



## **Entrust Managed Services PKI**

**COVER PAGE**

**REDACTED**

**15 November, 2017**

**Version 1.1 - FINAL**

This CPS implements the policy requirements of the X.509 Certificate Policy for CAs issuing Derived Credentials under [CP-EMS-SSP].

*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 without prior approval of the EMS PKI Policy Management Authority.*



# X.509 Certification Practices Statement For Entrust Managed Service PKI Derived PIV Credential Federal Shared Service Provider Certification Authorities

15 November, 2017

Version 1.1 – FINAL (REDACTED)

## SIGNATURE PAGE

---

Entrust MSO Policy Authority (Print Name)

---

Entrust Managed Services  
PKI Policy Authority

---

Date

## CONTENTS

<b>1.</b>	<b>INTRODUCTION.....</b>	<b>8</b>
1.1	Overview.....	8
1.1.1	Certificate Practices Statement .....	8
1.1.2	Relationship between [CCPS-EMS-SSP] and this Delta CPS.....	<b>Error! Bookmark not defined.</b>
1.1.3	Scope.....	<b>Error! Bookmark not defined.</b>
1.1.4	Interoperation with CAs issuing under different policies .....	<b>Error! Bookmark not defined.</b>
1.2	Document Name and Identification .....	<b>Error! Bookmark not defined.</b>
1.2.1	Federal Root CA .....	<b>Error! Bookmark not defined.</b>
1.2.2	Derived Credential CAs .....	<b>Error! Bookmark not defined.</b>
1.3	PKI Participants .....	<b>Error! Bookmark not defined.</b>
1.3.1	PKI Authorities .....	<b>Error! Bookmark not defined.</b>
1.3.2	Registration Authority .....	<b>Error! Bookmark not defined.</b>
1.3.3	Trusted Agents .....	<b>Error! Bookmark not defined.</b>
1.3.4	Subscribers.....	<b>Error! Bookmark not defined.</b>
1.3.5	Relying Parties .....	<b>Error! Bookmark not defined.</b>
1.3.6	Other Participants.....	<b>Error! Bookmark not defined.</b>
1.4	Certificate Usage.....	<b>Error! Bookmark not defined.</b>
1.4.1	Appropriate Certificate Uses.....	<b>Error! Bookmark not defined.</b>
1.4.2	Prohibited Certificate Uses .....	<b>Error! Bookmark not defined.</b>
1.5	Policy Administration .....	<b>Error! Bookmark not defined.</b>
1.5.1	Organization Administering the Document .....	<b>Error! Bookmark not defined.</b>
1.5.2	Contact Information .....	<b>Error! Bookmark not defined.</b>
1.5.3	Person Determining CPS Suitability for the Policy .	<b>Error! Bookmark not defined.</b>
1.5.4	CPS Approval Procedures.....	<b>Error! Bookmark not defined.</b>
1.6	Definitions and Acronyms .....	<b>Error! Bookmark not defined.</b>
1.6.1	List of Definitions .....	<b>Error! Bookmark not defined.</b>
1.6.2	List of Acronyms .....	<b>Error! Bookmark not defined.</b>
2.1	Repositories.....	<b>Error! Bookmark not defined.</b>
2.1.1	Root CA .....	<b>Error! Bookmark not defined.</b>
2.1.2	FSSP CA .....	<b>Error! Bookmark not defined.</b>
2.1.3	Derived Credential CAs.....	<b>Error! Bookmark not defined.</b>
2.2	Publication of Certification Information.....	<b>Error! Bookmark not defined.</b>
2.2.1	Publication of Certificates and Certificate Status ....	<b>Error! Bookmark not defined.</b>
2.2.2	Publication of CA Information .....	<b>Error! Bookmark not defined.</b>
2.2.3	Interoperability.....	<b>Error! Bookmark not defined.</b>
2.3	Time or Frequency of Publication .....	<b>Error! Bookmark not defined.</b>
2.4	Access Controls on Repositories .....	<b>Error! Bookmark not defined.</b>
2.4.1	Access Controls on Root CA Repositories	<b>Error! Bookmark not defined.</b>

