WIDEPOINT

PERSONAL IDENTITY VERIFICATION SHARED SERVICE PROVIDER

CERTIFICATION PRACTICE STATEMENT SUMMARY

[WP-NC-PIVSSP-CPS-Summary]

Version 2.13

June 2, 2026

11250 Waples Mill Road
South Tower, Suite 210
Fairfax, VA 22030

Notice: Operational Research Consultants, Inc. (ORC), a wholly owned subsidiary of WidePoint Corporation, has changed its legal name to WidePoint Cybersecurity Solutions Corporation, hereafter referred to simply as WidePoint. This is a legal name change only for branding purposes with no change to ownership, corporation type, or other status. All references to "WidePoint" within this document refers specifically and only to WidePoint Cybersecurity Solutions Corporation, the wholly owned subsidiary of WidePoint Corporation, and not to WidePoint Corporation as a whole. Any reference or citing of personnel within this document, such as "WidePoint CEO", refers to the CEO of WidePoint Cybersecurity Solutions Corporation and not the CEO of WidePoint Corporation.

DOCUMENT SIGNATURE PAGE

Luther Eltinge Deyo III ORC9010002290.ID

Digitally signed by Luther Eltinge Deyo III ORC9010002290.ID
Date: 2026.06.03 10:19:06 -04'00'

Luther Deyo, WidePoint Vice President ICAM

Godfrey.Caroline.R.ORC302001 9041.ID

Digitally signed by Godfrey.Caroline.R.ORC30 20019041.ID
Date: 2026.06.03 12:24:51 -04'00'

Caroline Godfrey, WidePoint Chief Security Officer

Webb.Richard.David.ORC30200 00752.ID

Digitally signed by Webb.Richard.David.ORC3 020000752.ID
Date: 2026.06.03 09:35:51 -04'00'

Richard Webb, WidePoint Corporate Security Auditor

DOCUMENT REVISION HISTORY

Date	Version	Description of Change
1999-09-01	1.0	The initial ORC ACES Certificate Practice Statement (CPS) was the implementation document for the ORC ACES Program, submitted in accordance with GSA ACES: GS000T99ALD0007, under which ORC: ➢ Entering into an appropriate GSA ACES contract; ➢ Documented the specific practices and procedures implement to satisfy the requirements of the ACES Certificate Policy; and ➢ Successfully completed GSA's ACES Security Certification and Accreditation.
2000-02-10	2.0	This CPS version updated and replaced Version 1.0, to include contract modifications stipulated by the ACES PMO as a result of the Certification and Accreditation.
2000-05-10	2.1	This CPS version updated and replaced Version 2.0, to include the review and approval of Version 2.0 changes by the ACES PMO.
2000-11-20	3.0	This CPS version updated and replaced Version 2.0, to include updates stipulated by the ACES PMO as a result of the Federal Bridge Certificate Authority Policy.
2001-02-02	3.1	This CPS version updated and replaced Version 3.0, to include contract modifications stipulated by the ACES PMO as a result of the Federal Bridge Certificate Authority Policy compliance requirements.
2004-10-01	3.2	This CPS version updated and replaced Version 3.1, to include modifications stipulated by the Federal Bridge Certificate Authority Policy audit review.
2005-04-15	3.2.1	This CPS version updated and replaced Version 3.2, to include modifications necessary to comply with the U.S. Federal PKI Common Policy Framework (FPCPF).
2005-06-06	3.2.2	This CPS version updated and replaced Version 3.2.1, to include modifications necessary to comply with FPKI subcommittee comments.
2005-09-16	3.3	This CPS version updated and replaced Version 3.2.2, to include modifications necessary to comply with FPKI subcommittee comments and OCD review.
2007-01-09	3.3.1	This CPS version updated and replaced Version 3.3, to include modifications necessary to comply with the following Common Policy Change Proposals: 2005-03, Addition of High Assurance Policy to the Common Policy Framework, 13 September 2005 2006-01, Alignment of Common Authentication Policies with FIPS 201 And the X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program, V1.2, 5 January 2006.
2007-05-04	3.3.2	Updates concerning the report from the PKI Shared Service Provider Working Group on ORC, dated 23 April 2007
2015-08-14	4.0	Separation of Shared Service Provider CPS from ACES CPS so that both are stand-alone documents; addition of Derived PIV to SSP offering
2016-05-12	4.0.1	Updates and edits to address findings of FPKI review
2016-07-08	4.0.2	Updates and edits to address findings from Annual PKI Compliance Audit; updates in response to FPKI White Space Review; update corporate name to WidePoint.
2016-09-23	4.0.2.1	Follow-up edits addressing findings resulting from FPKI CPS to CP mapping review and white-space review
2017	4.0.2.2	Updates in response to annual audit, including recommended changes.
2022-08-18	2.2	Updated to align with Federal Public Key Infrastructure Policy Authority X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework Version 2.2, dated December 1, 2021. Version number reset to Version 2.2 to keep alignment with Common Policy.
2024-01-02	2.6	Updated to align with Federal Public Key Infrastructure Policy Authority X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework Version 2.6, dated November 3, 2023. Version numbering is tracked to Common Policy versioning.
2024-05-13	2.7	Updated to align with Federal Public Key Infrastructure Policy Authority X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework Version 2.7, dated May 13, 2024.
2025-05-05	2.10	Updated to include changes as directed by U.S. Federal PKI Common Policy Framework Versions 2.8 through 2.10.

2025-06-20	2.11	Updated to include changes as directed by U.S. Federal PKI Common Policy Framework Version 2.11.
2025-09-10	2.12	Updated to include changes as directed by U.S. Federal PKI Common Policy Framework Version 2.12. Incorporate Annual Audit review findings and discrepancies.
2026-06-02	2.13	Updated to include changes as directed by U.S. Federal PKI Common Policy Framework Version 2.13. Incorporate Annual Audit review findings and discrepancies for 2025.

TABLE OF CONTENTS

1 INTRODUCTION

This document, the WidePoint Personal Identity Verification Shared Service Provider Certification Practice Statement, hereafter referred to as the WidePoint PIV SSP CPS, defines and describes the operations of the WidePoint Personal Identity Verification Shared Service Provider, hereafter referred to as the WidePoint PIV SSP. The WidePoint PIV SSP is cross certified by the Federal Common Policy Certification Authority operated by the Federal PKI Management Authority, hereafter referred to as the Common Policy CA, to support the issuance of federally approved digital certificates. This WidePoint PIV SSP CPS governs the operation of the WidePoint PIV SSP which consists of all products, services, systems, and system components and is applicable to all agencies, external entities, organizations, individuals – U.S citizens and Foreign Nationals, and devices that will interact with the WidePoint PIV SSP for the purposes of requesting, receiving, using, and revoking digital certificates issued by the WidePoint PIV SSP to end-entities.

This WidePoint PIV SSP CPS details the rights, duties, and obligations of Relying Parties whose applications may allow access to their users who hold digital certificates issued by the WidePoint PIV SSP. This WidePoint PIV SSP CPS also advises of the policies, practices, and procedures that the WidePoint PIV SSP follows for requesting, issuing, validating, and revoking certificates issued by the WidePoint PIV SSP.

This WidePoint PIV SSP CPS is written to conform to the requirements and format of the Federal Public Key Infrastructure Policy Authority X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework Version 2.12, dated August 4, 2025, hereafter referred to as Common Policy. In the event of any policy discrepancies between Common Policy and the WidePoint PIV SSP CPS, Common Policy takes precedence.

Digital certificates issued under this WidePoint PIV SSP CPS identify the entity named in the certificate and bind that entity to a particular public/private key pair. This WidePoint PIV SSP CPS addresses requirements defined in the Common Policy CP for the issuance of digital certificates to Subscribers of the WidePoint PIV SSP. Subscribers of the WidePoint PIV SSP are defined as employees, affiliated contractors, and devices of federal agencies. However, these certificates are not restricted to the conduct of business with the U.S. Government and may be used to support secure communications and transactions within the Subscriber's organization or between other organizations.

The WidePoint PIV SSP is an infrastructure that provides secure authentication, confidentiality, integrity, technical non-repudiation, and logical and physical access control through the implementation of Public Key Infrastructure, referred to hereafter as PKI. The reliability and trust of the WidePoint PIV SSP is a direct result of the secure and trustworthy operation of the underlying PKI architecture to include all equipment, facilities, policy, procedure, practices, and personnel defined herein or through referenced documentation. The WidePoint PIV SSP implements the security and privacy controls as required by the Common Policy CP. Additionally, the WidePoint PIV SSP maintains a MODERATE baseline as defined by the National Institutes of Standards and Technology Special Publication 800-53 Revision 5 Security and Privacy Controls for Information Systems and Organizations, hereafter referred to as NIST SP 800-53, and implemented in the WidePoint System Security Plan. Additional controls beyond the MODERATE baseline may be implemented where applicable. In the case of conflicting security or privacy control requirements, the more secure method will be implemented.

The WidePoint PIV SSP provides the following security management services:

- Key Generation for public-private key pair based digital certificates for people and devices.
- Certificate creation, update, renewal, re-key, and distribution
- Escrow and recovery of private keys for digital encryption certificates.
- Certificate Revocation List (CRL) generation and distribution.
- On-line Certificate Status Protocol (OCSP) Service for certificate revocation status checking.
- Directory management of certificate related items.
- Secure token initialization, programming, and management.
- Device life cycle management.
- FIPS 201-3 Compliant PIV/PIV-I credential issuance systems.
- Privilege and authorization management; and
- System management functions (e.g., security audit, configuration management, archive, etc.).

The WidePoint PIV SSP CPS defines requirements on all activities to ensure the security of the following services:

- Subscriber identification and authorization verification.
- Control of computer and cryptographic systems.
- Physical access to facilities.
- Operation of computer and cryptographic systems.
- Usage of keys and public key certificates by Subscribers and Relying Parties; and
- Definition of rules to limit liability and to provide a high degree of certainty that the stipulations of this policy are being met.

Note: When discussing digital certificates and public key infrastructure, there can be some ambiguity introduced between what is called a certificate, what is called a credential and how do these things relate to a Level of Assurance. Often these words are used interchangeably which can create confusion for all concerned. For the purposes of this WidePoint PIV SSP CPS, the following descriptions are offered in the hopes of alleviating this confusion. Additional definitions or clarifying statements may appear later in the document where needed.

Level of Assurance – This term is described in Office of Management and Budget Memorandum E-Authentication Guidance for Federal Agencies (OMB M-04-04) and defines assurance as "*the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued*." Levels of Assurance as it pertains to Common Policy and this WidePoint PIV SSP CPS are further described in Section 1.4.1.1 of both documents.

Certificate – This term is used in this WidePoint PIV SSP CPS to describe a digital file (i.e., a digital certificate) that identifies the owner of that file and that ties the owner to a public key that is generated by the WidePoint PIV SSP. The level of assurance used in determining the identity of the entity that the certificate represents will be identified in the certificate. Various types of certificates may also be issued to perform different functions for the entity that is identified in the certificate. These certificate types are described further in Section 1.4.1 of this WidePoint PIV SSP CPS.

Credential – This term is often generically applied to almost any type of authenticator that can be used to grant access. Within this WidePoint PIV SSP CPS, this term is used to describe a form factor where a certificate may reside and that may increase security for the private key pair for that associated certificate and introduce additional functionalities for the holder of the certificate. There may be various credential types and form factors that may hold certificates. These credential types and their contents are described further in Section 1.4.1 and throughout this WidePoint PIV SSP CPS.

Note: Throughout this WidePoint PIV SSP CPS, the term "Applicant" may be used to describe a WidePoint PIV SSP Subscriber that is applying for a certificate issued by the WidePoint PIV SSP. An "Applicant" is a person or device that is applying for a certificate from the WidePoint PIV SSP. Once the "Applicant" has been approved for issuance of a certificate by the WidePoint PIV SSP, the "Applicant" will then become a Subscriber to the WidePoint PIV SSP. The use of the term "Applicant" throughout this WidePoint PIV SSP CPS will pertain to the time prior to approval for issuance by the WidePoint PIV SSP. The use of the term "Subscriber" will pertain to the time after approval for issuance by the WidePoint PIV SSP. In the case where WidePoint PIV SSP Subscribers are renewing their certificates (i.e., reapplying), the term "Subscriber" shall be used since they are a known entity to the WidePoint PIV SSP.

1.1 OVERVIEW

The WidePoint PIV SSP issues X.509 version 3 digital certificates in accordance with assurance levels as defined in Common Policy. The practices and procedures in this WidePoint PIV SSP CPS are applicable to individuals who manage the certificates, who directly use these certificates, who act as the human sponsor for devices, and individuals who are responsible for applications or servers that rely on these certificates.

The WidePoint PIV SSP has been established as a subordinate certification authority to the Common Policy CA.

This WidePoint PIV SSP CPS describes the operations and processes for the services that the WidePoint PIV SSP provides. These services include:

- Subscriber Registration
- Subscriber Validation
- Certificate Issuance
- Certificate Publishing
- Certificate Revocation
- Encryption Key Escrow
- Encryption Key Recovery
- Certificate Status Information

1.1.1 CERTIFICATE POLICY (CP)

This WidePoint PIV SSP Certification Practice Statement is subordinate to the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 2.12 dated August 4, 2025 and is not subordinate to any other Certificate Policy.

Certificates issued by the WidePoint PIV SSP CA contain a registered Certificate Policy OID, which may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. The Certificate Policy OID corresponds to the specific type and specific level of assurance for all WidePoint PIV SSP certificates issued under this WidePoint PIV SSP CPS, which are available to all Relying Parties. Each WidePoint PIV SSP certificate issued asserts the appropriate level of assurance in the certificatePolicies extension.

