or FSSP CA complete and sign an Entrust Shared Service Provider Subscriber Agreement and present valid identification credentials as follows:

* One of the Photo IDs listed in the Column A of Exhibit 1,
* Or Two of the forms of ID -- one of the Government Photo IDs listed in the second column (Column B) of Exhibit 1 plus one of the Government IDs listed in the third column (Column C) of Exhibit 1.

Regardless of which Identification Credentials are presented, the Authority conducting the in-person identity verification will perform verification of all presented credentials. NOTE: The Entrust CA software is configured so that user activation codes expire after 14 days.

Where applicant is applying directly to the EMS team, the individual performing the identity verification verifies the identity credentials presented by the Applicant by performing a reasonable visual inspection of the original credentials: compare the photograph on the credentials to the applicant, check dates, look for holograms, use a UV Security Light to view security images that react to UV light, and look for appearance of obvious tampering.

Exhibit : Acceptable Identification Credentials

|  |  |
| --- | --- |
| Photo ID (Select Only One)Column A | Government IDs (-or- Select one from each column B and C) |
| Column B | Column C |
| Federal Government photo ID | State-issued driver’s license | US social security card issued by the Social Security Administration |
| Entrust / CygnaCom employee photo ID  | State-issued photo identification card | Original or certified copy of birth certificate issued by a state, municipal or county agency and bearing an official seal |
| US Passport (unexpired or expired) |  |  |
| Certificate of US Citizenship |
| Certificate of Naturalization |
| US Military ID card |

##### Security Officer / Master Users (SOMUs)

.

##### Registration Authorities and Security Compliance Officer

.

##### Local Registration Authorities

In the EMS PKI, the department/agency’s CMS fills the role of the Local Registration Authority, which acts as the PIV Issuer, as defined by FIPS 201. Each CMS is issued a certificate by the FSSP CA. The contracting officer, or his/her delegate, is responsible for requesting the CMS certificates from the EMS PKI Registration Authority via written or electronic communication.

In addition to the LRA, each department/agency may use Trusted Agents, also referred to as Enrollment Officers, who are responsible for performing the identification and authentication of the Subscribers. The contracting officer, or his/her delegate, is responsible for requesting certificates, or authorizing the TA to request certificates, from EMS PKI RA via written or electronic communication.

EMS PKI customers are responsible for providing a detailed registration plan and supporting documentation to the EMS PKI PMA, OA, or SCO for review to ensure that the customer’s plan satisfies the requirements of the Common Policy.

##### End User Subscribers

Similar to LRAs and Trusted Agents, FSSP CA end user Subscribers will enroll in person with the appropriate PIV Registrar for their department/agency. EMS PKI customers are responsible for providing a detailed registration plan and supporting documentation to the EMS PKI PMA, OA, or SCO for review to ensure that the customer’s plan satisfies the requirements of the Common Policy.

#### Authentication of Devices

In order to have a certificate issued by the FSSP CA to a component or a server identity, a human sponsor is required. The human sponsor assumes accountability and responsibility for the component or server device. The customer may submit a request to the EMS team or customers may also have LRAs that may use the Federal Admin Services portal to request device certificates. Regardless, the customer is responsible for designating a human sponsor for the devices

### Non-verified Subscriber Information

Information that is not verified will not be included in certificates.

### Validation of Authority

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

The EMS PKI RA and SO require all requests to come from an authorized requestor. The customer’s contracting officer provides EMS PKI with a list of authorized requestors. Any requests that are received from non-authorized requestors are returned to the requestor with a copy to the contracting officer.

### Criteria for Interoperation

The FPKIPA will determine the interoperability criteria for CAs operating under this policy.

No stipulation for the FSSP CA.

## Identification and Authentication for Re-Key Requests

### Identification and Authentication for Routine Re-key

#### Root CA

.

#### FSSP CA

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

Certificates are not issued under the id-fpki-common-High policy.

For Trusted Role subscribers, their identity may be established through use of current signature key, except that identity shall be re-established through an in-person registration process at least once every three (3) years from the time of initial registration.

For policies other than id-fpki-common-High, an End User subscriber’s identity may be established through use of current signature key, except that identity shall be re-established through an in-person registration process at least once every nine (9) years from the time of initial registration.

Refer to Section 4.7 Certificate Re-key (and it sub sections) for a description of the FSSP CA certificate re-key process.

### Identification and Authentication for Re-Key After Revocation

All Federal Root CA and FSSP CA subscribers will repeat the initial certificate registration and request process in order to obtain a new certificate after a revocation.

### Identification and Authentication for Certificate Recovery

Certificate recovery means re-issuing an existing, non-expired certificate. The re-issued certificate has the same characteristics as the original issued certificate. Certificate recovery is typically required when a Subscriber no longer has access to the private key material due to a lost smartcards or tokens or corrupted software-based profiles.

All Federal Root CA or FSSP CA Subscribers requiring certificate recovery are required to satisfy the authentication requirements defined in Section 3.2.3 above. The Subscriber completes a new Subscriber Agreement, and marks the appropriate selection indicating Certificate Recovery.

## Identification and Authentication for Revocation Request

Revocation requests will 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.

### Root CA

.

### FSSP CA

Requests from an SOMU, RA, or LRA to the FSSP CA to revoke a FSSP CA Subscriber’s certificate require Entrust Administrator privilege credentials be supplied at login to the Entrust Security Manager Administration or web-based User Administration portal application before revocation requests can be serviced by the FSSP CA.

Revocation requests can be made by a FSSP CA Subscriber or another person authorized to request revocation of the Subscriber’s certificates, with or without the Subscriber’s advanced notice or approval. All certificate revocation requests are communicated to an SOMU, RA, or LRA via secure means, either electronically or in person.

An SOMU, RA, or LRA may process a revocation request from a FSSP CA Subscriber, based on an email revocation request that has been digitally signed by the Subscriber.

An SOMU, RA, or LRA may process a revocation request based on a digitally signed email from an individual authorized to request revocation on behalf of the Subscriber (see Section 4.9.2.1). In this case, the SOMU, RA or LRA will verify the authority of the requestor to submit the revocation request by validating the digital signature against an authoritative source. Alternatively, the revocation request may be processed through a delegated RA using a card management system (CMS), or an LRA may access the Federal Admin Services portal to process the request. In all cases the identity of the requestor is authenticated using credentials issued by the SSP CA.

An SOMU, RA or LRA may process an in-person revocation request from a Subscriber, following authentication as outlined in Section 3.2.3.

# OPERATIONAL REQUIREMENTS

## Certificate Application

.

**FSSP CA**

The Certificate application process provides sufficient information to:

* Establish the applicant’s authorization (by the employing or sponsoring agency) to obtain a certificate. (per section 3.2.3)
* Establish and record identity of the applicant. (per section 3.2.3)
* Obtain the applicant’s public key and verify the applicant’s possession of the private key for each certificate required. (per section 3.2.1)
* Verify any role or authorization information requested for inclusion in the certificate.

With regard to Federal Employee and Federal Contractor subscribers, the registration processes are operated and maintain by the delegated RAs listed in Appendix B. It is their responsibility to ensure that the subscribers present themselves in person to the appropriate Registrar and provide the required identification, as specified in Section 3.2.3 above.

All SOMUs (except the First Officer), Registration Authorities and Local Registration Authorities use either smartcards or other hardware tokens for generation and storage of their private keys. The Registrar performing the enrollment issues the smartcard or token during the registration process.