- 2.4.2 Access Controls on FSSP CA Repositories ..... **Error! Bookmark not defined.**
- 3 IDENTIFICATION AND AUTHENTICATION ..... ERROR! BOOKMARK NOT DEFINED.**
  - 3.1 Naming.....**Error! Bookmark not defined.**
    - 3.1.1 Types of Names .....**Error! Bookmark not defined.**
    - 3.1.2 Need for Names to be Meaningful.....**Error! Bookmark not defined.**
    - 3.1.3 Anonymity or Pseudonymity of Subscribers ..... **Error! Bookmark not defined.**
    - 3.1.4 Rules for Interpreting Various Name Forms ..... **Error! Bookmark not defined.**
    - 3.1.5 Uniqueness of Names .....**Error! Bookmark not defined.**
    - 3.1.6 Recognition, Authentication, and Role of Trademarks .. **Error! Bookmark not defined.**
  - 3.2 Initial Identity Validation.....**Error! Bookmark not defined.**
    - 3.2.1 Method to Prove Possession of Private Key ..... **Error! Bookmark not defined.**
    - 3.2.2 Authentication of Organization Identity ....**Error! Bookmark not defined.**
    - 3.2.3 Authentication of Individual Identity.....**Error! Bookmark not defined.**
    - 3.2.4 Non-verified Subscriber Information.....**Error! Bookmark not defined.**
    - 3.2.5 Validation of Authority.....**Error! Bookmark not defined.**
    - 3.2.6 Criteria for Interoperation.....**Error! Bookmark not defined.**
  - 3.3 Identification and Authentication for Re-Key Requests..... **Error! Bookmark not defined.**
    - 3.3.1 Identification and Authentication for Routine Re-key.... **Error! Bookmark not defined.**
    - 3.3.2 Identification and Authentication for Re-Key After Revocation..... **Error! Bookmark not defined.**
    - 3.3.3 Identification and Authentication for Certificate Recovery..... **Error! Bookmark not defined.**
  - 3.4 Identification and Authentication for Revocation Request.. **Error! Bookmark not defined.**
- 4 OPERATIONAL REQUIREMENTS ..... ERROR! BOOKMARK NOT DEFINED.**
  - 4.1 Certificate Application.....**Error! Bookmark not defined.**
    - 4.1.1 Who Can Submit a Certificate Application ..... **Error! Bookmark not defined.**
    - 4.1.2 Enrollment Process and Responsibilities ...**Error! Bookmark not defined.**
  - 4.2 Certificate Application Processing .....**Error! Bookmark not defined.**
    - 4.2.1 Performing Identification and Authentication Functions **Error! Bookmark not defined.**
    - 4.2.2 Approval or Rejection of Certificate Applications .. **Error! Bookmark not defined.**
    - 4.2.3 Time to Process Certificate Applications ..**Error! Bookmark not defined.**
  - 4.3 Certificate Issuance.....**Error! Bookmark not defined.**
    - 4.3.1 CA Actions during Certificate Issuance ....**Error! Bookmark not defined.**

- 4.3.2 Notification to Subscriber by the CA of Issuance of Certificate ..... **Error! Bookmark not defined.**
- 4.4 Certificate Acceptance ..... **Error! Bookmark not defined.**
  - 4.4.1 Conduct Constituting Certificate Acceptance..... **Error! Bookmark not defined.**
  - 4.4.2 Publication of the Certificate by the CA.... **Error! Bookmark not defined.**
  - 4.4.3 Notification of Certificate Issuance by the CA to Other Entities ..... **Error! Bookmark not defined.**
- 4.5 Key Pair and Certificate Usage..... **Error! Bookmark not defined.**
  - 4.5.1 Subscriber Private Key and Certificate Usage..... **Error! Bookmark not defined.**
  - 4.5.2 Relying Party Public key and Certificate Usage..... **Error! Bookmark not defined.**
- 4.6 Certificate Renewal..... **Error! Bookmark not defined.**
  - 4.6.1 Circumstance for Certificate Renewal ..... **Error! Bookmark not defined.**
  - 4.6.2 Who May Request Renewal..... **Error! Bookmark not defined.**
  - 4.6.3 Processing Certificate Renewal Requests.. **Error! Bookmark not defined.**
  - 4.6.4 Notification of New Certificate Issuance to Subscriber . **Error! Bookmark not defined.**
  - 4.6.5 Conduct Constituting Acceptance of a Renewal Certificate..... **Error! Bookmark not defined.**
  - 4.6.6 Publication of the Renewal Certificate by the CA... **Error! Bookmark not defined.**
  - 4.6.7 Notification of Certificate Issuance by the CA to Other Entities ..... **Error! Bookmark not defined.**
- 4.7 Certificate Re-key ..... **Error! Bookmark not defined.**
  - 4.7.1 Circumstance for Certificate Re-key ..... **Error! Bookmark not defined.**
  - 4.7.2 Who May Request Certification of a New Public Key... **Error! Bookmark not defined.**
  - 4.7.3 Processing Certificate Re-keying Requests ..... **Error! Bookmark not defined.**
  - 4.7.4 Notification of New Certificate Issuance to Subscriber . **Error! Bookmark not defined.**
  - 4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate ..... **Error! Bookmark not defined.**
  - 4.7.6 Publication of the Re-keyed Certificate by the CA . **Error! Bookmark not defined.**
  - 4.7.7 Notification of Certificate Issuance by the CA to Other Entities ..... **Error! Bookmark not defined.**
- 4.8 Certificate Modification..... **Error! Bookmark not defined.**
  - 4.8.1 Circumstance for Certificate Modification **Error! Bookmark not defined.**
  - 4.8.2 Who May Request Certificate Modification..... **Error! Bookmark not defined.**
  - 4.8.3 Processing Certificate Modification Requests ..... **Error! Bookmark not defined.**