1.1.2 RELATIONSHIP BETWEEN THE COMMON POLICY CP AND THE WIDEPOINT PIV SSP CPS

This WidePoint PIV SSP CPS is subordinate to the FPCPF, Version 2.12 dated August 4, 2025. The FPCPF states what assurance can be placed in a certificate issued by the WidePoint PIV SSP CAs. This WidePoint PIV SSP CPS states how the WidePoint PIV SSP CA(s) establishes that assurance. The policies and procedures in this WidePoint PIV SSP CPS are applicable to individuals who manage the certificates, who directly use these certificates, and individuals who are responsible for applications or servers that rely on these certificates.

1.1.3 SCOPE

This WidePoint PIV SSP CPS is applicable to federal employees, contractors, and other affiliated personnel, relying parties, and agency applications who [that] directly use these certificates, and who are responsible for applications or servers that use certificates. Certificate users include, but are not limited to, Certificate Management Authorities (CMAs), Registration Authorities (RAs), Local Registration Authorities (LRAs) including Issuers, Registrars and Sponsors, subscribers, and relying parties.

1.1.4 INTEROPERATION WITH THE WIDEPOINT PIV SSP AND CERTIFICATE AUTHORITIES ISSUING UNDER DIFFERENT POLICIES

The FPKIPA determines the interoperability criteria for certificate authorities operating under the FPCPF. WidePoint PIV SSP CAs operate under the FPCPF.

1.2 DOCUMENT NAME AND IDENTIFICATION

The WidePoint PIV SSP operates in a manner consistent with the practices established in Common Policy. Common Policy designates certificate policy object identifiers (OIDs) that are registered under the Computer Security Objects Registry (CSOR) which is maintained by the National Institute of Standards and Technology (NIST).

Note: There are two meanings of certificate policy that may appear in this document. The Certificate Policy with capitalized first letters refers to the overarching document that governs the Common Policy Framework and is written and maintained by the Federal PKI Policy Authority as described in Section 1.3.1 of this WidePoint PIV SSP CPS. Whenever this is the intended use, this WidePoint PIV SSP CPS shall refer to the Certificate Policy as Common Policy. The other use case, certificate policy with lower case first letters is to define an object identifier (OID) value that allows Relying Parties to know the method in which the certificate that is presented to the Relying Party was issued. The certificate policy OID, which is embedded in every digital certificate issued by the WidePoint PIV SSP, identifies the Level of Assurance of the identity vetting processed performed, the private key protection that was employed when the key was generated. When addressing the requirements throughout this document, descriptions shall be specific to the certificate policy name that the requirement is addressing and not the more generic Level of Assurance unless it help to clarify the requirement for the reader.

The following table identifies the Common Policy certificate policy name, the certificate policy OIDs that may be asserted in digital certificates created by the WidePoint PIV SSP, and the Level of Assurance as defined in Section 1.4.1.4 of this WidePoint PIV SSP CPS that each one represents:

Certificate Policy Name	Certificate Policy Object Identifier	LOA
id-fpki-common-policy	2.16.840.1.101.3.2.1.3.6	Med
id-fpki-common-hardware	2.16.840.1.101.3.2.1.3.7	MHW
id-fpki-common-devices	2.16.840.1.101.3.2.1.3.8	Med
id-fpki-common-devicesHardware	2.16.840.1.101.3.2.1.3.36	Med
id-fpki-common-authentication	2.16.840.1.101.3.2.1.3.13	PIV
id-fpki-common-cardAuth	2.16.840.1.101.3.2.1.3.17	CA-PIV
id-fpki-common-piv-contentsigning	2.16.840.1.101.3.2.1.3.39	CS-PIV
id-fpki-common-derived-pivAuth	2.16.840.1.101.3.2.1.3.40	Med
id-fpki-common-derived-pivAuth-hardware	2.16.840.1.101.3.2.1.3.41	MHW
id-fpki-common-pivi-authentication	2.16.840.1.101.3.2.1.3.45	PIVI
id-fpki-common-pivi-cardAuth	2.16.840.1.101.3.2.1.3.46	CA-PIVI
id-fpki-common-pivi-contentSigning	2.16.840.1.101.3.2.1.3.47	CS-PIVI

where LOA = Level of Assurance, Med = Medium, MHW=Medium Hardware, PIV/PIVI = Authentication, CA-PIV/CA-PIVI = Card Authentication PIV/PIVI, CS-PIV/CS-PIVI = Content Signing PIV/PIVI

The WidePoint PIV SSP supports all certificate policies defined in the table above. The WidePoint PIV SSP CPS supports all of the OIDs defined in Common Policy, listed above.

Certificate Authority certificates issued to the WidePoint PIV SSP program will assert the certificate policies above for every certificate policy OID that that CA may issue.

The requirements associated with **id-fpki-common-pivi-authentication** are identical to **id-fpki-common-authentication**, with the exception of the need for a National Agency Check with Inquiries (NACI) and associated favorable adjudication. See Appendix A for additional comparisons between PIV and Common PIV-I credentials.

1.3 PKI PARTICIPANTS

The following section introduces the roles involved in issuing and maintaining public key certificates as part of the WidePoint PIV SSP.

WidePoint PIV SSP Certification Authorities, hereafter referred to as WidePoint PIV SSP CA(s), and WidePoint PIV SSP Registration Authorities, hereafter referred to as WidePoint PIV SSP RA(s), are considered the WidePoint PIV SSP Certificate Management Authorities, hereafter referred to as WidePoint PIV SSP CMA(s). This WidePoint PIV SSP CPS will use the term WidePoint PIV SSP CMA when a function may be assigned to either a WidePoint PIV SSP CA or a WidePoint PIV SSP RA or when a requirement and its implementation applies to both.

WidePoint PIV SSP Certificate Status Services, hereafter referred to as WidePoint PIV SSP CSA(s) that provide Online Certificate Status Protocol (OCSP) and Server-based Certificate Validation Protocol (SCVP) status responses are operated by the WidePoint PIV SSP and are also considered a part of a WidePoint PIV SSP CMA. All WidePoint PIV SSP CMA(s) are operated in compliance with this WidePoint PIV SSP CPS and Common Policy.

1.3.1 FEDERAL PKI POLICY AUTHORITY (FPKIPA)

The Federal Public Key Infrastructure Policy Authority (FPKIPA) is a sub-council comprised of U.S. Federal Government agency representatives and is chartered under the Federal Chief Information Security Officer (CISO) Council, under the Federal CIO Council. The FPKIPA owns this certificate policy and represents the interest of the Federal CIOs and Federal CISOs.

The FPKIPA is responsible for:

- Maintaining the Common Policy CP,
- Approving this WidePoint PIV SSP CPS that issues certificates under Common Policy,
- Approving the compliance audit report for the WidePoint PIV SSP issuing certificates under Common Policy, and
- Ensuring continued conformance of WidePoint PIV SSP that issues certificates under Common Policy with applicable requirements as a condition for allowing continued participation.

1.3.2 WIDEPOINT CERTIFICATION AUTHORITIES

The WidePoint PIV SSP is issued a cross-certificate by the Common Policy CA for each WidePoint PIV SSP issue certificate authority. Each WidePoint PIV SSP CA encompasses all component parts which may be on the same hardware/software system or an integrated set of hardware and software within the control of the WidePoint PIV SSP security boundary. Each WidePoint PIV SSP CA generates certificates in accordance with this WidePoint PIV SSP CPS and in compliance with the certificate profiles described in Section 10. Each WidePoint PIV SSP CA manages the life-cycle of its issued certificates to include issuance, escrow, publication, renewal, expiration, revocation, and recovery in accordance with the stipulations of the WidePoint PIV SSP CPS. Each WidePoint PIV SSP Certificate Authority is responsible for issuing and managing certificates including:

- The certificate manufacturing process
- Publication of certificates
- Revocation of certificates
- Generation and destruction of WidePoint PIV SSP Certificate Authority signing keys
- Ensuring that all aspects of the WidePoint PIV SSP Certificate Authority services, operations, and infrastructure related to certificates issued under this WidePoint PIV SSP CPS are performed in accordance with the requirements, representations, and warranties of this WidePoint PIV SSP CPS.

Each WidePoint PIV SSP CA is governed by this WidePoint PIV SSP CPS and the WidePoint System Security Plan.

Each WidePoint PIV SSP CA is assigned a WidePoint Asset Identification as described in the WidePoint Configuration Management Plan Section 3.1.1 Asset Identification which is used to track each WidePoint PIV SSP CA throughout its lifecycle. WidePoint assigns an asset identification code to all systems (host, virtual machines, appliances, etc.) and applies the operational and technical security controls described in this WidePoint PIV SSP CPS, as well as additional controls described in the WidePoint System Security Plan, to all system software layers.

1.3.3 WIDEPOINT REGISTRATION AUTHORITIES

WidePoint Registration Authorities are entities that enter into an agreement with the WidePoint PIV SSP for the purpose of collecting and submitting digitally signed verification of Applicant and WidePoint PIV SSP Subscriber identities and information to be entered into public key certificates. WidePoint Registration Authorities are

required to perform their functions in accordance with this WidePoint PIV SSP CPS which is approved by the WidePoint PIV SSP and the FPKIPA. WidePoint Registration Authorities register Applicants and WidePoint PIV SSP Subscribers, approve certificate issuance, and perform key recovery operations. WidePoint Registration Authorities are further separated into various roles to perform a subset of the Registration Authority functions. These WidePoint PIV SSP roles are listed below with the functions performed by each and if they are a human or device entity. WidePoint Registration Authorities may assume the following roles:

- WidePoint Registration Authorities issue and revoke certificates that assert all certificate policies identified in Section 1.2 of this WidePoint PIV SSP CPS;
- WidePoint Registrars perform the registration process associated with WidePoint PIV SSP PIV and PIV-I credentials and approve Applicants and WidePoint PIV SSP Subscribers credential requests for issuance of a WidePoint PIV SSP PIV or PIV-I credential to an Applicant or WidePoint PIV SSP Subscriber;
- WidePoint Issuers reaffirm the identity of the WidePoint PIV SSP Subscriber who has been approved for issuance of a WidePoint PIV SSP PIV or PIV-I credential by a WidePoint Registrar and authorize and witness the key generation of the WidePoint PIV SSP PIV or PIV-I credential to the WidePoint PIV SSP Subscriber; and
- WidePoint Key Recovery Agents recover escrowed keys in accordance with the stipulations of this WidePoint PIV SSP CPS.

WidePoint Registration Authorities may delegate the identity proofing tasks associated with Trusted Agents to WidePoint Local Registration Authorities who have been approved by the WidePoint PIV SSP and trained by a WidePoint Registration Authority on the processes of identity verification and authorization tasks. WidePoint Local Registration Authorities may be employees of WidePoint PIV SSP Subscriber organizations. A WidePoint Local Registration Authority may also serve as a WidePoint Key Recovery Official who may process requests for key recovery by WidePoint PIV SSP Subscribers or third-party requestors and forward those requests to WidePoint Registration Authorities.

A Trusted Agent is authorized to act as a representative of the WidePoint PIV SSP in providing Applicant or WidePoint PIV SSP Subscriber identity verification during the registration process which includes identity proofing, as well as witness and acknowledgment functions. Trusted Agents do not have any privileged or automated access to WidePoint PIV SSP CAs or any WidePoint PIV SSP CMA system or function. Trusted Agents are not Trusted Roles; however, the WidePoint PIV SSP shall document any Trusted Agent authorization requirements to include:

- trustworthiness vetting, and
- training or government appointment (e.g., notary public).

All identity proofing audit artifacts produced by a Trusted Agent shall be traceable to an individual.

1.3.4 KEY RECOVERY AUTHORITIES

The WidePoint PIV SSP has implemented Key Recovery with the applicable requirements for physical, personnel, and procedural security controls, technical security controls, and Compliance Audit applied as follows:

- WidePoint PIV SSP Certificate Authority requirements are applied to all WidePoint Key Escrow Databases and to all WidePoint PIV SSP Data Decryption Servers (if applicable)
- WidePoint Registration Authority requirements are applied to the WidePoint Key Recovery Agent and WidePoint Key Recovery Agent automated systems

1.3.4.1 WidePoint Key Escrow Database

A WidePoint Key Escrow Database is defined as the function, system, or subsystem that maintains the key escrow repository and responds to key registration requests. A WidePoint Key Escrow Database also responds to key recovery requests from two or more KRAs or self-recovery by a current subscriber.

Section 5.2.1.2 contains the description of trusted roles required to operate the A WidePoint Key Escrow Database.

1.3.4.2 Data Decryption Server

A WidePoint PIV SSP Data Decryption Server is an automated system that has the capability to obtain subscriber private keys from the WidePoint PIV SSP Key Escrow Database or another WidePoint PIV SSP Data Decryption

Server for data monitoring or other purposes (e.g., email inspection). WidePoint PIV SSP Data Decryption Servers do not provide keys to WidePoint PIV SSP Subscribers or other Third-Party Requestors. A WidePoint PIV SSP Data Decryption Server has access to escrowed key management keys and must meet all security requirements of the KED as outlined in this policy.

Implementation of a WidePoint PIV SSP Data Decryption Server is optional based on customer agency requirements. As of this publication of the WidePoint PIV SSP CPS, no WidePoint PIV SSP Data Decryption Server is operated by the WidePoint PIV SSP or any of WidePoint's customer agencies.

1.3.4.3 WidePoint Key Recovery Agent

A WidePoint Key Recovery Agent is an appointed and trusted individual who, using a two-party control procedure with a second WidePoint Key Recovery Agent, is authorized to interact with the WidePoint PIV SSP Key Escrow Database in order to extract an escrowed decryption private key. WidePoint Key Recovery Agents have high-level sensitive access to the WidePoint PIV SSP Key Escrow Database and are considered Trusted Roles (see Section 5.2.1). Registration Authorities (RA) as defined in the WidePoint Shared Service Provider Certificate Policy may fill the role of KRA; however, because KRAs can recover large number of keys, the number and location of WidePoint Key Recovery Agents are tightly controlled without limiting the ability to recover or operate. The WidePoint PIV SSP may allow WidePoint PIV SSP Subscriber organizations to designate non-WidePoint employees to fulfill the role of WidePoint Key Recovery Agent with the stipulation that those WidePoint Key Recovery Agents may recover keys of WidePoint PIV SSP Subscribers only from the Organization/Enterprise by which that Key Recovery Agent is employed.