Should an application for certificate issuance include any role or authorization information to be included in the certificate, the Registrar verifies the information against official department/agency records prior to certificate issuance.

Details concerning the certificate issuance process are found in Section 4.3.

### Who Can Submit a Certificate Application

#### CA Certificates

.

##### Cross-Certification Certificate Application

.

##### Subordinate CA Certificate Application

Subordinate CA certificates are requested by the EMS OA in writing (digitally signed email is acceptable) to the EMS PMA. The EMS OA then develops a CPS for the subordinate CA.

The EMS PMA may approve or deny the request and notifies the EMS OA of the decision. If the request is approved, the EMS PMA then authorizes the issuance of the certificate to the subordinate CA via a digitally signed email to the EMS OA.

As required by the Common Policy CP, certificate issuance to a Subordinate CA requires that a functioning public/private key pair for the requested certificate, as well as proof of possession of the private key be provided by the EMS OA. The EMS OA will use the PKIX-CMP protocol to secure the communication between the Subordinate CA and the Federal Root CA. Proof of possession of the private key is a function of the CA software as required by PKIX-CMP.

#### User Certificates

Prior to certificate issuance, Human Subscribers (Trusted Role Personnel) present themselves in-person to an existing Federal Root CA SOMU (acting as the Registrar) and provide the required identification, as specified in Section 3.2 (and subsections). The SOMU performing the identity verification will validate that the applicant is authorized by retrieving a list signed by the PMA (may be wet signature or digitally signed) of “authorized Federal Root CA subscribers” and verifying that the applicant is identified on this list.

The SOMU (registrar) performing the verification will then record the type of identification used by the applicant and the unique number assigned to the identification by the issuing authority (ex: Driver’s license number, Passport number, etc.). As required by the CP, these trusted role applicant/subscribers use hardware tokens validated to at least FIPS 140 Level 2 for generation and storage of their cryptographic materials. The applicant then indicates acceptance of the token and shared secret data in a signed acceptance document; which requires their handwritten signature.

The applicant/subscriber will be provided with a reference number and authorization code, both of which are required to complete the issuance process.

If the Subscriber does not complete the certificate issuance process within the allowable 30-day window, the Subscriber will have to repeat the initial application.

The EMS OA keeps a copy of all completed Subscriber Agreements for Trusted Role personnel.

Details concerning the certificate issuance process are found in Section 4.3.

For the FSSP CA, an application for a user (subscriber) certificate is submitted by either the applicant or a trusted agent. See Section 3.2.3.1, above, for more detailed information regarding subscriber registration.

#### Device Certificates

The Federal Root CA does not issue certificates to Components or Servers, with the exception of OCSP servers.

For the FSSP CA, an application for a device certificate is submitted by the human sponsor of the device. See section 3.2.3.2 for more detailed information regarding this process.

### Enrollment Process and Responsibilities

All communications among EMS PKI Authorities (e.g., CA or RA) supporting the certificate application and issuance process are authenticated and protected from modification using the Public Key Infrastructure (X.509) - Certificate Management Protocol (PKIX-CMP) protocol (refer to Section 3.2.1 for additional information about PKIX-CMP); as such, any electronic transmission of shared secrets are protected. Furthermore, since PKIX-CMP is used, electronic communication between the customer enrollment environments and the EMS PKI are encrypted and digitally signed. In addition, secure communication capabilities are provided by hardware-based virtual private networking. The VPN uses Triple DES with 168-bit keys. Any out-of-band electronic communications that contain shared secrets are encrypted and digitally signed to maintain the confidentiality and integrity of the message contents.

## Certificate Application Processing

Information in certificate applications is verified as accurate before certificates are issued. The EMS PMA specifies procedures to verify information in certificate applications. The procedures followed are described in detail in section 3.2.3.1 of this CPS. The Acceptable forms of identification are detailed in Exhibit 1.

### Performing Identification and Authentication Functions

The identification and authentication of the subscriber meets the requirements specified for subscriber authentication as specified in sections 3.2.1 – 3.2.3 and 3.3 of this CPS. Section 3.2.3 and subsections therein (3.2.3.1, 3.2.3.1.1-3.2.3.1.4) of this CPS identifies the components of the EMS PMA (e.g., CA or RA) that are responsible for authenticating the subscriber’s identity in each case.

#### Cross-Certificates

.

#### Subordinate CA Certificates

.

### Approval or Rejection of Certificate Applications

For the Federal Root CA or FSSP CA, approval or rejection of certificate applications is at the discretion of the EMS PMA or its designee.

### Time to Process Certificate Applications

Certificate applications are processed and a certificate issued within 30 days of identity verification. This is accomplished by configuring the Entrust CA software to force the user activation codes to expire after 14 days.

## Certificate Issuance

### CA Actions During Certificate Issuance

Upon receiving the request, the Federal Root CA/RAs -

* Verify the identity of the requester by following the Trusted Role user registration process outlined above in Section 3.2.3 (and subsections)
* Verify the authority of the requester (i.e., that they are an Entrust / CygnaCom Solutions employee that is a US Citizen) and the integrity of the information in the certificate request as described above in Section 3.2.1
* Once all of the certificate request requirements have been met, use the Security Manager Administrator (SMA) software to generate a CA signed a certificate.
* Make the certificate available to the subscriber after confirming that the subscriber has formally acknowledged their obligations (i.e., has signed an EMS PKI Subscriber Agreement form) as described in section 9.6.3. Refer also to Section 3.2.3 (and subsections), above, for additional user registration details.

#### Root CA

#### FSSP CA

With regard to customer subscribers, the user registration processes are maintained and operated by the delegated RAs listed in Appendix B. For the FSSP subscribers, the user registration requests are submitted to the CA via a third party Card Management System (CMS).

The certificate request may already contain a certificate built by either the RA or the subscriber. For Federal End-Entity subscribers, it is the responsibility of each delegated RA to ensure that only properly vetted requests (in accordance with Sections 3.2 and 3.3 of this CPS) are submitted to the FSSP for certificate creation and signature.

The FSSP CA binds the identity information in the certificate application with the public keys during the certificate issuance process.

Upon receipt of a valid request, the FSSP CA automatically generates an encryption key pair and issues a signature verification public key certificate and an encryption public key certificate for that Subscriber. The FSSP CA then posts the Subscriber’s newly generated encryption certificate to the FSSP CA Master directory.

### Notification to Subscriber by the CA of Issuance of Certificate

As stated in section 4.3.1 above, each Trusted Role Subscriber is actively involved with the issuance of their certificates, so notification by the CA of issuance of the certificate is unnecessary. The Subscriber accesses the Entrust Security Manager Administration on the Registrar’s workstation and enters the shared secret data and other information requested by the Security Manager Administration. This is also true for device certificates. An EMS PKI Trusted Role human sponsor is actively involved with the issuance of the device certificate issued from the Federal Root CA. The Federal Root CA only issues certificates to the FSSP SubCA, Trusted Role users, and the OCSP server. Refer to Sections 3.2.3.1 and 3.2.3.2 for additional information about how Trusted Role human sponsors are vetted.

For the FSSP CA subscribers, the registration processes are operated and maintained by the delegated RAs listed in Appendix B. As such, the delegated RAs are responsible for ensuring that the recipients notified when their certificate has been created and their smartcard is ready (may happen all in one visit or recipient may be notified to come and pickup their smartcard).