- 4.8.4 Notification of New Certificate Issuance to Subscriber . **Error! Bookmark not defined.**
- 4.8.5 Conduct Constituting Acceptance of Modified Certificate ..... **Error! Bookmark not defined.**
- 4.8.6 Publication of the Modified Certificate by the CA.. **Error! Bookmark not defined.**
- 4.8.7 Notification of Certificate Issuance by the CA to Other Entities ..... **Error! Bookmark not defined.**
- 4.9 Certificate Revocation and Suspension ..... **Error! Bookmark not defined.**
  - 4.9.1 Circumstances for Revocation ..... **Error! Bookmark not defined.**
  - 4.9.2 Who Can Request a Revocation ..... **Error! Bookmark not defined.**
  - 4.9.3 Procedure for Revocation Request..... **Error! Bookmark not defined.**
  - 4.9.4 Revocation Grace Period ..... **Error! Bookmark not defined.**
  - 4.9.5 Time within which CA must Process the Revocation Request..... **Error! Bookmark not defined.**
  - 4.9.6 Revocation Checking Requirements for Relying Parties **Error! Bookmark not defined.**
  - 4.9.7 CRL Issuance Frequency ..... **Error! Bookmark not defined.**
  - 4.9.8 Maximum Latency for CRLs ..... **Error! Bookmark not defined.**
  - 4.9.9 Online Revocation/Status Checking Availability .... **Error! Bookmark not defined.**
  - 4.9.10 On-line Revocation Checking Requirements..... **Error! Bookmark not defined.**
  - 4.9.11 Other Forms of Revocation Advertisements Available .. **Error! Bookmark not defined.**
  - 4.9.12 Special Requirements Related To Key Compromise..... **Error! Bookmark not defined.**
  - 4.9.13 Circumstances for Suspension ..... **Error! Bookmark not defined.**
  - 4.9.14 Who Can Request Suspension ..... **Error! Bookmark not defined.**
  - 4.9.15 Procedure for Suspension Request..... **Error! Bookmark not defined.**
  - 4.9.16 Limits on Suspension Period ..... **Error! Bookmark not defined.**
- 4.10 CERTIFICATE STATUS SERVICES ..... **Error! Bookmark not defined.**
  - 4.10.1 Operational Characteristics ..... **Error! Bookmark not defined.**
  - 4.10.2 Service Availability ..... **Error! Bookmark not defined.**
  - 4.10.3 Optional Features ..... **Error! Bookmark not defined.**
- 4.11 End of Subscription..... **Error! Bookmark not defined.**
- 4.12 Key Escrow and Recovery ..... **Error! Bookmark not defined.**
  - 4.12.1 Key Escrow and Recovery Policy and Practices ..... **Error! Bookmark not defined.**
  - 4.12.2 Session Key Encapsulation and Recovery Policy and Practices ..... **Error! Bookmark not defined.**
  - 4.12.3 Certificate Update ..... **Error! Bookmark not defined.**
- 5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS.....ERROR! BOOKMARK NOT DEFINED.**
  - 5.1 Physical Controls ..... **Error! Bookmark not defined.**
    - 5.1.1 Site Location and Construction..... **Error! Bookmark not defined.**