A WidePoint PIV SPP Key Recovery Agent performs the following functions:

- Confirm validity and completeness of requests,
- Recover copies of escrowed keys; and
- Distribute copies of recovered keys to Requestor, with protection as described in Section 4.12.1.3.

WidePoint PIV SSP Key Recovery Agents may conduct requestor identity verification and authorization when WidePoint Key Recovery Officials are not used.

1.3.4.4 WidePoint Key Recovery Official

A WidePoint Key Recovery Official may optionally be used to support identity verification and authorization validation tasks; however, a WidePoint Key Recovery Official is not a Trusted Role.

A KRO's responsibilities are to perform the following functions:

- Verify a Requestor's identity and authorization as stated by this policy;
- Assist authorized requestors in building key recovery requests;
- Utilize secure communication for key recovery requests to and responses from the KRA; and
- Participate in the distribution of escrowed keys to the Requestor, ensuring that it occurs as described by the associated practice statement (CPS or KRPS).

Practice Note: The responsibilities of the Key Recovery Official do not require access to the WidePoint PIV SSP Key Encryption Databases and as a result the WidePoint PIV SSP Key Recovery Official is not considered a Trusted Role. However, the WidePoint PIV SSP may assign multiple responsibilities to one person due to resource constraints. In scenarios where Trusted Roles may also be assigned to perform the duties of the WidePoint PIV SSP Key Recovery Official, the requirements for Separation of Duties per Section 5.2.4 must be enforced.

1.3.5 KEY RECOVERY REQUESTORS

A Requestor is the person who requests the recovery of decryption private key(s). A Requestor is generally the WidePoint PIV SSP Subscriber, a third-party from the WidePoint PIV SSP Subscriber's organization (e.g., supervisor,

corporate officer) or a law enforcement officer who is authorized to request recovery of a WidePoint PIV SSP Subscriber's escrowed key. Any individual who can demonstrate a reasonably verifiable authority in accordance with the WidePoint PIV SSP Subscriber's organization information access and release policy and need to obtain a recovered key can be considered a Requestor.

1.3.5.1 Internal Third-Party Requestor

An Internal Third-Party Requestor is any Requestor who is in the WidePoint PIV SSP Subscriber's supervisory chain or otherwise authorized to obtain the WidePoint PIV SSP Subscriber's key from the WidePoint PIV SSP Key Encryption Database. A list of personnel authorized to make such a request is provided to the WidePoint PIV SSP by the WidePoint PIV SSP Subscriber's organization with those personnel designated as WidePoint PIV SSP Key Recovery Officials.

1.3.5.2 External Third-Party Requestor

An external Requestor is someone (e.g., investigator) outside the WidePoint PIV SSP Subscriber's organization with an authorized court order or other legal instrument to obtain the decryption private key of the WidePoint PIV SSP Subscriber. An External Third-Party Requestor must submit the key recovery request via a signed court order or other legal instrument to the WidePoint PIV SSP that clearly and uniquely identifies the WidePoint PIV SSP Subscriber. Nothing in this document is intended to change the current procedures for obtaining information about individuals in connection with such requests. WidePoint PIV SSP and the WidePoint PIV SSP Subscriber's organizations will appoint authorized personnel and implement this WidePoint PIV SSP CPS so that the existing organization policy regarding release of sensitive information can be met.

1.3.6 WIDEPOINT PIV SSP SUBSCRIBERS

A WidePoint PIV SSP Subscriber is an entity whose name appears as the subject in a certificate issued by the WidePoint PIV SSP, and who asserts that they will use the key and the associated certificate in accordance with this WidePoint PIV SSP CPS. Subscribers to the WidePoint PIV SSP are limited to the following categories of entities:

- Federal employees, contractors, affiliated personnel; and
- Devices such as workstations, guards and firewalls, routers, trusted servers (e.g., database, FTP, and WWW), and other infrastructure components that are devices operated by or on behalf of federal agencies.

There is a subset of Human WidePoint PIV SSP Subscribers who will be issued role-based certificates. These certificates identify a specific role on behalf of which the WidePoint PIV SSP Subscriber or "private key holder" is authorized to act rather than the WidePoint PIV SSP Subscriber's name. These certificates are issued in the interest of supporting accepted business practices. The role-based certificate can be used in situations where non-repudiation is desired. Normally, role-based certificates will be issued in addition to an individual WidePoint PIV SSP Subscriber certificate. A specific role may be identified in signing certificates issued to multiple WidePoint PIV SSP Subscribers; however, the key pair will be unique to each individual role-based signature certificate. For example, there may be four individuals with a certificate issued in the role of "General Counsel, DHS." However, each of the four certificates will have unique keys and certificate serial numbers. A specific example of a role-based certificate may be a delegated digital signature certificate that is issued to private key holder(s) who have been delegated the authority to sign documents on behalf of a "role holder" who is another individual assigned or appointed to a role that has unique authorization (e.g., "Secretary of Commerce," who has the authority to provide official submissions to the Office of the Federal Register). Roles Delegated digital signature certificates, are limited to those roles that are held by a unique individual within an organization (e.g., Chief Information Officer, GSA is a unique individual whereas Program Analyst, GSA is not).

Practice Note: In many cases a Role-Based certificate may be authorized for the individual(s) assigned to that role, in which case the role holder and the private key holder(s) are the same person. Delegated digital signature certificates are the only instance where an authorized private key holder is a different individual than the role holder named in the subjectDN. In these instances, private key holder traceability is maintained via unique identifiers asserted in the Subject Alternative Name extension."

Another category of subscriber certificates includes group key management keys and certificates, also known as group encryption certificates. These private encryption keys and certificates facilitate scenarios where multiple individuals, using a shared private key, have the ability to decrypt information that was encrypted using one public key (e.g., group email address).

1.3.7 RELYING PARTIES

A Relying Party is an entity who, by using another's WidePoint PIV SSP Subscriber certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate, relies on the validity of the binding of that WidePoint PIV SSP Subscriber's name to a public key. A Relying Party may use information in the certificate (such as certificate policy object identifiers) to determine the suitability of the certificate for a particular use and does so at their own risk.

1.3.8 OTHER PARTICIPANTS

Participating agencies under this WidePoint PIV SSP CPS identify the Agency Points of Contact and shall act as liaisons to the WidePoint PIV SSP and the FPKIPA.

1.3.8.1 WidePoint PIV SSP Card Management Systems

Each WidePoint PIV SSP Card Management System, hereafter referred to as a WidePoint PIV SSP CMS, is authorized by the WidePoint PIV SSP to process, issue, and revoke WidePoint PIV SSP PIV or PIV-I credentials, which contain printed card elements, certificates asserting a certificate policy of **id-fpki-common-authentication**, **id-fpki-common-cardAuth**, **id-fpki-common-hardware, and id-fpki-common-policy** in the case of a PIV credential or **id-fpki-common-pivi-authentication**, **id-fpki-common-pivi-cardAuth**, **id-fpki-common-hardware, and id-fpki-common-policy** in the case of a PIV-I credential and their private keys including previous encryption keys, and other data objects including digitally signed biometrics in accordance with Common Policy, the WidePoint PIV SSP CPS, and the FIPS 201-3 Personal Identity Verification (PIV) of Federal Employees and Contractors and referenced NIST Special Publication Guidance documents. Each WidePoint PIV SSP CMS is authorized by the WidePoint PIV SSP through the issuance of a content signing certificate that asserts a certificate policy of **id-fpki-common-piv-contentSigning** for a WidePoint PIV SSP CMS that issues PIV credentials or a content signing certificate that asserts a certificate policy of **id-fpki-common-pivi-contentSigning** for a WidePoint PIV SSP CMS that issues PIV-I credentials by a WidePoint PIV SSP CA. Each WidePoint PIV SSP CMS's content signing certificate is used by the WidePoint PIV SSP CMS to digitally sign data elements on WidePoint PIV SSP PIV or PIV-I credentials. Each WidePoint PIV SSP CMS is also issued a connector certificate with assigned privileges on the corresponding WidePoint PIV SSP CA for requesting certificate issuance and revocation. Each WidePoint PIV SSP CMS is considered a WidePoint PIV SSP Registration Authority and adheres to all the requirements specified for WidePoint PIV SSP Registration Authorities in this WidePoint PIV SSP CPS. Additionally, privileged users of a WidePoint PIV SSP CMS who can direct the WidePoint PIV SSP CMS to perform certificate related actions are considered to be WidePoint PIV SSP Registration Authorities, as described in Section 1.3.4 of this WidePoint PIV SSP CPS.

Each WidePoint PIV SSP CMS is assigned a WidePoint Asset Identification as described in the WidePoint Configuration Management Plan Section 3.1.1 Asset Identification which is used to track each WidePoint PIV SSP CMS throughout its lifecycle.

1.3.8.2 WidePoint PIV SSP PKI Sponsor

A WidePoint PIV SSP PKI Sponsor fills the role of a WidePoint PIV SSP Subscriber for non-human system components and organizations that are named as public key certificate subjects of WidePoint PIV SSP issued certificates. A WidePoint PIV SSP PKI Sponsor works with the WidePoint PIV SSP and, when appropriate, WidePoint PIV SSP Trusted Agents, to register components (routers, firewalls, etc.) in accordance with Section 3.2.3.3 of this WidePoint PIV SSP CPS and is responsible for meeting the obligations of Subscribers as defined throughout. A WidePoint PIV SSP PKI Sponsor is not considered a trusted role as defined in Section 5.2 of this WidePoint PIV SSP CPS.

1.3.8.3 WidePoint PIV SSP Agency PKI Point of Contact

A WidePoint PIV SSP PKI Agency Point of Contact is a representative(s) of the WidePoint PIV SSP Customer Agency that are governed by this WidePoint PIV SSP CPS and shall provide their Point of Contact information to the WidePoint PIV SSP and the Federal PKI Policy Authority. The WidePoint PIV SSP PKI Agency Point of Contact serves as the organization's WidePoint PIV SSP Key Recovery Official.

1.3.8.4 Other Authorities

1.3.8.4.1 WidePoint Corporate Security Auditor

WidePoint Corporate Security Auditors ensure that compliance audits as stipulated in this WidePoint PIV SSP CPS and the WidePoint System Security Plan are independently administered. WidePoint Corporate Security Auditors act as independent assessors and are outside the reporting chain of any role or person identified in this WidePoint PIV SSP CPS or the WidePoint System Security Plan. Additionally, WidePoint Corporate Security Auditors do not have any personnel or roles that report to them other than other WidePoint Corporate Security Auditors. WidePoint Corporate Security Auditors are designated directly by the WidePoint Chief Executive Officer.

WidePoint Corporate Security Auditors also coordinate and support external auditing, as described in Section 8 of this WidePoint PIV SSP CPS, including aperiodic audits. Audits of the WidePoint PIV SSP will follow the guidelines and specifications of currently accepted standards and practices, as approved by the FPKIPA.

1.3.8.4.2 External Independent Compliance Auditor

The WidePoint PIV SSP retains a nationally recognized firm with expertise in IT Security Auditing and Evaluation as an external independent compliance auditor. The external auditing firm is an industry leader with focus on the design, implementation and operation of information assurance systems and the technologies that enable and support the implementation of information security services.

1.4 CERTIFICATE USAGE

1.4.1 APPROPRIATE CERTIFICATE USES

The WidePoint PIV SSP is intended to support the following security services: *confidentiality, integrity, authentication,* and *technical non-repudiation*. The WidePoint PIV SSP supports these security services by providing identification and authentication, integrity, technical non-repudiation through digital signatures, and confidentiality through key exchange. These basic security services support the long-term integrity of application data but may not by themselves provide a sufficient integrity solution for all application circumstances. For example, when a requirement exists to verify the authenticity of a signature beyond the certificate validity period, such as contracting, other services such as trusted archival services or trusted timestamp may be necessary. These solutions are application based and must be addressed by WidePoint PIV SSP Subscribers and Relying Parties. The WidePoint PIV SSP provides support of security services to a wide range of applications that protect various types of information, up to and including sensitive unclassified information.