## Certificate Acceptance

Before a Subscriber can make effective use of its private key, the EMS PKI Authority explains to the subscriber its responsibilities as defined in section 9.6.3. All Subscribers submit a signed Subscriber Agreement, which includes the Subscriber Obligations. The Subscriber’s signature on the subscriber Agreement Form will be deemed as the acceptance of the certificates and acceptance of the obligations and responsibilities as defined in the Common Policy CP and this CPS. The EMS OA keeps the original signed Subscriber Agreement Form documents.

The successful completion of the Certificate Issuance process constitutes the technical acceptance of the certificate(s).

### Conduct Constituting Certificate Acceptance

No Stipulation.

### Publication of the Certificate by the CA

As specified in 2.1, all CA certificates are published in repositories. Subscriber encryption certificates are published in the repositories.

### Notification of Certificate Issuance by the CA to Other Entities

The Federal PKI Policy Authority is notified whenever a CA operating under the Common Policy issues a CA certificate. Notification is delivered via electronic mail.

The only CA certificates that are issued by the FSSP CA are its own self-signed CA certificates.

## Key Pair and Certificate Usage

### Subscriber Private Key and Certificate Usage

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

### Relying Party Public key and Certificate Usage

Common Policy-issued certificates specify restrictions on use through critical certificate extensions, including the basic constraints and key usage extensions. The Federal Root CA and FSSP CA issue CRLs specifying the current status of all unexpired certificates (except for OCSP responder certificates that include the id-pkix-ocsp-nocheck extension).

## Certificate Renewal

Renewing a certificate means creating a new certificate with the same name, key, and other information as the old one, but with a new, extended validity period and a new serial number. The CA does not renew certificates in this manner. At no time is a certificate renewed using the same key material. All renewed certificates have new key material, new serial number and a new validity period. The old certificate may or may not be revoked, but is not further re-keyed, renewed, or modified.

### Circumstance for Certificate Renewal

Subscriber and CA certificates issued under this CPS are not renewed.

In the event that OCSP Responder certificates are renewed, the aggregated lifetime of the public key within the certificate does not exceed the certificate lifetime specified in section 6.3.2.

### Who May Request Renewal

For the Federal Root CA, FSSP CA and OCSP responders, the EMS OA may request renewal of its own CA certificates.

### Processing Certificate Renewal Requests

No Stipulation.

### Notification of New Certificate Issuance to Subscriber

Under this CPS, subscriber certificates are not renewed. In the event of a CA key compromise new subscriber certificates are issued.

### Conduct Constituting Acceptance of a Renewal Certificate

No Stipulation.

### Publication of the Renewal Certificate by the CA

As specified in Section 2.1, all Federal Root and FSSP CA certificates are published in repositories. The Subscriber encryption certificates are also published in the repositories.

### Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

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

**Root CA**

.

**FSSP CA**

.

The FSSP CA End User Subscriber keys are setup to be automatically re-keyed prior to expiration of the current key pair within the Entrust Security Manager CA software. However, in practice, since the subscriber’s credentials are stored on a PIV card, the credentials cannot be automatically updated and subscribers’ are notified by the RA in advance of expiration to start the process of the having their credentials updated on their PIV card. NOTE: The PIV card has a firm lifetime of 5 years, after which it must be replaced. As such, at the end of 3 years, a subscriber will receive notification to have their credentials updated. The new certificates will be no longer than the remaining lifetime of the PIV card. At the end of the PIV card lifetime, the subscriber will, again, be notified to start the process of obtaining both a new PIV card and new credentials. The End User Subscriber processes are described in more detail in the delegated RAs (listed in Appendix B) registration processes documentation. In person authentication of the Subscriber’s identity as defined in Section 3.2.3 of this CPS will be repeated at least once every nine (9) years. When certificate re-key is required, PKIX-CMP protected messages invoked by the FSSP CA application update the Subscriber’s keys.

### Circumstance for Certificate Re-key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a subscriber periodically obtain new keys. (Section 6.3.2 establishes usage periods for private keys for both CAs and subscribers.) Examples of circumstances requiring certificate re-key include: expiration, loss or compromise, issuance of a new hardware token, and hardware token failure.

### Who May Request Certification of a New Public Key

#### Root CA

.

#### FSSP CA

Subscribers with a currently valid certificate may request certification of a new public key. CAs and RAs are also permitted to request certification of a new public key on behalf of a subscriber. For device certificates, the human sponsor of the device may request certification of a new public key. See section 3.3.1 for more information regarding the identification and authentication process of a routine re-key.

### Processing Certificate Re-keying Requests

Certificate re-key is an automated process initiated by the Entrust software. In order for routine re-key to occur, the Subscriber authenticates to the Entrust software with his/her unexpired certificate issued by the Federal Root CA or FSSP CA. No additional application for re-key is required.

### Notification of New Certificate Issuance to Subscriber

No stipulation.

### Conduct Constituting Acceptance of a Re-keyed Certificate

No stipulation.

### Publication of the Re-keyed Certificate by the CA

All Federal Root CA and FSSP CA certificates are published as specified in section 2.1. The Subscriber encryption certificates are also published in the repositories.

### Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

## Certificate Modification

Modifying a certificate means creating a new certificate that has the same or a different key and a different serial number, and that differs in one or more other fields from the old certificate. The old certificate may or may not be revoked, but is not further re-keyed, renewed, or modified.

### Circumstance for Certificate Modification

The CAs operating as part of the EMS PKI do not perform certificate modification where the modified certificate contains the same subject public key. If data within the certificate is to be modified, new encryption and signature key pairs are generated, following the procedures defined in section 4.8.3.

EMS PKI CAs may modify a CA or OCSP responder certificate whose characteristics have changed (e.g. assert new policy OID). A CA may also perform certificate modification for a subscriber certificate whose characteristics have changed (e.g., name change due to marriage). In all cases, the new certificate shall have a different subject public key.

### Who May Request Certificate Modification

Subscribers with a currently valid certificate may request certificate modification. CAs and RAs may request certificate modification on behalf of a Subscriber.

With regard to FSSP CA device certificates, the human sponsor of the device may request certificate modification.

### Processing Certificate Modification Requests

If an individual’s name changes (e.g., due to marriage), then proof (e.g., a Certificate of Name Change, a Marriage Certificate, or a driver’s license with their new name) of the name change is provided to the RA or other designated agent (e.g., customer LRA) in order for a certificate with the new name to be issued. If an individual’s authorizations or privileges change, the RA will verify those authorizations. If authorizations have reduced, the old certificate is revoked.

Proof of all subject information changes are provided to the RA or other designated agent and verified before the modified certificate is issued.

Certificate modification is an automated process initiated by the Entrust software. In order for the name change, serial number, or any other field from the old certificate to be modified a key recovery has to be initiated. In order for routine re-key to occur, the Subscriber authenticates to the Entrust software with his/her unexpired certificate issued by the Federal Root CA or FSSP CA. No additional application for re-key is required.

### Notification of New Certificate Issuance to Subscriber

No stipulation.

### Conduct Constituting Acceptance of Modified Certificate

No stipulation.

### Publication of the Modified Certificate by the CA

All Federal Root and FSSP CA certificates are published as specified in section 2.1. The Subscriber encryption certificates are also published in the repositories.

### Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

## Certificate Revocation and Suspension

**Root CA**

**.**

**FSSP CA**

The FSSP CA issues CRLs covering all unexpired certificates issued under this policy except for OCSP responder certificates that include the id-pkix-ocsp-nocheck extension.

All certificates issued by the FSSP CA include the cRLDistributionPoints extension field, which indicates the specific CRL that includes the certificate if it is revoked. Only unexpired certificates that have been revoked are included in the CRLs issued by the FSSP CA.

All CRLs include a revocation reason for each revoked certificate issued by the FSSP CA. The Request Approver performing the revocation is required to enter a revocation reason by the FSSP CA Administration Services application. Revocation reasons are identified in Section 4.9.1.

The FSSP CA makes public a description of how to obtain revocation information for the certificates they publish, and an explanation of the consequences of using dated revocation information. This information is given to Subscribers during certificate request or issuance, and is readily available to any potential relying party at the following URL:

<http://sspweb.managed.entrust.com/EMSPKIFSSPRevocationInformation.html> Each certificate issued by the FSSP CA includes the full DN of the CRL Distribution Point to be checked during the verification of the certificate. Relying parties, when working in an online mode, check the current CRL identified by the DN in the certificate's cRLDistributionPoints extension field, along with any other CRLs required in certificate chain processing prior to trusting the certificate. CRL checking is done automatically by the Entrust client software.

When working in an offline mode, relying parties are not able to perform full CRL checking. When relying parties do not perform CRL checking, they accept the certificates at their own risk. Whenever a user chooses to work with out-of-date revocation information, they should be aware of the following security implications:

* + - * A user may successfully verify a signature made by another user whose certificate is revoked or suspended. It is recommended that users re-verify any signatures when they establish a network connection.
			* A user may encrypt a file for an invalid user, for example, for a user whose certificate has been revoked.
			* A user may not have access to other user’s certificates or to the most up-to-date certificate revocation lists (CRLs).
* Users could potentially secure files for people in the recipient lists that they have already securely communicated with who now may be revoked or suspended.

### Circumstances for Revocation

A certificate is revoked when the binding between the subject and the subject’s public key defined within the certificate is no longer considered valid. Certificates are revoked when any of the following circumstances occur:

* Subscriber’s private key is lost, stolen, or suspected of having been compromised
* Subscriber is suspected of fraud or other adverse behavior
* Subscriber is no longer affiliated with the operation or maintenance of the Federal Root CA and FSSP CA
* Subscriber leaves Entrust/CygnaCom
* Subscriber leaves the Department/Agency
* Subscriber’s identifying information contained in the certificate is no longer valid
* Subscriber forgets the password and no recovery is possible
* Subscriber violates the Subscriber Agreement
* Subscriber or other authorized party asks for Subscriber's certificate to be revoked.
* An affiliated organization terminates its contract upon which certificates will be revoked based upon contractual agreement or based upon and of the above stated reasons, whichever occurs first.

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

When the Federal Root CA or FSSP CA revokes a certificate, a revocation reason is included in the CRL entry for the revoked certificate. Exhibit 2 identifies the revocation reasons and the associated definitions:

Exhibit 2: Revocation Reasons

| Revocation Reason | Definition |
| --- | --- |
| Superseded | The certificate has been replaced but there is no suspicion of compromise. |
| Key Compromise | The private key corresponding to the public key in the certificate has been compromised or is suspected to be compromised. |
| Affiliation Change | Some information on the subject of the certificate has changed, but there is no suspicion of compromise. |
| Cessation of Operation | The certificate is no longer needed for its original purpose, but there is no suspicion of compromise. |
| Unspecified | None of the other four revocation reasons apply as to why the certificate was revoked. |

This revocation reason code is not considered confidential and can be shared with the general public.

### Who Can Request a Revocation

#### Root CA

#### FSSP CA

The EMS PMA or OA can request revocation of any Subscriber certificate issued by the FSSP CA.

A Subscriber can always request revocation of a certificate in which they are listed as the certificate subject.

The Subscriber is notified by email or other written means when revocation of their certificate is completed. This notification includes a brief explanation of the revocation reason.

Exhibit 3b identifies the various Subscriber categories and those authorized to request and approve revocation for each category.

Exhibit 3b: FSSP CA Authorized Revocation Requestors

| Subscriber Category | Authorized Requestor(s) |
| --- | --- |
| Security Officer / Master Users (SOMUs) | * Certificate Subject
* Subscriber’s Supervisor
* SOMU
* EMS OA
* EMS PMA
 |
| Registration Authorities | * Certificate Subject
* Subscriber’s Supervisor
* Registration Authority
* SOMU
* EMS OA
* EMS PMA
 |
| Local Registration Authorities | * Certificate Subject
* Subscriber’s Supervisor
* Registration Authority
* SOMU
* EMS OA
* EMS PMA
 |
| Security Compliance Officer | * Certificate Subject
* Subscriber’s Supervisor
* SOMU
* EMS OA
* EMS PMA
 |
| End user Subscribers | * Certificate Subject
* Subscriber’s Supervisor
* Local Registration Authority
* Registration Authority
* SOMU
* EMS OA
* EMS PMA
 |

### Procedure for Revocation Request

#### Root CA

.

#### FSSP CA

A request to revoke a certificate identifies the certificate to be revoked, explains the reason for revocation, and allows the request to be authenticated (e.g., digitally or manually signed). Authorized revocation request approvers are identified in Section 4.9.2. In order to revoke a certificate issued by the FSSP CA, the following actions take place:

1. Requestor submits a digitally signed certificate revocation request to the appropriate Request Approver. The revocation request includes identification information, such as the DN of the certificate subject or certificate serial number, for the certificate to be revoked.
2. The Request Approver verifies the information in the request and validates the authorization of the requestor to submit the request
3. The Request Approver (or their delegate) authenticates themselves to the FSSP CA Administration Services web application using their FSSP CA-issued certificates
4. The Request Approver instructs the CA to revoke the Subscriber’s certificates and issue a new CRL.

When any of the circumstances in Section 4.9.1 occur, the revocation request will be processed as quickly as practical after receiving the request.

Normally, the FSSP CA publishes CRLs no later than every 14 hours, with a *nextUpdate* time of 48 hours, although additional CRLs may be published immediately following certificate revocation. When a revocation request is received at least 2 hours prior to the next scheduled CRL issuance, the revocation request is processed as soon as practical, prior to the next scheduled CRL issuance. When a revocation request is received within 2 hours of the next scheduled CRL issuance, the revocation request is processed as soon as practical after the next scheduled CRL issuance but before the following issuance.

All revocation requests are reviewed to ensure that the revocation requests are legitimate. All legitimate revocation requests will be revoked as follows:

1. Authenticate revocation request, as defined in Section 3.4 of this CPS
2. Establish a secure connection to the CA server
3. Authenticate to the CA server using their FSSP CA credentials
4. Use the FSSP CA Administration Services application to indicate the certificate to be revoked.
5. Verify that the CA server completes the revocation process.
6. Upon completion of revocation process, provide notification to the Subscriber by e-mail or other written means that their certificate has been revoked, including a brief explanation of the revocation reason.

If the revocation is being requested for reason of key compromise or suspected fraudulent use, then the revocation request so indicates.

All FSSP CA Subscribers filling Trusted Roles store their certificates on hardware tokens. The hardware token is surrendered to a FSSP CA SOMU and the SOMU will immediately zeroize the token using the Entrust approved vendor provided utility, or destroy it.