5.1.2	Physical Access.....	<b>Error! Bookmark not defined.</b>
5.1.3	Power and Air Conditioning .....	<b>Error! Bookmark not defined.</b>
5.1.4	Water Exposures .....	<b>Error! Bookmark not defined.</b>
5.1.5	Fire Prevention and Protection.....	<b>Error! Bookmark not defined.</b>
5.1.6	Media Storage .....	<b>Error! Bookmark not defined.</b>
5.1.7	Waste Disposal.....	<b>Error! Bookmark not defined.</b>
5.1.8	Off-Site Backup .....	<b>Error! Bookmark not defined.</b>
5.2	Procedural Controls .....	<b>Error! Bookmark not defined.</b>
5.2.1	Trusted Roles .....	<b>Error! Bookmark not defined.</b>
5.2.2	Number of Persons Required per Task .....	<b>Error! Bookmark not defined.</b>
5.2.3	Identification and Authentication for Each Role .....	<b>Error! Bookmark not defined.</b>
5.2.4	Roles Requiring Separation of Duties.....	<b>Error! Bookmark not defined.</b>
5.3	Personnel Controls .....	<b>Error! Bookmark not defined.</b>
5.3.1	Qualifications, Experience, and Clearance Requirements .....	<b>Error! Bookmark not defined.</b>
5.3.2	Background Check Procedures .....	<b>Error! Bookmark not defined.</b>
5.3.3	Training Requirements.....	<b>Error! Bookmark not defined.</b>
5.3.4	Retraining Frequency and Requirements...	<b>Error! Bookmark not defined.</b>
5.3.5	Job Rotation Frequency and Sequence .....	<b>Error! Bookmark not defined.</b>
5.3.6	Sanctions for Unauthorized Actions .....	<b>Error! Bookmark not defined.</b>
5.3.7	Independent Contractor Requirements .....	<b>Error! Bookmark not defined.</b>
5.3.8	Documentation Supplied to Personnel.....	<b>Error! Bookmark not defined.</b>
5.4	Audit Logging Procedures .....	<b>Error! Bookmark not defined.</b>
5.4.1	Types of Events Recorded .....	<b>Error! Bookmark not defined.</b>
5.4.2	Frequency of Processing Log.....	<b>Error! Bookmark not defined.</b>
5.4.3	Retention Period for Audit Log .....	<b>Error! Bookmark not defined.</b>
5.4.4	Protection of Audit Log .....	<b>Error! Bookmark not defined.</b>
5.4.5	Audit Log Backup Procedures .....	<b>Error! Bookmark not defined.</b>
5.4.6	Audit Collection System (Internal vs. External).....	<b>Error! Bookmark not defined.</b>
5.4.7	Notification to Event-Causing Subject .....	<b>Error! Bookmark not defined.</b>
5.4.8	Vulnerability Assessments.....	<b>Error! Bookmark not defined.</b>
5.5	Records Archival .....	<b>Error! Bookmark not defined.</b>
5.5.1	Types of Data Archived .....	<b>Error! Bookmark not defined.</b>
	No stipulation.....	<b>Error! Bookmark not defined.</b>
5.5.2	Retention Period for Archive .....	<b>Error! Bookmark not defined.</b>
5.5.3	Protection of Archive .....	<b>Error! Bookmark not defined.</b>
5.5.4	Archive Backup Procedures.....	<b>Error! Bookmark not defined.</b>
5.5.5	Requirement for Time-Stamping of Archive Records....	<b>Error! Bookmark not defined.</b>
5.5.6	Archive Collection System (Internal and External).	<b>Error! Bookmark not defined.</b>
5.5.7	Procedures to Obtain and Verify Archive Information...	<b>Error! Bookmark not defined.</b>
5.6	Key Changeover.....	<b>Error! Bookmark not defined.</b>