Certificates issued by the WidePoint PIV SSP may be used for authentications to federal systems as well as key management, signature, and confidentiality requirements for federal government processes. Additionally, certificates issued by the WidePoint PIV SSP are intended to support use cases involving unclassified information, which can include sensitive unclassified data protected pursuant to federal statutes and regulations. The

WidePoint PIV SSP offers various digital certificate types (i.e., certificates that perform a specific function) to promote these security services. The WidePoint PIV SSP issues certificates to WidePoint PIV SSP Subscribers that assert one of the certificate policy object identifiers specified in Section 1.2 of this WidePoint PIV SSP CPS. Enrollment processes differ depending upon the type of certificate that is requested and the Level of Assurance, as specified in Section 1.4.1.4 of this WidePoint PIV SSP CPS, which is required. The WidePoint PIV SSP issues the following certificate types:

Signature Certificates *– This certificate type, sometimes referred to as an identity certificate, is issued to a WidePoint PIV SSP Subscriber as a means for the WidePoint PIV SSP Subscriber to identify themselves electronically to applications and other people. The Identity Certificate type uniquely identifies the WidePoint PIV SSP Subscriber and allows for the WidePoint PIV SSP Subscriber to present this certificate to webservers and applications as a means of authentication. Additionally, the identity certificate type can be used to sign documents and email to promote integrity and ensure that the signed document or a signed email originated from the holder of the signature certificate and that its content has not been altered. Signature certificates assert non-repudiation in the key usage extension which means that a copy of the private key associated with this certificate is not in the possession of anyone other than the WidePoint PIV SSP Subscriber.*

Encryption Certificates *– This certificate type is issued to a WidePoint PIV SSP Subscriber as a means for the WidePoint PIV SSP Subscriber to encrypt/decrypt documents and emails. The encryption certificate is a complimentary certificate to the Identity certificates and is issued to a WidePoint PIV SSP Subscriber whenever they receive a signature certificate. Encryption certificates are escrowed as part of the issuance process of the WidePoint PIV SSP to facilitate self-recovery and third-party recovery and may only assert the certificate policy object identifier of* ***id-fpki-common-policy****. Encryption certificates do not assert the key-usage of non-repudiation.*

Derived Certificates *– This certificate type is issued to a WidePoint PIV SSP Subscriber based on proof of possession and control of a PIV credential. Derived PIV certificates are typically used in situations that do not easily accommodate a PIV Card, such as in conjunction with mobile devices. Derived certificates are issued in accordance with this WidePoint PIV SSP CPS and following the guidance as defined in NIST SP 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials.*

Device Certificates *– This certificate type, sometimes referred to as a component certificate, is issued to a variety of devices so that those devices can identify themselves electronically and securely encrypt communications to applications, devices, and people. This certificate type may be used for webserver communications, domain controllers, virtual private networks (VPNs), firewalls and routers, computers, mobile devices, etc. The certificate for each use case listed may have unique attributes encoded in various fields of the certificate such as the Extended Key Usage field or other fields that a particular application (i.e., domain controllers) may require.*

OCSP Signing Certificates *– This certificate type is only issued to a WidePoint PIV SSP CSA, as described in Section 1.3 of this WidePoint PIV SSP CPS, to sign the On-line Certificate Status Protocol (OCSP) responses that provide revocation status on all types of certificates issued by the WidePoint PIV SSP. An OCSP Signing Certificate identifies the name of the WidePoint PIV SSP CSS that is providing the OCSP response, has a key usage of non-repudiation and digital signature, and must have its private key generated in a FIPS 140-3 Level 2 compliant hardware security module. Additionally, this certificate asserts all the same certificate policies as identified in Section 1.2 as the WidePoint PIV SSP CA that signed it.*

The following certificate types are specific to the WidePoint PIV SSP PIV-I Credential which is defined immediately after this section of certificate types.

Authentication Certificates – *This certificate type identifies the WidePoint PIV SSP Subscriber to whom a WidePoint PIV SSP PIV or PIV-I credential was issued and can only be issued to and whose private key can only exist within a WidePoint PIV SSP PIV-I Credential. This certificate ties the WidePoint PIV SSP Subscriber*

to the physical card that constitutes the physical aspect of the WidePoint PIV SSP PIV or PIV-I Credential through data elements embedded in the digital certificate. This certificate is meant to promote electronic authentication to logical access systems such as webservers and smart card logon to operating systems, among others. This certificate does not assert non-repudiation and should not be used to perform digital signing.

***Card Authentication Certificates** – This certificate type is only issued to a WidePoint PIV SSP PIV or PIV-I Credential and uniquely identifies the FIPS 201-3 compliant card that holds the WidePoint PIV SSP issued card authentication certificate. This certificate type does not contain any Personally Identifiable Information (PII) data about the WidePoint PIV SSP Subscriber to whom the WidePoint PIV SSP PIV or PIV-I credential is issued. Additionally, this certificate is not protected by a PIN or password combination and is allowed to be accessed by proximity readers to promote physical access capabilities.*

***Content Signing Certificates** - This certificate type is only issued to a WidePoint PIV SSP CMS, as described in Section 1.3.3 of this WidePoint PIV SSP CPS, to sign the data elements (i.e. the content) that is captured during the issuance process for a WidePoint PIV SSP PIV or PIV-I Credential and that will be stored on the credential. This certificate type identifies the name of the WidePoint PIV SSP CMS that controls the issuance process for WidePoint PIV SSP PIV or PIV-I credentials. This certificate has a key usage of digital signature and is only used to sign the data elements on the WidePoint PIV SSP PIV-I Credential and must have its private key generated in a FIPS 140-3 Level 2 compliant hardware security module. No other use of this certificate type is permitted.*

Within the WidePoint PIV SSP program, a credential is used to describe a form factor that contains certificate types as described above and provides additional security and may provide additional functionality such that the WidePoint PIV SSP Subscriber to whom the credential is issued can maximize the credential's usage. The following credentials are defined as being available to Applicants and WidePoint PIV SSP Subscribers as part of the WidePoint PIV SSP program. The credential types described may or may not have a direct correlation to Common Policy but are used to define a package that contains elements that do have a direct correlation. Additionally, an Applicant or a WidePoint PIV SSP Subscriber will receive at least an identity certificate and an encryption certificate in most cases for human end-entities. These certificates combined with a cryptographic token constitute the minimum extent of a WidePoint PIV SSP credential. The credential types that the WidePoint PIV SSP offers are defined below.

***Medium Hardware Credential –** This credential consists of a FIPS 140-3 Level 2 cryptographic token (i.e., a smart card or USB crypto token) that contain an identity certificate that asserts a certificate policy of **id-fpki-common-hardware** and an encryption certificate that asserts a certificate policy of **id-fpki-common-policy**. The identity proofing performed for the Hardware Credential is consistent with the identity vetting requirements for Medium Hardware Level of Assurance as defined in Section 1.4.1.4 of this WidePoint PIV SSP CPS.*

***PIV Credential –** This credential consists of a FIPS 201-3 compliant smart card that contain four (4) certificate types described above: a card authentication certificate that asserts the certificate policy of **id-fpki-common-cardAuth**, an authentication certificate that asserts the certificate policy of **id-fpki-common-authentication**, an identity certificate that asserts the certificate policy of **id-fpki-common-hardware** and an encryption certificate that asserts a certificate policy of **id-fpki-common-policy**. WidePoint PIV SSP PIV Credentials may only be issued through the WidePoint PIV SSP CMS which is configured to follow the PIV issuance process as specified in FIPS 201-3. As part of this enrollment process, an Applicant or WidePoint PIV SSP Subscriber's biometric data is captured and is written to the FIPS 201-3 compliant smart card to promote additional factors of authentication for the WidePoint PIV SSP PIV Credential holder. The biometric data is signed by a WidePoint PIV SSP Content Signing certificate to ensure the integrity of the biometric data and is protected from use by a PIN selected by and only know to the Applicant or the WidePoint PIV SSP Subscriber. Additional features of the WidePoint PIV SSP PIV credential include internal*

antennae for use with proximity readers as well as printed elements on the credential to facilitate visual recognition. Escrowed encryption keys that were previously issued to the WidePoint PIV SSP Subscriber as part of a previous WidePoint PIV SSP PIV Credential issuance are also recovered to the new WidePoint PIV SSP PIV Credential for decrypting previously encrypted information by the WidePoint PIV SSP Subscriber.

PIV-I Credential – *This credential consists of a FIPS 201-3 compliant smart card that contain four (4) certificate types described above: a card authentication certificate that asserts the certificate policy of **id-fpki-common-pivi-cardAuth**, an authentication certificate that asserts the certificate policy of **id-fpki-common-pivi-authentication**, an identity certificate that asserts the certificate policy of **id-fpki-common-hardware** and an encryption certificate that asserts a certificate policy of **id-fpki-common-policy**. WidePoint PIV SSP PIV-I Credentials may only be issued through the WidePoint PIV SSP CMS which is configured to follow the PIV-I issuance process as specified in FIPS 201-3. As part of this enrollment process, an Applicant or WidePoint PIV SSP Subscriber's biometric data is captured and is written to the FIPS 201-3 compliant smart card to promote additional factors of authentication for the WidePoint PIV SSP PIV-I Credential holder. The biometric data is signed by a WidePoint PIV SSP Content Signing certificate to ensure the integrity of the biometric data and is protected from use by a PIN selected by and only know to the Applicant or the WidePoint PIV SSP Subscriber. Additional features of the WidePoint PIV SSP PIV-I credential include internal antennae for use with proximity readers as well as printed elements on the credential to facilitate visual recognition. Escrowed encryption keys that were previously issued to the WidePoint PIV SSP Subscriber as part of a previous WidePoint PIV SSP PIV-I Credential issuance are also recovered to the new WidePoint PIV SSP PIV-I Credential for decrypting previously encrypted information by the WidePoint PIV SSP Subscriber.*

Elevated Privileges Credential – *This credential is a companion credential to a WidePoint PIV SSP Subscriber who holds an existing WidePoint PIV SSP Medium Hardware, or PIV-I Credential. This credential, sometimes referred to as an EP Credential, consists of a single identity certificate that may assert a certificate policy of **id-fpki-common-hardware**. This is typically for Systems Administrators or other personnel who have privileged rights on a system or systems. When a WidePoint PIV SSP Subscriber uses their primary credential to authenticate to their network (i.e., Microsoft Windows Domain Controller) they are granted the privileges associated with their primary account. The WidePoint PIV SSP Subscriber would need to then authenticate again to receive the privileges to administer the system. Since the primary credential is already in use and authenticate as their base account, the Elevated Privileges Credential is used to authenticate in order to receive these administrative privileges.*

A single solution providing support to every application would appear to be desirable but because of different legal, security and national policy requirements for protection of the different categories of information, the most cost-effective solution is one that supports multiple certificate type functionality, issued at multiple levels of assurance utilizing credentials that add to its security and functionality.

Applicability statements in Common Policy are provided as guidance; applications and Relying Parties may require different levels of assurances.

1.4.1.1 Level of Assurance

The Level of Assurance associated with a public key certificate is an assertion by the WidePoint PIV SSP of the degree of confidence that a Relying Party may reasonably place in the binding of a WidePoint PIV SSP Subscriber's public key to the identity and privileges asserted in the certificate. Assurance level depends on the proper registration of WidePoint PIV SSP Subscribers and the proper generation and management of the certificate and associated private keys, in accordance with the stipulations of this WidePoint PIV SSP CPS. Personnel, physical, procedural, and technical security controls, as described in this WidePoint PIV SSP CPS, are used to maintain the assurance level of the certificates issued by the WidePoint PIV SSP.

1.4.1.2 Factors in determining usage

The amount of reliance a Relying Party chooses to place on the certificate issued by the WidePoint PIV SSP will be determined by various risk factors. Specifically, the value of the information, the threat environment, and the existing protection of the information environment are used to determine the appropriate level of assurance of certificates required to protect and authenticate the information.

1.4.1.3 Threat

Threat is any circumstance or event with the potential to cause harm. In terms of information systems, harm includes destruction, disclosure, or modification of data, processes, or processing components. Threats to systems include environmental disasters, physical damage, system penetration, and violation of authorization, human error, and communications monitoring or tampering.

1.4.1.4 General Usage

This section contains definitions for Levels of Assurance addressed in this WidePoint PIV SSP CPS, and guidance for their application. The guidance is based on the previous discussion of information value and environmental protection. Emphasis is placed on two types of activity: integrity and access control to information considered sensitive, and information related to electronic financial transactions and other e-commerce. The final selection of the security mechanisms and level of strength and assurance requires a risk management process that addresses the specific mission and environment. Each Relying Party is responsible for carrying out this risk analysis. The Level of Assurances defined here are derived from Common Policy. Additional detail has been added to identify the security benefits of each Level of Assurance.

Medium Assurance: This Level of Assurance indicates to Relying Parties that the WidePoint PIV SSP Subscriber may have generated the key for their identity certificate request prior to the identity proofing being performed (i.e. the key generation was not witnessed) and that the private key may not be generated in a non-exportable token (i.e. an operational backup copy of the private key may be made)**.** Medium Assurance also applies to all device certificates issued by the WidePoint PIV SSP regardless of where the key generation took place for the private-key of the device (i.e., in the application cryptographic store or on a hardware security module. Medium Assurance certificates issued by the WidePoint PIV SSP can only assert the certificate policy value of **id-fpki-common-policy** for human WidePoint PIV SSP Subscribers and a certificate policy value of **id-fpki-common-devices** or **id-fpki-common-devicesHardware**. Medium Assurance is intended for applications handling sensitive medium value information based on the Relying Party's assessment, with the exception of transactions involving issuance or acceptance of contracts and contract modifications. Examples of medium assurance applications include:

- Non-repudiation for small and medium value financial transactions other than transactions involving issuance or acceptance of contracts and contract modifications
- Authorization of payment for small and medium value financial transactions
- Authorization of payment for small and medium value travel claims
- Authorization of payment for small and medium value payroll
- Acceptance of payment for small and medium value financial transactions

Medium Hardware Assurance: This Level of Assurance meets the same conditions and expectation for use as the Medium Level of Assurance with the exception that the WidePoint PIV SSP Subscriber has generated their private keys in the presence of a WidePoint PIV SSP Registration Authority or WidePoint PIV SSP Local Registration Authority upon completion of the identity proofing process and that the private-key has been generated in a FIPS 140-3 Level 2 security module (i.e. their key generation was witnessed by a duly appointed agent of the WidePoint PIV SSP). This ensures that there is only one identity certificate private key in existence and that it is protected by a cryptographic module that does not allow the private key to be exported and that the key generation was witnessed by an agent trained and fluent in the policies and practices of Common Policy and the WidePoint PIV SSP. Medium Hardware Assurance certificates issued by the WidePoint PIV SSP can only assert the certificate policy value of **id-fpki-common-hardware** and only for human WidePoint PIV SSP Subscribers. Medium Hardware Assurance is intended for all applications operating in environments appropriate for medium assurance, but which require a higher degree of assurance and technical non-repudiation based on the Relying Party's assessment.

- All applications appropriate for medium assurance certificates
- Applications performing contracting and contract modifications

The following Levels of Assurance are specific to the WidePoint PIV SSP PIV and PIV-I credentials as described in Section 1.4.1.