### Revocation Grace Period

The EMS Federal Root CA and FSSP CA do not support a grace period for requesting certificate revocation. All certificate revocation requests are made, as indicated by Sections 4.9.1 – 4.9.3, immediately upon indication that one of the circumstances identified in Section 4.9.1 has occurred.

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

#### Root CA

.

#### FSSP CA

CAs revoke certificates as quickly as practical upon receipt of a proper revocation request. Currently, the EMS PKI CRLs are configured with a lifetime of 18 hours with a pre-update of 12 hours (so new CRLs are issued every 6 hours). The Entrust CA Software automates certificate revocation and the publishing of CRLs. So, processing revocation requests before the next CRL is published is automatically handled by the CA software. Note however, that requests received within two hours of CRL issuance may not be processed before the next CRL issuance. In that case, the revocation will be processed before and published on the subsequent CRL update.

Revocation requests received within two hours of CRL issuance are processed before the following CRL is published.

### Revocation Checking Requirements for Relying Parties

No Stipulation.

### CRL Issuance Frequency

CRLs are issued periodically, even if there are no changes to be made, to ensure timeliness of information.

Certificate status information is published not later than the next scheduled update. Refer to Section 4.9.5 for information on CRL issuance frequency.

CAs that issue certificates to subscribers or operate on-line automatically issue CRLs at least once every 24 hours, and the *nextUpdate* time in the CRL may be no later than 48 hours after issuance time (i.e., the *thisUpdate* time).

The EMS PKI team uses automated monitoring and hourly status notifications (via email) to ensure that the CRL/ARL is up-to-date according to the practices in Section 4.9.1 of this CPS.

#### Root CA

.

#### FSSP CA

The FSSP CA server is configured to issue CRLs/ARLs at least once per 18-hour period. Additional CRLs/ARLs will be issued upon certificate revocation. Upon issuance, the new CRL/ARL will be published in the EMS PKI Master directory, and subsequently pushed out to the FSSP CA Shadow Directory.

### Maximum Latency for CRLs

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

### Online Revocation/Status Checking Availability

The EMS PKI supports on-line status checking via OCSP [RFC 2560] for end entity certificates issued under id-fpki-common-authentication and id-fpki-common-cardAuth. The EMS PKI supports OCSP services to provide alternate forms of revocation status checking. Certificate revocation information is digitally signed by the Validation Authority prior to distribution to the OCSP Responders. The OCSP server pulls the latest CRL information every 15 minutes to create a new response list, which then sent out to the OCSP responder (so the responder is updated every 15 minutes). Each certificate (except for the Root self-signed certificate) issued as part of the EMS PKI contains a reference pointer (contained in the AuthorityInformationAccess field) to the OCSP responder:

[**http://ocsp.managed.entrust.com/OCSP/EMSSSPCAResponder**](http://ocsp.managed.entrust.com/OCSP/EMSSSPCAResponder)

To support relying parties that cannot accommodate on-line communications, EMS PKI (as noted above throughout Section 4.9 and subsections) does support CRLs. Entrust software allows users to read from cache archive files containing X.509 certificates, cross certificates, authority revocation lists (ARLs) and CRLs. These cache archive files also provide sources of certificates, CRLs, and ARLs during the certificate validation process.

### On-line Revocation Checking Requirements

No stipulation.

### Other Forms of Revocation Advertisements Available

No alternate methods of revocation advertisements are used for Subscriber certificates.

### Special Requirements Related To Key Compromise

When a CA certificate is revoked or subscriber certificate is revoked because of compromise, or suspected compromise, of a private key, a CRL is issued within 18 hours of notification. Refer to Section 4.9.5 above for details on the EMS PKI standard CRL issuance frequency. The Entrust CA Software automates certificate revocation and the publishing of CRLs. In addition, when a CA certificate is revoked, the Entrust Security Manager allows an authorized administrator to instruct the system to immediately issue the CRL associated with the revoked certificate.

In the event of a Federal Root CA or FSSP CA private key compromise, the Federal Root CA or FSSP CA follows the procedures outlined in Section 5.7.3 – Entity (CA) Private Key Compromise.

### Circumstances for Suspension

For CA certificates, suspension is not permitted.

#### Root CA

For Trusted Role user certificates, suspension is not permitted.

#### FSSP CA

For end entity certificates, certificates are suspended when any of the following circumstances occur:

* Subscriber’s private key suspected of having been compromised
* Subscriber is suspected of fraud or other adverse behavior
* Subscriber takes an extended leave of absence from the Department/Agency
* Subscriber or other authorized party asks for Subscriber's certificate to be suspended.

### Who Can Request Suspension

The EMS PMA or OA can request suspension of any Subscriber certificate issued by the Federal Root CA (only has Trusted Role users) and the FSSP CA.

A Subscriber can always request suspension of a certificate in which they are listed as the certificate subject.

The Subscriber is notified by email or other written means when suspension of their certificate is completed. This notification includes a brief explanation of the suspension reason.

Exhibits 3a & 3b above identify the various Subscriber categories and those authorized to request suspension for each category.

### Procedure for Suspension Request

In order to suspend a certificate issued by the FSSP CA, the following actions take place:

1. Requestor submits a digitally signed certificate suspension request. The suspension request includes identification information, such as the DN of the certificate subject or certificate serial number, for the certificate to be suspended.
2. The request approver verifies the information in the request and validates the authorization of the requestor to submit the request
3. The request approver authenticates themselves to SMA or to the FSSP CA Administration Services web application using their FSSP CA-issued certificates
4. The request approver instructs the CA to suspend the Subscriber’s certificates and issue a new CRL.

When any of the circumstances in Section 4.9.13 occur, the request approver who receives the suspension request processes the request as quickly as practical after receiving the request.

Normally, the FSSP CA publishes CRLs every 6 hours, with a *nextUpdate* time of 18 hours, although additional CRLs may be published immediately following certificate suspension. When a suspension request is received at least 2 hours prior to the next scheduled CRL issuance, the request approver processes the suspension request as soon as practical, prior to the next scheduled CRL issuance. When a suspension request is received within 2 hours of the next scheduled CRL issuance, the request approver processes the suspension request as soon as practical after the next scheduled CRL issuance but before the following issuance.

The certificate is suspended, as follows:

1. Authenticate suspension request, as defined in Section 3.4 of this CPS
2. Establish a secure connection to the CA server
3. Authenticate to the CA server using their FSSP CA credentials
4. Use the FSSP CA Administration Services application to indicate the certificate to be suspended, including the duration of the suspension
5. Verify that the CA server completes the suspension process.
6. Upon completion of suspension process, provide notification to the Subscriber by e-mail or other written means that their certificate has been suspended, including a brief explanation of the suspension reason.

If the suspension is being requested for reason of suspected fraudulent use, then the request so indicates.

All FSSP CA Subscribers filling Trusted Roles store their certificates on hardware tokens. The hardware token is surrendered to a FSSP CA SOMU who locks the token in a secure storage location until the suspension is lifted or until the certificate is revoked.

### Limits on Suspension Period

No stipulation.

## CERTIFICATE STATUS SERVICES

No stipulation.

### Operational Characteristics

No stipulation.

### Service Availability

No stipulation.

### Optional Features

No stipulation.

## End of Subscription

No stipulation.