- 5.6.1 Root CA .....**Error! Bookmark not defined.**
- 5.6.2 Derived Credential FSSP CA.....**Error! Bookmark not defined.**
- 5.7 Compromise and Disaster Recovery.....**Error! Bookmark not defined.**
  - 5.7.1 Incident and Compromise Handling Procedures ..... **Error! Bookmark not defined.**
  - 5.7.2 Computer Resources, Software, and/or Data are Corrupted..... **Error! Bookmark not defined.**
  - 5.7.3 Entity (CA) Private Key Compromise Procedures .. **Error! Bookmark not defined.**
  - 5.7.4 Business Continuity Capabilities after a Disaster .... **Error! Bookmark not defined.**
- 5.8 CA or RA Termination .....**Error! Bookmark not defined.**
- 6 TECHNICAL SECURITY CONTROLS ..... ERROR! BOOKMARK NOT DEFINED.**
  - 6.1 Key Pair Generation and Installation .....**Error! Bookmark not defined.**
    - 6.1.1 Key Pair Generation.....**Error! Bookmark not defined.**
    - 6.1.2 Private Key Delivery to Subscriber .....**Error! Bookmark not defined.**
    - 6.1.3 Public Key Delivery to Certificate Issuer ..**Error! Bookmark not defined.**
    - 6.1.4 CA Public Key Delivery to Relying Parties ..... **Error! Bookmark not defined.**
    - 6.1.5 Key Sizes .....**Error! Bookmark not defined.**
    - 6.1.6 Public Key Parameters Generation and Quality Checking ..... **Error! Bookmark not defined.**
    - 6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)..... **Error! Bookmark not defined.**
  - 6.2 Private Key Protection and Cryptographic Module Engineering Controls ... **Error! Bookmark not defined.**
    - 6.2.1 Cryptographic Module Standards and Controls..... **Error! Bookmark not defined.**
    - 6.2.2 Private Key (n out of m) Multi-Person Control ..... **Error! Bookmark not defined.**
    - 6.2.3 Private Key Escrow.....**Error! Bookmark not defined.**
    - 6.2.4 Private Key Backup .....**Error! Bookmark not defined.**
    - 6.2.5 Private Key Archival.....**Error! Bookmark not defined.**
    - 6.2.6 Private Key Transfer into or from a Cryptographic Module ..... **Error! Bookmark not defined.**
    - 6.2.7 Private Key Storage on Cryptographic Module..... **Error! Bookmark not defined.**
    - 6.2.8 Method of Activating Private Key .....**Error! Bookmark not defined.**
    - 6.2.9 Method of Deactivating Private Key .....**Error! Bookmark not defined.**
    - 6.2.10 Method of Destroying Private Key .....**Error! Bookmark not defined.**
    - 6.2.11 Cryptographic Module Rating .....**Error! Bookmark not defined.**
  - 6.3 Other Aspects of Key Pair Management .....**Error! Bookmark not defined.**
    - 6.3.1 Public Key Archival.....**Error! Bookmark not defined.**
    - 6.3.2 Certificate Operational Periods and Key Usage Periods **Error! Bookmark not defined.**
  - 6.4 Activation Data .....**Error! Bookmark not defined.**