Card Authentication PIV Assurance: This Level of Assurance is intended only for use in physical access situations to support high volume throughput. Because Card Authentication PIV Assurance certificates do not require activation data to unlock the private key, validation of a PIV Card Authentication certificate provides only proof of the physical presence of the credential. Card Authentication PIV Assurance provides no proof of the identity of the individual in possession of the token. WidePoint PIV SSP PIV Credentials and their associated WidePoint PIV SSP certificates are not intended to replace existing approval mechanisms for physical access, but they may provide additional layers of protection to identify the holder of the WidePoint PIV SSP PIV Credential. Card Authentication PIV Assurance certificates issued by the WidePoint PIV SSP can only assert the certificate policy value of **id-fpki-common-cardAuth** and may only be issued to WidePoint PIV SSP PIV Credentials through a WidePoint PIV SSP CMS.

Authentication PIV Assurance: This Level of Assurance meets the same conditions and expectation for use as the Medium Hardware Level of Assurance with the exception that the WidePoint PIV SSP Subscriber has generated their private keys in the presence of a WidePoint PIV SSP Issue upon completion of the WidePoint PIV SSP PIV registration and issuance process and that the private-key has been generated in a FIPS 201-3 PIV card. Medium Hardware PIV Assurance certificates issued by the WidePoint PIV SSP can only assert the certificate policy value of **id-fpki-common-authentication** and may only be issued to WidePoint PIV SSP PIV Credentials through a WidePoint PIV SSP CMS.

Content Signing PIV Assurance: This Level of Assurance is intended only for use in digitally signing data objects on a WidePoint PIV SSP PIV credential and may not be used for any other purpose. WidePoint PIV SSP Content Signing PIV certificates are only issued to a WidePoint PIV SSP CMS as required by this WidePoint PIV SSP CPS and Common Policy. Content Signing PIV Assurance certificates are only issued to a WidePoint PIV SSP CMS by the WidePoint PIV SSP and can only assert the certificate policy value of **id-fpki-common-contentsigning**.

Card Authentication PIV-I Assurance: This Level of Assurance is intended only for use in physical access situations to support high volume throughput. Because Card Authentication PIV-I Assurance certificates do not require activation data to unlock the private key, validation of a PIV-I Card Authentication certificate provides only proof of the physical presence of the credential. Card Authentication PIV-I Assurance provides no proof of the identity of the individual in possession of the token. WidePoint PIV SSP PIV-I Credentials and their associated WidePoint PIV SSP certificates are not intended to replace existing approval mechanisms for physical access, but they may provide additional layers of protection to identify the holder of the WidePoint PIV SSP PIV-I Credential. Card Authentication PIV-I Assurance certificates issued by the WidePoint PIV SSP can only assert the certificate policy value of **id-fpki-common-pivi-cardAuth** and may only be issued to WidePoint PIV SSP PIV-I Credentials through a WidePoint PIV SSP CMS.

Authentication PIV-I Assurance: This Level of Assurance meets the same conditions and expectation for use as the Medium Hardware Level of Assurance with the exception that the WidePoint PIV SSP Subscriber has generated their private keys in the presence of a WidePoint PIV SSP Issue upon completion of the WidePoint PIV SSP PIV-I registration and issuance process and that the private-key has been generated in a FIPS 201-3 PIV-I card. Medium Hardware PIV-I Assurance certificates issued by the WidePoint PIV SSP can only assert the certificate policy value of **id-fpki-common-pivi-authentication** and may only be issued to WidePoint PIV SSP PIV-I Credentials through a WidePoint PIV SSP CMS.

Content Signing PIV-I Assurance: This Level of Assurance is intended only for use in digitally signing data objects on a WidePoint PIV SSP PIV-I credential and may not be used for any other purpose. WidePoint PIV SSP Content Signing PIV-I certificates are only issued to a WidePoint PIV SSP CMS as required by this WidePoint PIV SSP CPS and Common Policy. Content Signing PIV-I Assurance certificates are only issued to a WidePoint PIV SSP CMS by the WidePoint PIV SSP and can only assert the certificate policy value of **id-fpki-common-pivi-contentsigning**.

1.4.2 PROHIBITED CERTIFICATE USES

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

Delegated digital signature certificates must not assert authentication OIDs in a certificate Extended Key Usage (EKU) extension.

Certificates intended for code signing are not permitted under this policy.

1.5 POLICY ADMINISTRATION

1.5.1 ORGANIZATION ADMINISTERING THE DOCUMENT

WidePoint Corporation, located at 11250 Waples Mill Road, Suite 210, Fairfax, VA 22030, is responsible for the creation, revision, and promulgation of this WidePoint PIV SSP CPS, in accordance with the requirements stipulated in Common Policy.

1.5.2 CONTACT PERSON

Luther Deyo, WidePoint Vice-President ICAM and WidePoint PIV SSP Program Manager, is responsible for the registration, maintenance, and interpretation of this WidePoint PIV SSP CPS.

Questions regarding this WidePoint PIV SSP CPS should be directed to:

WIDEPOINT PIV SSP MANAGEMENT AUTHORITY

11250 WAPLES MILL ROAD, SUITE 210

FAIRFAX, VA 22030

WCSC-PKIPolicy@WidePoint.com

1.5.3 PERSON DETERMINING CPS SUITABILITY FOR THE POLICY

The FPKIPA determines the suitability of this WidePoint PIV SSP CPS using a compliance analysis and approval process.

FEDERAL PKI POLICY AUTHORITY

fpki@gsa.gov

1.5.4 WIDEPOINT PIV SSP CPS APPROVAL PROCEDURES

The FPKIPA will make the determination that this WidePoint PIV SSP CPS complies with Common Policy for a given level of assurance. The compliance analysis is performed by an external independent auditor. WidePoint has met all requirements for an approved Certification Practice Statement prior to commencing operations. This WidePoint PIV SSP CPS has been determined to be an approved CPS in compliance with the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 2.12, August 4, 2025V. Registration Authority practices are documented in the WidePoint PIV SSP Registration Practices Statement, hereafter referred to as the WidePoint PIV SSP RPS. In each case, the determination process must include an independent compliance auditor's results and recommendations. See Section 8 for further details.

1.6 DEFINITIONS AND ACRONYMS

See Sections 14 and 15.

2 PUBLICATIONS AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

The WidePoint PIV SSP operates and maintains repositories in support of WidePoint PIV SSP Subscribers and Relying Parties and their use and acceptance of certificates issued by the WidePoint PIV SSP. The location of any publication is available to Subscribers and Relying Parties as stipulated in this CPS.

Information in WidePoint PIV SSP Repositories is protected in accordance with the provisions of this WidePoint PIV SSP CPS, the WidePoint System Security Plan, and other referenced documents such as Public Law 093-579 Privacy Act of 1974 Title 5 United States Code §552a as set forth in WidePoint's Privacy Policy and Procedures documents.

The WidePoint PIV SSP Repository is responsible for:

- Maintaining a secure system for storing and retrieving Certificates.
- Maintaining a current copy of this CPS.
- Maintaining other information relevant to Certificates.
- Providing information regarding the status of Certificates as valid or invalid that can be determined by a Relying Party.

The WidePoint PIV SSP Repository is located at https://orc.widepoint.com/certificates-and-credentials/hspd-12-piv/. The WidePoint PIV SSP maintains the repository using two separate, but identical iterations run behind a load balancer. In addition, a copy of the WidePoint PIV SSP Repository is maintained at the WidePoint Secondary Site as described in the WidePoint System Security Plan and is activated in the event of the WidePoint Incident Response Plan[IR-8] activation. The WidePoint Primary Site has dedicated power[PE-11] and HVAC,[PE-14] separate from the facility, with a direct dedicated generator[PE-11], as cited in Section 5 of this WidePoint PIV SSP CPS and described in the WidePoint System Security Plan Physical and Environmental Protection Control Family.[PE] These capabilities allow the WidePoint PIV SSP to maintain 99% availability of the repository overall per year and scheduled downtime not to exceed 0.5% annually. Communication failures as a result of Internet problems external to the operating organization will not count against this availability requirement.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 PUBLICATION OF CERTIFICATE AND CERTIFICATE STATUS

The WidePoint PIV SSP posts WidePoint PIV SSP CA Certificates at the following locations, accessible via HTTP:

- http://crl-server.orc.com/caCerts/<CA-Name>.p7c

Certificate Authority certificates that are issued by the WidePoint PIV SSP are published to a file publicly available and encoded in the Subject Information Access (SIA) extension in all valid certificates issued to the WidePoint PIV SSP at:

- http://crl-server.orc.com/caCerts/caCertsIssuedByWPSSPIntCA.p7c

All Certificate Authority certificates issued to the WidePoint PIV SSP are published to a file publicly available and encoded in the Authority Information Access (AIA) extension in all valid certificates issued. This file is a binary (DER encoded) certs-only Cryptographic Message Syntax file that has an extension of .p7c and a http response content type header of 'application/pkcs7-mime' and is published to the following location:

- https://crl-server.orc.com/caCerts/caCertsIssuedTo<CA-Name>.p7c

All WidePoint PIV SSP Certificate Authorities and Subordinate Certificate Authorities that issue certificates under this WidePoint PIV SSP CPS publishes the latest Certificate Revocation List (CRL) covering all unexpired certificates via a publicly accessible HTTP URI until such time as all issued certificates have expired. This URI is asserted in the CRL distribution point extension of all certificates issued by that WidePoint PIV SSP Certificate Authorities and Subordinate Certificate Authorities, with the exception of Online Certificate Status Protocol (OCSP) responder certificates that include the id-pkix-ocsp-nocheck extension. The WidePoint PIV SSP posts CRLs at the following locations, accessible via HTTP:

- http://crl-server.orc.com/CRLs/<CA Name>.crl

The WidePoint PIV SSP maintains Certificate Status Servers (CSSs) that provides status information about certificates on behalf of each WidePoint PIV SSP Certificate Authority through on-line transactions. The WidePoint PIV SSP Certificate Status Servers are delegated OCSP services, as described in [RFC 6960], and provide on-line status information for WidePoint PIV SSP Subscriber certificates via a publicly accessible HTTP URI in the AIA extension of each WidePoint PIV SSP Subscriber certificate.

Pre-generated OCSP responses may be created by the WidePoint PIV SSP CSSs and distributed to OCSP servers. OCSP responses, like CRLs, are publicly distributable data. OCSP servers that lack OCSP response signing capability have the same security requirements as the repository hosting WidePoint PIV SSP CRLs.

OCSP services that are locally trusted, as described in [RFC 6960], are not covered by this WidePoint PIV SSP CPS.

The WidePoint PIV SSP posts certificate information in the WidePoint PIV SSP Repository. Only information contained in the certificate is posted in the WidePoint PIV SSP Repository. Access to the WidePoint PIV SSP Repository is available via HTTPS, via a directory gateway interface at:

- https://www.orc.com/repository/

The WidePoint PIV SSP Repository contains sub-trees (i.e., branches) that identify the organization of the end-entity to which the certificate was issued.

The WidePoint PIV SSP Repository meets the following obligations:

- To list all un-expired certificates for the WidePoint PIV SSP CAs to Relying Parties;
- To contain an accurate and current CRL for each respective WidePoint PIV SSP CA for use by Relying Parties;
- To be publicly accessible;
- To be maintained in accordance with the practices specified in this WidePoint PIV SSP CPS; and
- To meet or exceed the requirement of 99% availability for all components within the control of the operating organization.

The WidePoint PIV SSP maintains a copy of at least all certificates and CRLs issued by WidePoint PIV SSP CAs and provides this information for archiving. The WidePoint PIV SSP provides this information on a certificate accessed web server posted no later than 10 days after the end of the collection of the data.

The WidePoint PIV SSP Repository is a publicly accessible repository that is available to subscribers and relying parties that contains:

- All WidePoint PIV SSP issued encryption certificates that assert a certificate policy listed in Section 1.2 of this WidePoint PIV SSP CPS;
- The most recently issued CRL for each WidePoint PIV SSP CA;
- All WidePoint PIV SSP CA certificates used as signing key and CRLs;
- All certificates issued to WidePoint PIV SSP CAs;
- A copy of the current Common Policy CP, including any waivers granted to the WidePoint PIV SSP by the FPKIPA; and,
- An abridged version of this approved WidePoint PIV SSP CPS. The published version will include at a minimum the sections itemized below and all obligations and requirements levied on entities external to the WidePoint PIV SSP:
    - Section 1.5;
    - Section 3.2, Initial Identity Validation;
    - Section 4.9, Certificate Revocation and Suspension;
    - Section 9, Other Business and Legal Matters; and
    - Any additional policy, waiver, or practice information that is supplemental to Common Policy or this WidePoint PIV SSP CPS.

WidePoint PIV SSP CA and End Entity certificates shall only contain valid Uniform Resource Identifiers (URIs) that are accessible by relying parties.

2.2.2 Publication of WidePoint Certificate Authority Information

The WidePoint PIV SSP Repository is a publicly accessible repository that is available to subscribers and relying parties that contains:

- All certificates issued to WidePoint PIV SSP CAs;
- A copy of the current Common Policy CP;
- A copy of the WidePoint PIV SSP annual PKI Compliance Audit Letter; and,
- An abridged version of this approved WidePoint PIV SSP CPS. The published version will include at a minimum the sections itemized below and all obligations and requirements levied on entities external to the WidePoint PIV SSP:
    - Section 1.5;
    - Section 3.2, Initial Identity Validation;
    - Section 4.9, Certificate Revocation and Suspension;
    - Section 9, Other Business and Legal Matters; and
    - Any additional policy or practice information that is supplemental to Common Policy or this WidePoint PIV SSP CPS.