## Key Escrow and Recovery

### Key Escrow and Recovery Policy and Practices

CA private keys are never escrowed.

#### Root CA

.

#### FSSP CA

The FSSP CA escrows all managed (as opposed to unmanaged/web certificates) subscriber private decryption keys associated with an encryption certificate it has issued. . The FSSP CA generates encryption key pairs on behalf of its Subscribers and will store a copy of that key pair in the escrow at that time.

The FSSP CA escrows all private decryption keys associated with an encryption certificate it has issued (see section 6.2.3). Escrowed keys are protected at no less than the level of security in which they are generated, delivered, and protected by the subscriber.

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

### Session Key Encapsulation and Recovery Policy and Practices

The EMS PKI CAs do not support session key encapsulation and recovery.

### Certificate Update

#### Root CA

.

#### FSSP CA

The FSSP CA only supports certificate update that includes generation of a new key pair. When data contained in a certificate requires changing, a new certificate with a new public key/private key pair will be issued. The current certificates may be revoked if the information in the old certificate becomes invalid.

When the FSSP CA certificate is updated, the EMS OA will provide notification of the CA key update on the EMS PKI web site.

In addition to the notification provided by the EMS OA, the EMS PKI Root CA will sign a new certificate containing the new FSSP CA’s public verification key and publish this new certificate to the Directory.

In the event that the EMS PKI Root CA certificate is updated, the *old* EMS PKI Root CA signs a link certificate that includes the public key of the *new* EMS PKI Root CA. In addition, the *new* EMS PKI Root CA signs a link certificate that includes the public key of the *old* EMS PKI Root CA. Both link certificates are published to the Directory.

# Facility, Management, and Operational CONTROLS

##### Local Registration Authorities

Each customer participating in the FSSP CA is responsible for identifying (via the Contracting Officer) a number of individuals to fill the role of Local Registration Authority. The Local Registration Authorities are responsible for performing the user lifecycle management for all end user Subscribers within their department/agency. The LRAs are responsible for performing the identification and authentication of these Subscribers; issuance, revocation, and recovery of certificates issued to these Subscribers; and maintenance of completed documentation demonstrating compliance with this CPS and the CP.

The Local Registration Authority role will be created for each customer, pending execution of a Contracting Officer agreement by the customer.

### Identification and Authentication for Each Role

An individual identifies and authenticates him/herself before being permitted to perform any actions set forth above for that role or identity. Subscribers filling trusted roles authenticate to the Federal Root CA or FSSP CA system using PKI credentials stored on an approved cryptographic hardware module.

*

#### FSSP CA

FSSP CA Trusted Roles, i.e., SOMUs, Security Compliance Officers, Registration Authorities and System Administrators are selected based on loyalty, trustworthiness, and integrity. All individuals filling these roles for the FSSP CA meets the following requirements:

* Be a U.S. citizen
* Pass a pre-employment background investigation, as specified in section 5.3.2
* Be a Entrust employee or Entrust contractor employee
* Be appointed in writing by the EMS PMA.

The EMS OA can authorize personnel who meet the following requirements, to temporarily fill Entrust FSSP CA Trusted Roles:

* Be a U.S. citizen
* Be a Entrust employee or Entrust contractor employee
* Be appointed in writing by the EMS PMA.

However, the individual is immediately removed from the Trusted Role if their background investigation reveals items of consequence.

Copies of documentation proving individuals filling Trusted Roles for the FSSP CA meet these requirements will be maintained by the EMS OA, and made available during compliance audits.

In addition to the above, individuals filling Trusted Roles for the FSSP CA:

* Have no other duties that would interfere with their PKI duties and responsibilities
* Have not been previously relieved of PKI duties or responsibilities for reasons of negligence or non-performance of duties
* Have not knowingly been denied a security clearance, or had a security clearance revoked
* Have not been convicted of a felony offense
* Have successfully completed an appropriate training program
* Have demonstrated the ability to perform their duties

**.**

# TECHNICAL SECURITY CONTROLS

## Key Pair Generation and Installation

### Key Pair Generation

#### CA Key Pair Generation

An independent third party, Deloitte & Touche, validated the execution of the key generation procedures by witnessing the key generation ceremony that was performed June 1, 2006

#### Subscriber Key Pair Generation

Entrust software will initiate the process of generating the key pairs for Federal Root CA and FSSP CA Subscribers. Use of FIPS-approved cryptographic modules precludes exposure of plaintext keys outside of the cryptographic modules. The signature key pair for Federal Root CA and FSSP CA Subscribers filling trusted roles is generated using a hardware cryptographic module that is validated to FIPS 140 Security Level 2 (or higher). The Trusted Role Subscriber’s public verification key is delivered to the CA at that time. The Trusted Role Subscriber’s encryption key pair is generated at the CA machine and the Trusted Role Subscriber’s private decryption key is delivered to the Subscriber at that time using the PKIX-CMP protocol to provide both integrity and privacy.

For other end-user Subscriber’s, their signature key pair may be generated in either software or hardware that is validated to FIPS 140-2 Level 2. The Subscriber’s public verification key is delivered to the CA at that time. The Subscriber’s encryption key pair is generated at the CA machine and the Subscriber’s private decryption key is delivered to the Subscriber at that time, in a secure manner.

All pseudo-random numbers used for key generation material are generated by a FIPS-approved algorithm. The following protocols in the Entrust Product configured in FIPS mode use the FIPS186 RNG pseudo-random generator that has been FIPS 140-2 Validated (Certificate #261):

* SEP
* PKIX-CMP
* EntrustSession

The Entrust Security Kernel (Software Version 7.1) has been FIPS 140-2 Level 1 Validated (See NIST Module Validation List - Certificate No. 797). As such, this capability is inherent in the Entrust CA software. The SafeNet Luna SA cryptographic component (Luna PCI Cryptographic Module v2.2) has been FIPS 140-2 Level 3 Validated - Certificate No. 856

#### CSS Key Pair Generation

.

### Private Key Delivery to Subscriber

When the Federal Root CA, FSSP CA, or RAs generate keys on behalf of the subscriber, then the private key is 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 are met:

* Anyone who generates a private signing key for a subscriber will not retain any copy of the key after delivery of the private key to the subscriber.
	+ Private signature keys are generated and remain within the crypto boundary of the cryptographic module of the key owner. Delivery of a keyed module to its owner is performed by trusted personnel. Once a module is keyed, the trusted personnel can change the default activation data for the module. The trusted personnel seal the module in a tamper‑evident container and keep the module under their physical control until such time as it is delivered to the Subscriber. Activation data is not stored in the same tamper‑evident container as the module itself. The module and/or container is properly labeled with the common name of the Subscriber and the date and time of key generation. Delivery of the module and activation data occurs in person. Upon delivery, the Subscriber completes the Subscriber Agreement which acknowledges receipt of the module and activation data.
* The private key(s) are protected from activation, compromise, or modification during the delivery process.
	+ Private signature keys are generated and remain within the crypto boundary of the cryptographic module of the key owner. Delivery of a keyed module to its owner is performed by trusted personnel.
	+ Once a module is keyed, the trusted personnel change the default activation data for the module. The trusted personnel seal the module in a tamper‑evident container and keep the module under their physical control until such time as it is delivered to the Subscriber. Activation data is not stored in the same tamper‑evident container as the module itself.
	+ Private decryption keys will be delivered to the key owner’s cryptographic module by the Federal Root CA and FSSP CA using RSA encryption with the same key size as the keys being protected. Key exchange is performed over an authenticated Certificate Management Protocol (CMP) session between the subscriber and the CA. Authentication is performed with a HMAC derived from one‑time activation data provided to the Subscriber in person by an RA once the Subscriber has completed the necessary registration process.
* The subscriber acknowledges receipt of the private key(s).
	+ Upon delivery, the Subscriber completes the Subscriber Agreement which acknowledges receipt of the module and activation data.
* Delivery is accomplished in a way that ensures that the correct cryptographic module and activation data are provided to the correct subscribers.
	+ For hardware modules, accountability for the location and state of the module is maintained until the subscriber accepts possession of it. The module and/or container are properly labeled with the common name of the Subscriber and the date and time of key generation. Delivery of the module and activation data occurs in person.
	+ For electronic delivery of private keys, the key material is encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data is delivered using a separate secure channel. Private decryption keys are delivered to the key owner’s cryptographic module by the Federal Root and FSSP CA using RSA encryption with the same key size as the keys being protected. Key exchange is performed over an authenticated Certificate Management Protocol (CMP) session between the subscriber and the CA. Authentication is performed with a HMAC derived from one‑time activation data provided to the Subscriber in person by an RA once the Subscriber has completed the necessary registration process.

The delegated RA organizations maintain a record of the subscriber acknowledgment of receipt of the token.

### Public Key Delivery to Certificate Issuer

Where key pairs are generated by the subscriber or RA, the public key and the subscriber’s identity is delivered securely to the CA for certificate issuance. Public keys are delivered to the CA electronically in a signed certificate request.

The signature key pair for Federal Root CA or FSSP CA Subscribers filling trusted roles is generated using a SafeNet iKey 2032 hardware cryptographic module that is validated to FIPS 140 Level 2 (or higher).

The Subscriber’s public verification key is delivered to the CA at that time via a secure PKIX-CMP (RFC 2510) session. A PKIX-CMP secured session provides both confidentiality and integrity between the Federal Root CA or FSSP CA and the Entrust clients using digital signatures or Message Authentication Codes (MACs).

Entrust Software is able to relate the identity of the recipient of information via the activation code which is comprised of an authorization code and reference number. When a user is newly added to Entrust, keys are recovered, or activation codes are reissued Entrust Security Manager creates an activation code. The user then inputs the activation code when prompted by the Entrust client software. The Authorization code is used to derive a MAC key (for integrity and authentication) for communications between users and Entrust CA using the PKIX-CMP. Note: the PKIX-CMP uses Triple DES, which has an effective strength of 112 bits. According to NIST (http://www.keylength.com/en/4/), RSA-2048 (which the CA keys are) is equivalent to 112-bit symmetric encryption in its strength.

### CA Public Key Delivery to Relying Parties

When the Federal Root CA or FSSP CA updates its signature key pair, the CA distributes the new public key in a secure fashion. The new public key may be distributed in a self-signed certificate, in a key rollover certificate, or, for the Federal Root CA, in cross-certificates.

#### Federal Root CA

.

#### FSSP CA

.

.

### Key Sizes

.

### Public Key Parameters Generation and Quality Checking

.

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

#### Federal Root CA

.

#### FSSP CA

Keys are certified for use in signing, non-repudiation or encrypting. All certificates issued by the FSSP CA use the *keyUsage* extension to govern the use of a specific key.

Public keys that are bound into subscriber user certificates are used only for signing or encrypting, but not both. Subscriber certificates asserting id-fpki-common-authentication or id-fpki-common-cardAuth only set the *digitalSignature* bit. All other human Subscriber certificates to be used for digital signatures set both the *digitalSignature* bit and the *nonRepudiation* bit.

Subscriber certificates containing RSA public keys to be used for key transport set the *keyEncipherment* bit. User certificates that contain elliptic curve public keys that are to be used for key agreement set the *keyAgreement* bit.

Public keys that are bound into CA certificates are used only for signing certificates and status information (e.g., CRLs). CA certificates have the *keyCertSign* and *cRLSign* bits set. CA certificates whose subject public key is to be used to verify Online Certificate Status Protocol (OCSP) responses assert the *digitalSignature* and/or *nonRepudiation* bits.

Device certificates that contain RSA public keys that are used for key transport assert the *keyEncipherment* bit. Device certificates used for digital signatures set the *digitalSignature* bit. Device certificates to be used for data encryption set the *keyEncipherment* bit. Device certificates that contain elliptic curve public keys that are to be used for key agreement assert the *keyAgreement* bit. Device certificates to be used for both digital signatures and key management assert the *digitalSignature* bit and either the *keyEncipherment* (for RSA) or *keyAgreement* (for elliptic curve) bit. Device certificates do not assert the *nonRepudiation* bit.

The *dataEncipherment*, *encipherOnly*, and *decipherOnly* bits are not asserted in certificates issued under this CPS.

## Private Key Protection and Cryptographic Module Engineering Controls

### Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is the latest version of the FIPS 140 series, *Security Requirements for Cryptographic Modules* [FIPS 140-2]. The Entrust Security kernel is FIPS 140-2 validated using the following FIPS approved algorithms:

* Triple-DES (Cert. #495);
* AES (Cert. #484);
* DSA (Cert. #196);
* SHS (Cert. #551);
* RNG (Cert. #261);
* RSA (Cert. #198);
* HMAC (Cert. #238);
* ECDSA (Cert. #45).

.

Private key storage for Federal Root CA Subscribers (Trusted Role Personnel) is performed using a hardware cryptographic module that is validated to FIPS 140 Security Level 2.

Private key storage for FSSP CA Subscribers issued certificates under the id-fpki-common-hardware, id-fpki-common-authentication, or id-fpki-common-cardAuth is performed using a hardware cryptographic module that is validated to FIPS 140 Security Level 2. For all other Subscribers, the private key storage is performed using either hardware or software cryptographic modules validated to FIPS 140 Security Level 1 or 2.

All cryptographic modules mentioned above operate such that the private asymmetric cryptographic keys are never output in plaintext (unencrypted).

The CSS (OCSP Server) uses the SafeNet Luna SA HSM, which is validated to FIPS 140 Level 2 or higher (refer to Section 6.1.1.2, above).

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

.

### Private Key Escrow

Federal Root CA and FSSP CA private keys are never escrowed.

Subscriber key management keys (encryption/decryption key pair) are escrowed to provide key recovery as described in section 4.12.1. The Federal Root CA and FSSP CA escrow all private decryption keys associated with an encryption certificate it has issued. These keys are stored in a private database and are encrypted with a 128‑bit triple-DES key stored in the Federal Root CA’s or the FSSP CA’s cryptographic module. The Federal Root CA and FSSP CA generate encryption key pairs on behalf of its Subscribers and will store a copy of that key pair in the escrow at that time.

The Federal Root CA and FSSP CA will not release an escrowed key unless directed to by an authorized person serving in a trusted role with that privilege. All recovery of escrowed keys is logged by the CA as part of its audit trail.

The Federal Root CA and FSSP CA do not escrow keys used for digital signature. No external parties are authorized to maintain an escrow of keys associated with certificates issued by the Federal Root CA or FSSP CA.

### Private Key Backup

#### Backup of CA Private Signature Key

##### Federal Root CA

.