6.4.1	Activation Data Generation and Installation.....	<b>Error! Bookmark not defined.</b>
6.4.2	Activation Data Protection.....	<b>Error! Bookmark not defined.</b>
6.4.3	Other Aspects of Activation Data .....	<b>Error! Bookmark not defined.</b>
6.5	Computer Security Controls .....	<b>Error! Bookmark not defined.</b>
6.5.1	Specific Computer Security Technical Requirements ....	<b>Error! Bookmark not defined.</b>
6.5.2	Computer Security Rating.....	<b>Error! Bookmark not defined.</b>
6.6	Lifecycle Technical Controls .....	<b>Error! Bookmark not defined.</b>
6.6.1	System Development Controls .....	<b>Error! Bookmark not defined.</b>
6.6.2	Security Management Controls.....	<b>Error! Bookmark not defined.</b>
6.6.3	Life Cycle Security Controls .....	<b>Error! Bookmark not defined.</b>
6.7	Network Security Controls .....	<b>Error! Bookmark not defined.</b>
6.8	Time-Stamping .....	<b>Error! Bookmark not defined.</b>
<b>7</b>	<b>CERTIFICATE, CRL, AND OCSP PROFILES.....</b>	<b>ERROR! BOOKMARK NOT DEFINED.</b>
7.1	Certificate Profile.....	<b>Error! Bookmark not defined.</b>
7.1.1	Version Numbers .....	<b>Error! Bookmark not defined.</b>
7.1.2	Certificate Extensions .....	<b>Error! Bookmark not defined.</b>
7.1.3	Algorithm Object Identifiers.....	<b>Error! Bookmark not defined.</b>
7.1.4	Name Constraints.....	<b>Error! Bookmark not defined.</b>
7.1.5	Certificate Policy Object Identifier .....	<b>Error! Bookmark not defined.</b>
7.1.6	Usage of Policy Constraints Extension.....	<b>Error! Bookmark not defined.</b>
7.1.7	Policy Qualifiers Syntax and Semantics ....	<b>Error! Bookmark not defined.</b>
7.1.8	Processing Semantics for the Critical Certificate Policy Extension ..	<b>Error! Bookmark not defined.</b>
7.2	CRL Profile.....	<b>Error! Bookmark not defined.</b>
7.2.1	Version Numbers .....	<b>Error! Bookmark not defined.</b>
7.2.2	CRL and CRL Entry Extensions.....	<b>Error! Bookmark not defined.</b>
7.3	OCSP Profile.....	<b>Error! Bookmark not defined.</b>
7.3.1	Version Number(s).....	<b>Error! Bookmark not defined.</b>
7.3.2	OCSP Extensions .....	<b>Error! Bookmark not defined.</b>
<b>8</b>	<b>COMPLIANCE AUDIT AND OTHER ASSESSMENTS .....</b>	<b>ERROR! BOOKMARK NOT DEFINED.</b>
8.1	Frequency or Circumstances of Assessment.....	<b>Error! Bookmark not defined.</b>
8.2	Identity/Qualifications of Compliance Assessor ...	<b>Error! Bookmark not defined.</b>
8.3	Assessor’s Relationship to Assessed Entity.....	<b>Error! Bookmark not defined.</b>
8.4	Topics Covered by Assessment .....	<b>Error! Bookmark not defined.</b>
8.5	Actions Taken as a Result of Deficiency .....	<b>Error! Bookmark not defined.</b>
8.6	Communications of Results .....	<b>Error! Bookmark not defined.</b>
<b>9</b>	<b>OTHER BUSINESS AND LEGAL MATTERS .....</b>	<b>ERROR! BOOKMARK NOT DEFINED.</b>
	<b>APPENDIX A: DERIVED CREDENTIAL ISSUANCE SERVICE ..</b>	<b>ERROR! BOOKMARK NOT DEFINED.</b>
A.1	Derived Credential Issuance Architecture .....	<b>Error! Bookmark not defined.</b>

A.1.1 Entrust IdentityGuard Server .....**Error! Bookmark not defined.**  
A.1.2 Derived Credential Revocation Server .....**Error! Bookmark not defined.**  
A.2 Roles .....**Error! Bookmark not defined.**  
A.2.1 MSO IDG Administrator .....**Error! Bookmark not defined.**  
A.2.2 MSO System Administrator.....**Error! Bookmark not defined.**  
A.2.3 Customer IdentityGuard Administrator .....**Error! Bookmark not defined.**  
A.2.4 Customer DCRS Administrator .....**Error! Bookmark not defined.**  
**APPENDIX B: REFERENCES..... ERROR! BOOKMARK NOT DEFINED.**

## RECORD OF CHANGES

<b>Version</b>	<b>Date</b>	<b>Author(s)</b>	<b>Reason</b>	<b>Description</b>
1.0	15 November 2017	MSO Policy Authority; I. J. Schoen	Final version	Initial Release
1.1	15 November 2017	MSO Policy Authority; I. J. Schoen	Received comments from review team	Minor updates to text; changed the pagination and updated TOC
1.1	6 December 2017	Patrick Garritty	Redaction for public distribution	Redaction of proprietary content

## **1. INTRODUCTION**

### **1.1 Overview**

The Entrust Managed Service Offering (MSO) Policy Authority (PA) has identified a need to issue Derived PIV Credentials to MSO customers in order to PIV-enable mobile devices in accordance with the guidance provided by [SP800-157]. The MSO will be offering this service as part of the Federal Shared Service Provider (FSSP) program, which issues PIV credentials to US government customers.

The PA has authorized the construction and deployment of dedicated Derived Credential Certification Authorities (CAs) and the necessary associated issuance systems to issue derived PIV credentials. The Derived Credential CAs are subordinate CAs that are subordinated to the current FSSP Root CA. Derived Credential FSSP CAs are limited to issuing derived PIV credentials to relying parties in accordance with [SP800-157], and any certificates required for the Derived Credential support components. Certificate issuance is predicated upon presentation of a PIV certificate to an issuing service; the resulting credential is thus ‘derived’ from the presented certificate.

#### **1.1.1 Certificate Practices Statement**

The practices described in this delta CPS are supplemental to the practices documented in the [CCPS-EMS-SSP].

The remaining sections contain sensitive proprietary information and have been redacted accordingly. Please contact your agency’s ISSO representative for any further information regarding the CPS.