2.3 Time or Frequency of Publication

WidePoint PIV SSP CA issued certificates are published to the WidePoint PIV SSP Repository at the time of issuance. WidePoint PIV SSP CA CRL publication is in accordance with Section 4.9.7 and 4.9.12 of this WidePoint PIV SSP CPS.

2.4 ACCESS CONTROLS ON REPOSITORIES

There are no access controls on the reading of the abridged WidePoint PIV SSP CPS summary, any supplemental policy information, or any supplemental practice information published by the WidePoint PIV SSP. Certificate and CRL information are publicly available.

There are no access controls on the reading of repository information, including certificates and CRLs. Updating the WidePoint PIV SSP Repository is restricted only to specific trusted roles, as described in Section 5.2.1 of this WidePoint PIV SSP CPS, using certificate authenticated access control over TLS. The WidePoint PIV SSP protects any and all repository information not intended for public dissemination or modification as specified by the WidePoint System Security Plan Risk Assessment Control Family RA-8 Privacy Impact Assessment[RA-8], [PIA] and the WidePoint System Security Plan. Access controls include:

- Access to WidePoint PIV SSP systems and system components are limited to the appropriate trusted roles as described in Section 5.2.1 of this WidePoint PIV SSP CPS and protected by strong authentication methods[IA-5] as stipulated in this WidePoint PIV SSP CPS and the WidePoint System Security Plan.
- User authentication is via certificate authentication (or User ID and password when appropriate) and data encryption is used, as stipulated in this CPS.
- WidePoint PIV SSP personnel in trusted roles as identified in Section 5.2.1 of this WidePoint PIV SSP CPS are trained [AT-3] in accordance with the requirements of the trusted role and the WidePoint System Security Plan Awareness and Training Control Family prior to having access to the WidePoint PIV SSP systems and system components.
- The WidePoint Corporate Security Auditor determines and periodically reviews user access rights[AC-2].
- WidePoint PIV SSP certificates that contain the universally unique identifier (UUID) in the subject alternative name extension, or any other certificate field are restricted from publication to the WidePoint PIV SSP Repository or any public repository.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 TYPES OF NAMES

This WidePoint PIV SSP CPS establishes the requirements for both subject distinguished names and subject alternative names.

3.1.1.1 Subject Names

All certificates issued by the WidePoint PIV SSP CAs conform to the X.500 Distinguished Name (DN) format for subject and issuer name fields and conform to the format specified in the Common Policy.

For WidePoint PIV SSP certificates issued under **id-fpki-common-policy**, **id-fpki-common-hardware**, or **id-fpki-common-devices**, the WidePoint PIV SSP CAs will assign X.500 distinguished names to all subscribers. These distinguished names may be in either of two forms: a geo-political name or an Internet domain component name.

All geo-political distinguished names assigned to federal employees will be in the following directory information tree:

- C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=structural_container]

The organizational units **department** and **agency** appear when applicable and are used to specify the federal entity that employs the WidePoint PIV SSP Subscriber. At least one of these organizational units must appear in the DN. 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.

The distinguished name of the federal employee WidePoint PIV SSP Subscriber will be one of the five following forms:

- C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=structural_container], cn=<nickname lastname>
- C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=structural_container], cn=<firstname initial. lastname>
- C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=structural_container], cn=<firstname initial lastname>
- C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=structural_container], cn=<firstname middlename lastname>
- C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=structural_container], cn=<lastname.firstname.middlename>

In the first common name form, nickname may be the WidePoint PIV SSP Subscriber's first name, a form of the first name, middle name, or pseudonym (e.g., Buck) by which the WidePoint PIV SSP Subscriber is generally known. A generational qualifier, such as "Sr." or "III", or agency specific identifiers (e.g., CN=Giants.John.Gregory.1234567890) may be appended to any of the common name forms specified above.

Additional certificate qualifiers may be appended to the common name in order to provide additional context to the certificate's intended usage. The qualifier must be preceded by a space followed by a hyphen (e.g., CN=John G. Giants -ENC).

Distinguished names assigned to federal contractors and other affiliated persons must follow one of the name forms identified above with (affiliate) appended to the end of the common name (e.g., CN=John G. Giants (affiliate)). For names assigned to federal contractors and other affiliated persons, generational qualifiers may be inserted between lastname and "(affiliate)".

The WidePoint PIV SSP may supplement any of the distinguished name forms for Human WidePoint PIV SSP Subscribers specified in this section by including a dnQualifier, serial number, or user id. When any of these are included, they may appear:

- as part of a multi-valued RDN with the common name, or
- as a distinct RDN that follows the RDN containing the common name

Role-based signature certificates must assert a common name as follows:

- CN=role [, department/agency]

Where the department/agency is implicit in the role (e.g., Secretary of Commerce), it may be omitted. Where the role alone is ambiguous (e.g., Chief Information Officer) the department/agency must be present in the common name. The organizational information in the common name must correspond to that in the organizational unit attributes.

Additional descriptors that indicate role-based certificates may be included before the role if acceptable for relying party use. Examples of role-based certificate common names may include:

- CN=Secretary of Commerce
- CN=On behalf of the Secretary of Commerce
- CN=Office of the Secretary of Commerce

Role-based signature certificates that support delegated digital signature uses, must be issued under **id-fpki-common-hardware** (see Section 1.3.6). For these delegated digital signature certificates, the common name must specify the role, the department or agency associated with that role, the name of the individual role holder, and a general purpose for the certificate, as follows:

- CN=role [, department/agency] [,firstname lastname (purpose)]

When the role holder's name is included in the CN, a parenthetical purpose for the certificate must be included to identify the certificate as a delegated digital signature certificate and to more readily convey to relying parties that the private key holder is not the named role holder. The order of appearance of role, department, and name (purpose) in the CN is determined by the issuing authority. Examples of delegated digital signature certificate common names may include:

- CN=Secretary of the Treasury, Alexander Hamilton (OFR)[1]
- CN=Secretary of the Treasury, Alexander Hamilton (delegated)
- CN=On behalf of the Secretary of the Treasury, Alexander Hamilton (acting agent)

Practice Note: Common Name (CN) fields are limited to sixty-four (64) characters.

Practice Note: In the case of "Chief Information Officer," use of department/agency in the common name is redundant to the RDN but is included for usability purposes. Display of the common name is widely supported in applications. Other attributes may or may not be presented to users.

Group encryption certificate distinguished names must take the following form:

- Base DN, CN=group name

[1] The parenthetical purpose "(OFR)" is only for certificates used to digitally sign official documents submitted to the Office of the Federal Register and should not be used for any other purpose.

where the group name is descriptive for the group, to include group email names (e.g., OMBmax Support Email). The group encryption certificate must not imply that a subject is a single individual (e.g., by asserting a human subscriber name form in any field of the certificate).

The WidePoint PIV SSP coordinates with the customer agency to determine which one of the aforementioned name definitions is used.

Devices that are the subject of certificates issued under this policy shall take the following form:

- C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=structural_container], cn=<device name>

where device name is a descriptive name for the device.

For WidePoint PIV SSP certificates asserting either **id-fpki-common-piv-contentSigning** or **id-fpki-common-pivi-contentSigning** certificate policy OID, the certificate's subject distinguished name must indicate the organization administering the credential issuance system. The distinguished name will take the following form in the following two cases:

- In the case which WidePoint administers the card management system for the Customer agency, the DN shall take the following form:
  - C=US, O=ORC PKI, OU=WidePoint, CN=<PIV or PIV-I Content Signer>
- In the case which the card management system is administered by the Customer agency, the DN shall take the following form:
  - C=US, O=U.S. Government, [OU=department], [ou=agency], CN=[organization] [ID] PIV or PIV-I Content Signer

Where [ID] equals unique qualifier assigned by organization (e.g., CN=<Agency Name> 1 PIV Content Signer; CN=<Agency Name> 2 PIV Content Signer).

WidePoint PIV SSP certificates asserting the certificate policy OID of **id-fpki-common-cardAuth** will take one of the following forms:

- C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=structural_container], serialNumber=FASC-N
- C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=structural_container], serialNumber=UUID

WidePoint PIV SSP certificates asserting the certificate policy OID of **id-fpki-common-pivi-cardAuth** will take the following form:

- C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=structural_container], serialNumber=UUID

This WidePoint PIV SSP CPS does not restrict the directory information tree for names of WidePoint PIV SSP Certificate Authorities or WidePoint PIV SSP Certificate Status Services. However, WidePoint PIV SSP Certificate Authorities that issue certificates under this WidePoint PIV SSP CPS must have distinguished names. WidePoint PIV SSP Certificate Authority and WidePoint PIV SSP Certificate Status Services distinguished names will be composed of any combination of the following attributes:

- country;
- organization;
- organizational unit; and
- common name (e.g., WidePoint PIV SSP <number>).

3.1.1.2 Subject Alternative Names

WidePoint PIV SSP certificates that assert a certificate policy OID of **id-fpki-common-authentication** or i**d-fpki-common-cardAuth** will include a subject alternative name. The subject alternative name extension includes both:

- the pivFASC-N name type [FIPS 201], the value of which must be the FASC-N [PACS] of the subject's PIV credential; and
- a UUID encoded as a URI as specified in Section 3 of [RFC 4122].

WidePoint PIV SSP certificates that assert a certificate policy OID of **id-fpki-common-cardAuth** will not include any other name in the subject alternative name extension.

WidePoint PIV SSP certificates that assert a certificate policy OID of **id-fpki-common-pivi-authentication**, **id-fpki-common-pivi-cardAuth**, **id-fpki-common-derived-pivAuth-hardware** or **id-fpki-common-derived-pivAuth** will include a subject alternative name that includes:

- a UUID encoded as a URI as specified in Section 3 of [RFC 4122].
- For derived PIV, UUID is unique per certificate.

WidePoint PIV SSP certificates that assert a certificate policy OID of **id-fpki-common-pivi-cardAuth** will not include any other name in the subject alternative name extension.

WidePoint PIV SSP Subscriber certificates that contain id-kp-emailProtection in the Extended Key Usage field must include a subject alternative name extension that includes a rfc822Name.

Role-based signature certificates including those that support delegated digital signatures, must include at least one subject alternative name extension that uniquely identifies the individual subscriber that controls the private signature key (e.g., rfc822Name or otherName like Microsoft User Principal Name). Another example of a compliant identifier is the full Distinguished Name from the PIV Authentication certificate of the individual who is to be issued the role-based certificate (e.g., the private key holder) that may be included as a directoryName.

WidePoint PIV SSP device certificates that assert serverAuth in the Extended Key Usage field:

- A subject alternative name of type dNSName must be included.
- Wildcard Domain Names are permitted in the DNSName values if all sub-domains covered by the wildcard fall within the same application, cloud service, or system accreditation boundary within the scope of the sponsoring Agency.
- Wildcards are not used in subdomains that host more than one distinct application platform. The use of third-level Agency wildcards, (e.g., *.[agency].gov), are prohibited to reduce the likelihood that a certificate will overlap multiple systems or services. Third level wildcards are permitted for DNSName dedicated to a specific application (e.g., *.[applicationname].gov).
- Before issuing a publicly trusted serverAuth certificate containing a wildcard, the WidePoint PIV SSP ensures the sponsoring agency has a documented procedure for determining that the scope of the certificate does not now and will not infringe on other agency applications.

Practice Note: The FASC-N [PACS] consists of forty (40) decimal digits that are encoded as a 25-byte binary value. This 25-byte binary value may be encoded directly into the pivFASC-N name type in the subject alternative name extension, but when included in the subject field the FASC-N must be encoded as a PrintableString that is at most sixty-four (64) characters long. This policy does not mandate any particular method for encoding the FASC-N within the serial number attribute as long as the same encoding method is used for all certificates issued by a CA. Acceptable methods for encoding the FASC-N within the serial number attribute include encoding the 25-byte binary value as 50 bytes of ASCII HEX or encoding the forty (40) decimal digits as forty (40) bytes of ASCII decimal.

Practice Note: When the UUID appears in the subjectAltName extension of a certificate, it must be encoded as a uniformResourceIdentifier as specified in Section 3 of [RFC 4122]. An example of a UUID encoded as a URI, from RFC 4122, is "urn:uuid:f81d4fae-7dec11d0-a765-00a0c91e6bf6". This policy does not mandate any particular method for encoding the UUID within the serial number attribute as long as the same encoding method is used for all certificates issued by the CA and it is encoded as a PrintableString that is at most 64 characters long, however, it is recommended that the string representation from Section 3 of [RFC 4122] be used. An example would be "f81d4fae7dec-11d0-a765-00a0c91e6bf6".

3.1.2 Need of Names to be Meaningful

Names issued to WidePoint PIV SSP Subscriber certificates will be meaningful as individual names, as actual server URLs, IP addresses, unique device names or as code-signing organizational names. Names issued to WidePoint PIV SSP Subscriber certificates will identify the person or object to which they are assigned.

Within the DN structure of certificates issued by the WidePoint PIV SSP to WidePoint PIV SSP Subscribers, the Common Name, hereafter referred to as CN, will represent the WidePoint PIV SSP Subscriber in a way that is easily understandable for humans. For human and device Subscribers, the CN will take the form identified in Section 3.1.1 of this WidePoint PIV SSP CPS.

The subject name in WidePoint PIV SSP Certificate Authority certificates will match the issuer name extension in WidePoint PIV SSP certificates issued by the WidePoint PIV SSP Certificate Authority, as required by [RFC 5280].

3.1.3 Anonymity or Pseudonymity of Subscribers

The WidePoint PIV SSP does not issue anonymous certificates.

Role-based certificates may be issued by the WidePoint PIV SSP to support internal operations. WidePoint PIV SSP Certificate Authorities may also issue role-based certificates that identify subjects by their organizational roles, as described in Section 3.1.1 of this WidePoint PIV SSP CPS.