##### FSSP CA

.

Subscribers with certificates issued under id-fpki-common-authentication or id-fpki-common-cardAuth are not authorized to backup their private keys. All other Subscribers are permitted to make backup copies of their private keys, so long as they remain within the control of the Subscriber.

The Federal Root CA and FSSP CA each operate a private key escrow to allow for decryption key recovery for end entities as described in Section 6.2.3.

#### Backup of Subscriber Private Signature Key

Trusted Role subscribers are not permitted to backup their private keys because their credentials are generated on SafeNet iKey 2032 tokens that cannot be duplicated.

FSSP CA subscriber private signature keys whose corresponding public key is contained in a certificate asserting the id-fpki-common-authentication or id-fpki-common-cardAuth are not backed up or copied.

Private signature keys used to support non-repudiation and digital signature services are not archived by the Federal Root CA or FSSP CA.

#### Backup of Subscriber Private Key Management Key

The Federal Root CA operates a private key escrow to allow for decryption key recovery for end entities as described in Section 4.12.1.

For the Federal Root CA and FSSP CA, backed up subscriber private key management keys are not stored in plaintext form outside the cryptographic module. Storage ensures security controls consistent with the protection provided by the subscriber’s cryptographic module.

#### Backup of CSS Private Key

.

### Private Key Archival

The Federal Root CA, FSSP CA, and subscriber private signature keys are not archived. The Federal Root CA and FSSP CA archive all private decryption keys as part of its normal operating process in accordance with section 5.5.

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

.

All other keys are 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 is encrypted during transport; private keys never exist in plaintext form outside the cryptographic module boundary.

The Federal Root CA and FSSP CA will generate private decryption keys on behalf of end entity Subscribers within its own software cryptographic module. The private key will be securely transported to the Subscriber using a temporary encryption key generated by the Subscriber and transmitted through a secure CMP session.

The Subscriber’s software will then request a wrapping key from the Subscriber’s hardware cryptographic module. The wrapping key is used to encrypt the private decryption key for transport into the module at which point it is unwrapped for permanent storage.

Certificates are not issued to end entities that generate their own encryption key pair, nor will certificates be issued for signature key pairs that are not generated directly within the Subscriber module at the time the request is made.

### Private Key Storage on Cryptographic Module

No stipulation beyond that specified in FIPS 140.

### Method of Activating Private Key

#### Root CA

.

#### FSSP CA

.

FSSP CA Subscribers with certificates issued under id-fpki-common-authentication, id-fpki-common-policy, id-fpki-common-hardware, or id-fpki-common-devices activate their private key by authenticating to their cryptographic module. Methods of authentication include but are not limited to pass phrases, PINs or biometrics. Entry of activation data is protected from disclosure (i.e., the data is not displayed while it is entered).

For certificates issued under id-fpki-common-cardAuth, subscriber authentication is not required to use the associated private key.

### Method of Deactivating Private Key

.

Cryptographic modules used to store Subscriber private keys that have been activated are not left unattended or otherwise available to unauthorized access. Federal Root CA and FSSP CA Subscribers deactivate their private keys by logging out of the application controlling their cryptographic module or by disconnecting the module from its power source. Logout may also occur automatically as determined by a preset timer. For Federal Root CA and FSSP CA Subscribers, the idle-timer is set to no more than 15 minutes.

All Federal Root CA and FSSP CA Subscribers sign Subscriber Agreements. The agreement delineates the rules of behavior regarding the control of cryptographic modules that have been activated.

Refer to Section 5.1.2.1 above for information on the physical security controls and storage locations implemented to protect activated and deactivated private keys for Federal Root CA and FSSP CA Subscribers.

### Method of Destroying Private Key

Private keys located on hardware cryptographic modules are destroyed by reinitializing the cryptographic module using a vendor-supplied utility. The private key can also be destroyed by physically destroying the token (or PIV card for FSSP CA End-Entity subscribers).

Individuals in trusted roles destroy CA, RA, and CSS (e.g., OCSP server) private signature keys when they are no longer needed.

For the Federal Root CA, the only subscribers are trusted personnel. SOMUs and SCOs can either surrender their cryptographic module to another SOMU for reinitialization/destruction or destroy their private signature keys, when they are no longer needed or when the certificates to which they correspond expire or are revoked.

FSSP CA subscribers can either surrender their cryptographic module to CA/RA personnel for destruction or destroy their private signature keys, when they are no longer needed or when the certificates to which they correspond expire or are revoked.

For FSSP CA subscribers, those entities that hold PIV cards, the destruction of their token is under the control of the issuing agency and per FIPS 201 its surrender and destruction is controlled and documented.

For all other tokens, the destruction or re-initialization of the token is recorded and signed by the party performing the destruction or re-initialization

### Cryptographic Module Rating

See section 6.2.1.

## Other Aspects of Key Pair Management

Because the Federal Root CA and FSSP CA are “medium assurance” certificate authorities, all Subscribers to the Federal Root CA and FSSP CA are issued, at a minimum, 2-key pairs, where one key pair is used for encryption/decryption operations and the second key pair is used for digital signature creation/verification.

### Public Key Archival

The Federal Root CA and FSSP CA maintain an archive of all public key certificates they issue.

### Certificate Operational Periods and Key Usage Periods

#### Federal Root CA

.

#### FSSP CA

.

FSSP CA Subscribers will be issued certificates with a validity of three years and a corresponding private key usage period of three years for signature keys. Subscribers may use their private decryption keys as needed without constraint. For Subscribers public keys, the maximum usage period is three years.

The FSSP CA does not issue a CA certificate whose validity period extends beyond its own certificate’s validity period.

For OCSP responders operating under this policy and all other subscriber public keys, the maximum usage period is three years.

## Activation Data

### Activation Data Generation and Installation

For user initialization, user key update, and user key recovery Entrust CA software generates a one time use activation code. The activation code is comprised of an authorization code and reference number. This activation code is used to derive MAC keys that are used for integrity and authentication in PKIX-CMP sessions. The one time use activation code is established by the Entrust Authority cryptographic module which is FIPS 140-2 Level 1 Validated.

The Entrust Authority cryptographic module used in conjunction with a cryptographic hardware module meets the FIPS 140-2 Level 2 validation.

Since the end user registration process is operated and maintained by the delegated RAs (listed in Appendix B), the delegated RAs are responsible for ensuring that subscribers select appropriate passwords.

### Activation Data Protection

Activation data for Subscribers is not to be written down. Refer to the EMS PKI Subscriber Agreement for more details.

Activation data is never to be shared.

Activation data is never to be transmitted unencrypted over the network.

.

Data used to unlock private keys is protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data is currently recorded and secured at the level of assurance associated with the activation of the cryptographic module, and is not stored with the cryptographic module (refer to Section 5.1.2.1).

Activation data may also be memorized or be Biometric in nature. Trusted Role personnel may also store the passwords electronically in a form that is protected by a crypto module that has been evaluated, at a minimum, at FIPS 140-2 Level 2.

### Other Aspects of Activation Data

.

FSSP CA Subscribers change their cryptographic module activation data in accordance with applicable policies defined by the Federal Agency sponsoring the Subscriber.

Activation data for cryptographic modules for which control is transferred (such as when a person serving in a trusted role departs the organization) is changed as soon as practical following transfer.

Activation data for Federal Root CA and FSSP CA cryptographic modules is changed not less than once every year.