All WidePoint PIV SSP Certificate Authority or Subordinate Certificate Authority certificates do not contain anonymous or pseudonymous identities.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting distinguished name forms are specified in [X.501]. Rules for interpreting e-mail addresses are specified in [RFC 5322]. Rules for interpreting the pivFASC-N name type are specified in [PACS].

3.1.5 Uniqueness of Names

The WidePoint PIV SSP complies with uniqueness of names; including X.500 DNs. The WidePoint PIV SSP CA(s) share a single public directory information tree for the publication of certificates (please refer to Section 3.1.1 of this WidePoint PIV SSP CPS for method of naming assignment). WidePoint enforces name uniqueness, as described in Section 3.1.1 and Section 3.1.2 of this WidePoint PIV SSP CPS.

The WidePoint PIV SSP ensures the following for subscriber names:

- The name contains the subscriber identity and organization affiliation (if applicable) that is meaningful to humans.
- The naming convention is described in This WidePoint PIV SSP CPS (see Section 3.1.1 of this WidePoint PIV SSP CPS).
- The WidePoint PIV SSP complies with the FPKIPA for the naming convention.

This does not prevent devices from sharing a Fully Qualified Domain Name (FQDN) as CN.

3.1.6 Recognition, Authentication and Role of Trademarks

A corporate entity is not guaranteed that its common name will contain a trademark if requested. The WidePoint PIV SSP will not knowingly issue a certificate from the WidePoint PIV SSP that includes a name that a court of competent jurisdiction has determined infringes the trademark of another. Upon being made aware by a

competent court or ruling that a WidePoint PIV SSP issued certificate contains a name that has infringed the referenced ruling. The WidePoint PIV SSP will revoke the previous issued certificates in accordance with Section 4.9.1 of this WidePoint PIV SSP CPS. WidePoint PIV SSP Subscribers who have been revoked under this stipulation will have to reapply at cost and without refund for new WidePoint PIV SSP Subscribers certificates that assert a trademark name that they or their organization have not infringed upon another party. Additionally, the WidePoint PIV SSP is not required to re-issue a correctly issued WidePoint PIV SSP Subscriber with the trademark name to the rightful owner if it has already issued one sufficient for identification.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

For Applicants and WidePoint PIV SSP Subscribers generating keys for requesting certificates (identity, device and non-escrowed encryption) that assert **id-fpki-common-policy**, **id-fpki-common-hardware**, **id-fpki-common-authentication**, **id-fpki-common-cardAuth**, **id-fpki-common-pivi-authentication**, **id-fpki-common-pivi-cardAuth**, **id-fpki-common-piv-contentSigning** and **id-fpki-common-pivi-contentSigning**, the WidePoint PIV SSP authenticates the Applicant or WidePoint PIV SSP Subscriber with a Proof of Possession test when requesting and retrieving the certificate by requiring the subscriber to perform a private key operation that verifies that the public key presented by the subscriber matches the private key. The WidePoint PIV SSP uses CRMF and PKCS #10 in support of Proof of Possession.

To affect Proof of Possession, the CA supplies a random challenge string to the browser as part of the KEYGEN tag.

For **id-fpki-common-policy**, the public key generated by the browser's associated Cryptographic Service Provider (CSP) and the challenge string supplied by the WidePoint PIV SSP CA are DER (Distinguished Encoding Rules) encoded together, and the resulting PublicKeyAndChallenge value is then digitally signed with the private key to produce a SignedPublicKeyAndChallenge value. This signed value is then base64 encoded and sent to the WidePoint PIV SSP CA as part of the certificate request; the WidePoint PIV SSP CA verifies the signature using the included public key, thus proving possession by the browser's CSP of the private key corresponding to that public key.

For **id-fpki-common-devices**, the WidePoint PIV SSP PKI Sponsor generates a key pair (private/public) using the device's associated Cryptographic Service Provider (CSP) and creates a signed PKCS10 object. The WidePoint PIV SSP PKI Sponsor submits the PKCS10 object to the WidePoint PIV SSP CA for certificate processing.

For **id-fpki-common-hardware**, **id-fpki-common-devicesHardware**, **id-fpki-common-authentication**, **id-fpki-common-cardAuth**, **id-fpki-common-pivi-authentication**, **id-fpki-common-pivi-cardAuth**, **id-fpki-common-piv-contentSigning** and **id-fpki-common-pivi-contentSigning** the key pair is generated by the CSP associated with the cryptographic device (smartcard or another crypto-token). To affect Proof of Possession, the WidePoint PIV SSP CA supplies a random challenge string to the browser as part of the KEYGEN tag. The public key generated by the CSP and the challenge string supplied by the WidePoint PIV SSP CA are DER (Distinguished Encoding Rules) encoded together, and the resulting PublicKeyAndChallenge value is then digitally signed with the private key to produce a SignedPublicKeyAndChallenge value. This signed value is then base64 encoded and sent to the WidePoint PIV SSP CA as part of the certificate request; the WidePoint PIV SSP CA verifies the signature using the included public key, thus proving possession by the browser of the private key corresponding to that public key.

The WidePoint PIV SSP only provides escrow for the encryption certificate issued through the WidePoint PIV SSP CMS for certificates asserting the **id-fpki-common-policy** certificate policy OID. The WidePoint PIV SSP Subscriber's private key for the PIV-I encryption certificate is generated in the hardware security module (HSM) and stored encrypted and protected by the Key Encryption Key (KEK) in a WidePoint PIV SSP Key Encryption Database, prior to the key being injected onto the PIV-I card. The FIPS 201-compliant card used, enforces using a secure channel for writing this information to the card. During card personalization certificate keys are created in KMS under the protection of an HSM. In a secure channel session (SCP-03), the key is exchanged with the card. The secure channel is secured with AES keys, additionally, key data is encrypted with an AES data encryption key. The WidePoint PIV SSP Subscriber's encryption keys are protected by a KEK, which is a 24-byte AES key. All cryptographic operations occur in the HSM. The private key is encrypted in the HSM with the KEK for secure storage in the database.

When retrieving the completed certificate, the browser also checks before importing the certificate into its database, to verify that the public key in the certificate being installed matches the private key it originally generated.

3.2.2 AUTHENTICATION OF ORGANIZATION IDENTITY

Applicants and WidePoint PIV SSP Subscribers affiliated with an organization which has a current contractual relationship with WidePoint for the purposes of obtaining digital certificates or credentials as described by this WidePoint PIV SSP CPS will provide proof of their relationship to the organization to whom they are employed. This proof can be done by:

- Applicant or WidePoint PIV SSP Subscriber requests a certificate accompanied by a US Government sponsor. The Government Sponsor is vetted by presentation of a government issued photo ID card (e.g., a DoD Common Access Card (CAC) or Federal Employee Personal Identity Verification (PIV) Credential). The Government sponsor will attest to the Applicant or WidePoint PIV SSP Subscriber's affiliation.
- Applicant or WidePoint PIV SSP Subscriber presenting a government-issued photo badge including the Applicant or WidePoint PIV SSP Subscriber's affiliation.
- Applicant or WidePoint PIV SSP Subscriber providing a signed letter on agency or department letterhead from an authorized organization official attesting to the relationship (this is the only method approved for device and code signing certificate requests); or,
- Applicant or WidePoint PIV SSP Subscriber presenting an un-expired photo ID badge issued by the organization.

In addition to verifying the Applicant or WidePoint PIV SSP Subscriber's authorization to represent the Sponsoring Organization, the WidePoint PIV SSP verifies the Sponsoring Organization's current operating status, and that the organization conducts business at the address listed in the WidePoint PIV SSP Certificate application.

Requests for Third-Party recovery of WidePoint PIV SSP Subscriber keys shall include validation of the individual's authority to act on behalf of the requesting organization (i.e., through a law enforcement agency or a competent court). Verification shall include identify proofing of the requestor and their affiliation with the requesting organization or a signed court order from a court with jurisdiction.

3.2.3 AUTHENTICATION OF INDIVIDUAL IDENTITY

3.2.3.1 Authentication of Human Subscribers

Verification of an Applicant or WidePoint PIV SSP Subscriber's identity will be performed prior to certificate issuance and the applicant's identity must be verified no more than 30 days before initial certificate issuance. For WidePoint PIV SSP Subscriber certificates that will assert the certificate policy OID of **id-fpki-common-policy** or **id-fpki-common-hardware**, the Applicant or WidePoint PIV SSP Subscriber's in-person identity verification may be performed by a WidePoint Trusted Agent as defined in Section 1.3.7.1 of this WidePoint PIV SSP CPS. Authentication by a WidePoint Trusted Agent does not relieve the WidePoint PIV SSP Registration Authority of their responsibility to verify that the required procedures were followed as detailed in this section.

Minors and others not competent to perform face-to-face registration alone are not supported under this WidePoint PIV SSP CPS.

At a minimum, authentication procedures for WidePoint PIV SSP certificate Federal employee applicants must include the following steps:

- Verify that a request for certificate issuance to the applicant was submitted by agency management.
- Verify Applicant's employment through use of official agency records.
- Establish applicant's identity by in-person proofing before a WidePoint PIV SSP Registration Authority, based on either of the following processes:

  1. Process #1:

A. The Applicant or WidePoint PIV SSP Subscriber presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and
B. The WidePoint PIV SSP Registration Authority examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and
C. The credential presented above is verified by the WidePoint PIV SSP Registration Authority for currency and legitimacy (e.g., the agency ID is verified as valid). Typically, this is accomplished by querying a database maintained by the organization that issued the credential, but other equivalent methods may be used.

2. Process #2:

A. The Applicant or WidePoint PIV SSP Subscriber presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and
B. The WidePoint PIV SSP Registration Authority examines the presented credential for biometric data that can be linked to the Applicant or WidePoint PIV SSP Subscriber (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and
C. The Applicant or WidePoint PIV SSP Subscriber presents current corroborating information to the WidePoint PIV SSP Registration Authority. The identifying information (e.g., name and address) on the credential presented above is verified by the WidePoint PIV SSP Registration Authority for currency and legitimacy (e.g., the agency ID is verified as valid).

Practice Note: This may be accomplished by querying a database maintained by the organization that issued the financial instrument or through use of a commercial credit database. In some instances, commercial credit card databases will validate the name and address of current cardholders on-line; this validation is acceptable if the card is presented to the RA. Other methods may be accepted.

- Record and maintain a biometric of the Applicant or WidePoint PIV SSP Subscriber (e.g., a photograph or fingerprint). (Handwritten signatures and other behavioral characteristics are not accepted as biometrics for the purposes of this policy.) This establishes an audit trail for dispute resolution.

For contractors and other affiliated personnel, the authentication procedures must include the following steps:

- Verify that a request for certificate issuance to the Applicant or WidePoint PIV SSP Subscriber was submitted by an authorized sponsoring agency employee (e.g., contracting officer or contracting officer's technical representative).
- Verify sponsoring agency employee's identity and employment through either one of the following methods:

1. A digitally signed request from the sponsoring agency employee, verified by a currently valid employee signature certificate issued by a WidePoint PIV SSP CA, may be accepted as proof of both employment and identity,
2. Authentication of the sponsoring agency employee with a valid employee PIV-authentication certificate issued by the agency may be accepted as proof of both employment and identity, or
3. In-person identity proofing of the sponsoring agency employee may be established before the WidePoint PIV SSP Registration Authority as specified in employee authentication above and employment validated through use of the official agency records.

- Establish Applicant or WidePoint PIV SSP Subscriber's identity by in-person proofing before the registration authority, based on either of the following processes:

1. Process #1:

A. The Applicant or WidePoint PIV SSP Subscriber presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and
B. The WidePoint PIV SSP Registration Authority examines the presented credential for biometric data that can be linked to the Applicant or WidePoint PIV SSP Subscriber (e.g., a photograph on the credential itself or a securely linked photograph of Applicant or WidePoint PIV SSP Subscriber), and
C. The credential presented shall be verified by the WidePoint PIV SSP Registration Authority for currency and legitimacy (e.g., the agency ID is verified as valid). Typically, this is accomplished by querying official records maintained by the organization that issued the credential.

2. Process #2:

A. The Applicant or WidePoint PIV SSP Subscriber presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and
B. The WidePoint PIV SSP Registration Authority examines the presented credential for biometric data that can be linked to the Applicant or WidePoint PIV SSP (e.g., a photograph on the credential itself or a securely linked photograph of Applicant or WidePoint PIV SSP), and
C. The Applicant or WidePoint PIV SSP Subscriber presents current corroborating information (e.g., current credit card bill or recent utility bill) to the WidePoint PIV SSP Registration Authority. The identifying information (e.g., name and address) on the credential presented in Step 3) b) i) above shall be verified by the WidePoint PIV SSP Registration Authority for currency and legitimacy (e.g., the agency ID is verified as valid).

- Record and maintain a biometric of the applicant (e.g., a photograph or fingerprint) by the WidePoint PIV SSP Registration Authority or a WidePoint PIV SSP Certificate Authority Administrator. (Handwritten signatures and other behavioral characteristics are not accepted as biometrics for the purposes of this policy.) This establishes an audit trail for dispute resolution.

In all cases, a WidePoint PIV SSP Registration Authority records the following information:

- The identity of the person performing the validation process.
- Applicant or WidePoint PIV SSP Subscriber s name as it appears in the certificate Common Name field.
- A signed declaration by the identity-verifying agent that they verified the identity of the applicant, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury).
- Method of application (i.e., online, in-person).
- The method used to authenticate the Applicant or WidePoint PIV SSP Subscriber's identity, including identification type and unique number or alphanumeric identifier on the ID.
- A biometric of the Applicant or WidePoint PIV SSP Subscriber (facial image, fingerprint, etc.).
- The date and time of verification.
- A handwritten signature by the Applicant or WidePoint PIV SSP Subscriber in the presence of the person performing the identity verification using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury).

For each data element accepted for proofing, including electronic forms:

- Name of document presented for identity proofing.
  - For PIV certificates the identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 1615-0047, Employment Eligibility Verification.
- Issuing authority.
- Date of issuance; and,
- Date of expiration.

Additionally, all fields must be verified:

- Source of verification (i.e., which databases used for cross-checks);
- Method of verification (i.e., online, in-person);
- Date/time of verification.
- All associated error messages and codes.
- Date/time of process completion; and

In all cases, the WidePoint PIV SSP may request additional information or verification if deemed necessary to confirm the requestor's identity.

For WidePoint PIV SSP Subscriber certificates that assert the certificate policies OID of **id-fpki-common-authentication** or **id-fpki-common-pivi-authentication**, identity-proofing is performed in accordance with Section 2.7, PIV Identity Proofing and Registration Requirements, of FIPS 201-3.

For WidePoint PIV SSP Subscriber certificates that assert the certificate policies OID of **id-fpki-common-authentication** or **id-fpki-common-pivi-authentication**, the Applicant or WidePoint PIV SSP Subscriber must appear before the WidePoint PIV SSP Registration Authority either in person or via supervised remote.

For WidePoint PIV SSP Subscriber certificates that assert the certificate policies OID of **id-fpki-common-policy** or **id-fpki-common-hardware**, WidePoint PIV SSP Registration Authorities may accept authentication of the Applicant or WidePoint PIV SSP Subscriber's identity attested to and documented by a Trusted Agent, assuming agency identity requirements are otherwise satisfied. Authentication by a trusted agent does not relieve the WidePoint PIV SSP Registration Authority of its responsibility to verify required procedures were followed as described above.

For WidePoint PIV SSP Subscriber certificates issued under **id-fpki-common-derived-pivAuth-hardware** or **id-fpki-common-derived-pivAuth**, identity must be verified in accordance with the requirements specified for issuing derived credentials in [SP 800-157]. For **id-fpki-common-derived-pivAuth-hardware**, the Applicant or WidePoint PIV SSP Subscriber must appear at the WidePoint PIV SSP Registration Authority in person or via supervised remote.

The WidePoint PIV SSP Registration Authority must:

- Verify that the request for certificate issuance to the Applicant or WidePoint PIV SSP Subscriber was submitted by an authorized agency employee.
- Use the PKI-AUTH authentication mechanism from Section 6 of [FIPS 201] to verify that the PIV Authentication certificate on the Applicant or WidePoint PIV SSP Subscriber's PIV credential is valid and that the Applicant or WidePoint PIV SSP Subscriber is in possession of the corresponding private key.
- Maintain a copy of the Applicant or WidePoint PIV SSP Subscriber's PIV Authentication certificate.

Seven days after issuing the derived credential, the WidePoint PIV SSP Registration Authority or the WidePoint PIV SSP Certificate Authority shall recheck the revocation status of the PIV Authentication certificate. This step can detect use of a compromised PIV credential to obtain a derived credential.

For certificates issued that assert a certificate policy OID of **id-fpki-common-derived-pivAuth-hardware**, the Applicant or WidePoint PIV SSP Subscriber must appear in person or via supervised remote to present the PIV credential and perform the PKI-AUTH authentication mechanism. The WidePoint PIV SSP Registration Authority must perform a one-to-one comparison of the Applicant or WidePoint PIV SSP Subscriber against biometric data stored on the PIV credential, in accordance with [SP 800-76], and must record and maintain the biometric sample used to validate the Applicant or WidePoint PIV SSP Subscriber.

In cases where a 1:1 biometric match against the biometrics available on the PIV credential or in the chain-of-trust, as defined in [FIPS 201] is not possible:

- The Applicant or WidePoint PIV SSP Subscriber must present a government-issued form of identification (e.g., a passport or driver's license) in addition to the PIV credential, and

- The RA must examine the presented credentials for biometric data that can be linked to the Applicant or WidePoint PIV SSP Subscriber (e.g., a photograph on the credential itself or a securely linked photograph of the Applicant or WidePoint PIV SSP Subscriber), and

The process documentation and authentication requirements must include the following:

- The identity of the person performing the authentication and either:
  - A signed declaration by that person that he or she verified the identity of the Applicant or WidePoint PIV SSP Subscriber using the format set forth at [28 U.S.C. 1746] (declaration under penalty of perjury); or
  - An auditable record linking the authentication of the person performing the identification to their verification of each Applicant or WidePoint PIV SSP Subscriber.
- Unique identifying number(s) from second form of identification of the Applicant or WidePoint PIV SSP Subscriber, or a facsimile of the ID(s);
- The biometric of the Applicant or WidePoint PIV SSP Subscriber.
- The date and time of the verification.

3.2.3.2 Authentication of Component Identities

Some computing and communications components (web servers, routers, firewalls, etc.) may be named as certificate subjects. In such cases, the component must have a human Sponsor who is affiliated with the agency under which the certificate is being issued as described in Section 4.1.1.3. The Sponsor is responsible for providing the WidePoint PIV SSP CAA, or approved WidePoint PIV SSP Registration Authorities, through an application form, correct information regarding:

- Equipment identification (e.g., serial number) or service name (e.g., DNS name) or unique software application name.
- Equipment or software application public keys.
- Equipment or software application authorizations and attributes (if any are to be included in the certificate).
- Contact information to enable WidePoint to communicate with the PKI sponsor when required.

These certificates will only be issued to authorized devices under the subscribing organization's control. In the case a human PKI Sponsor is changed, the new Sponsor must review the status of each device under their sponsorship to ensure it is still authorized to receive certificates. See Section 9.6.3 for WidePoint PIV SSP Subscriber responsibilities.

For each WidePoint Card Management System and each agency Card Management System, a digitally-signed e-mail from an authorized person is sent requesting authorization for issuance of a connector certificate to the WidePoint PIV SSP.

For each Fully-Qualified Domain Name listed in certificate that asserts a certificate policy OID of **id-fpki-common-devices** or **id-fpki-common-devicesHardware**, the WidePoint PIV SSP confirms and maintains documented evidence that, as of the date the certificate was issued, that the Sponsor's agency has control over the FQDN and the sponsor is authorized to request the certificate.

Each agency must have a naming policy for devices that receive a certificate that asserts a certificate policy OID of **id-fpki-common-devices** or **id-fpki-common-devicesHardware** that specifies unique meaningful FQDN names and the WidePoint PIV SSP CPS documents how the WidePoint PIV SSP ensures compliance with the sponsoring agency's policy.

Note: FQDNs shall be listed in the certificate that asserts a certificate policy OID of **id-fpki-common-devices** or **id-fpki-common-devicesHardware** using dNSNames in the subjectAltName extension or in Subordinate CA Certificates via dNSNames in permittedSubtrees within the Name Constraints extension.

Before issuing a certificate with a wildcard character (*) in a common name or subject alternative name of type dNSName, the WidePoint PIV SSP Certificate Authority uses and follows an established and documented procedure to ensure that the wildcard does not fall immediately to the left of an agency or organization name, but is qualified

down to a unique application, server, or server farm under control of the sponsor's organization (see Section 3.1.1). The device sponsor must demonstrate that the domain name requested is entirely within the namespace to be covered by the wildcard certificate.

The identity of the sponsor must be authenticated by:

- Verification of digitally signed messages sent from the sponsor using a certificate issued under this policy; or
- In-person or supervised remote registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of Section 3.2.3.1.

3.2.3.3 Authentication of Human Subscribers for Role-Based Certificates

Prior to issuance of a delegated digital signature certificate, authentication of both the private key holder and an authorizing sponsor is required. These authentications can be performed using either the same procedures for authentication of individual identity (see Section 3.2.3.1), or the use of a private key associated with a current certificate that has the same or higher assurance than the certificate being requested and identifies the individual.

Practice Note: In the context of a delegated digital signature certificate, an "authorizing sponsor" is an individual other than the private key holder who can attest to the need to issue the certificate under the authority of the role holder in support of a documented business practice. For example, an "authorizing sponsor" can either be the role holder themselves or a Chief of Staff, Deputy, legal counsel, or similar position relative to the role holder.

Practice Note: The RA or CA can leverage a digital signature from supporting auditable artifacts (e.g., authorization form or subscriber agreement) to fulfill authentication requirements for role-based certificates.

3.2.3.4 Authentication for Human Subscribers for Group Certificates

Normally, a certificate is issued to a single WidePoint PIV SSP Subscriber. However, for cases where there are several individuals acting in one capacity to decrypt data, an encryption certificate may be issued to a group composed of multiple WidePoint PIV SSP Subscribers. Each group certificate has a sponsor who is responsible for ensuring that only authorized individuals have access to the corresponding private key. Prior to group encryption certificate issuance, WidePoint PIV SSP Registration Authorities shall authenticate the group sponsor using a current signature key of equal or greater assurance than the group certificate itself, or follow the authentication process identified in Section 3.2.3.1. In addition to the authentication of the group sponsor, the following applies to group encryption certificates:

- The group sponsor assigns the subject DN and SAN of the group encryption certificate, must ensure that each group member has signed an individual Shared Key Usage Agreement and must maintain a list of subscribers with access to the shared private key at all times. This list must be provided to an authorized representative of the WidePoint PIV SSP Registration Authority upon request or at certificate revocation or expiration (see Section 9.6.3.2); and
- The procedures for issuing hardware tokens for use in shared key applications comply with all other stipulations of this WidePoint PIV SSP CPS (e.g., key generation, private key protection, and Subscriber obligations)

3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION

WidePoint PIV SSP Subscriber certificates only contain information that is verified through the application process and generated in accordance with the process described herein.

3.2.5 VALIDATION OF AUTHORITY

Certificates that contain explicit or implicit organization affiliations, such as role-based certificates and content signing certificates will be issued only after ascertaining the Applicant or the WidePoint PIV SSP Subscriber has the authorizations to act on behalf of the organization in the implied capacity. Examples of these include certificates that would be issued to a WidePoint PIV SSP Registration Authority or a WidePoint PIV SSP Local Registration Authority. The WidePoint PIV SSP accomplishes this validation for WidePoint PIV SSP Registration Authority and WidePoint PIV SSP Local Registration Authority via an Organizational Affiliation letter which is available on the WidePoint PIV SSP website. The Organizational Affiliation letter must be completed on organization letterhead and submitted with the certificate request documentation.

Prior to issuing role-based certificates, the WidePoint PIV SSP shall validate that the individual role-based certificate applicant either holds that role or, in support of delegated digital signature certificates, has been appropriately delegated the authority to sign official documents on behalf of the role or the role holder.

Practice Note: Some organizations may have established policies that indicate which positions are authorized to receive delegated digital signature certificates. While these policies may not individually name the private key holders, other supporting documents; such as official appointment letters provided by an authorizing sponsor, can indicate the individual private key holders to whom delegated digital signature certificates can be issued.

3.2.6 CRITERIA FOR INTEROPERATION

The Certificate and CRL Profile in this WidePoint PIV SSP CPS form a basis for assessing interoperability with the WidePoint PIV SSP. The decision to cross certify the Common Policy CA with the WidePoint PIV SSP will reside with the FPKIPA, as specified in Section 1 of Common Policy.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

WidePoint PIV SSP CAs are not re-keyed. The maximum lifetime of keys for WidePoint PIV SSP CAs is 10 years.

WidePoint PIV SSP Subscriber PIV or PIV-I identity is established through the use of a current signature key, except that identity must be re-established and biometrics re-collected through an in-person or supervised remote registration at least every twelve years.

In the event a WidePoint PIV SSP Subscriber PIV or PIV-I signature key cannot be used, identity may be verified through the use of biometrics on file through the chain of trust defined in [FIPS 201].

For **id-fpki-common-policy**, **id-fpki-common-hardware**, **id-fpki-common-authentication**, **id-fpki-common-pivi-authentication**, **id-fpki-common-derived-pivAuth**, and **id-fpki-common-derived-pivAuth-hardware**, a human WidePoint PIV SSP Subscriber identity may be established through use of current signature key, except that identity must be re-established through an in-person or supervised remote registration process at least once every twelve years from the time of initial registration.

For re-key of Subscriber certificates issued under **id-fpki-common-derived-pivAuth** and **id-fpki-common-derived-pivAuth-hardware**, the department or agency must verify that the WidePoint PIV SSP Subscriber is eligible to have a PIV credential (i.e., PIV credential is not terminated).

For re-key of WidePoint PIV SSP-Subscriber certificates issued under **id-fpki-common-derived-pivAuth-hardware**, identity must be established via mutual authentication between the issuer and the cryptographic module containing the current key, if the new key will be stored in the same cryptographic module as the current key. Identity must be established through the initial registration process per Section 3.2 if the new key will be stored in a different cryptographic module than the current key.

For WidePoint PIV SSP Subscriber certificates that assert a certificate profile object identifier of **id-fpki-common-devices** or **id-fpki-common-devicesHardware**, identity may be established through the use of a current signature key or using means commensurate with the strength of the certificate being requested.

3.3.2 Identification and Authentication for Re-Key After Revocation

Identification and authentication of individuals for re-key after certificate revocation requires the steps for initial registration, as outlined in Section 3.2.3.1 of this WidePoint PIV SSP CPS unless identity can be verified through the use of biometrics on file through the chain of trust defined in [FIPS 201]. A WidePoint PIV SSP Subscriber who has had their certificate revoked will revert to being an Applicant and will be unknown to the WidePoint PIV SSP in terms of applying for certificate requests from the WidePoint PIV SSP in the future.

3.4 Identification and Authentication for Revocation Request

The WidePoint PIV SSP authenticates all revocation requests for end-entity certificates issued by the WidePoint PIV SSP CAs as specified in Section 4.9.3 of this WidePoint PIV SSP CPS. A WidePoint PIV SSP Subscriber may request revocation of their own certificate by authenticating to the WidePoint PIV SSP CA revocation web interface, regardless of whether or not their private key has been compromised.

A WidePoint Registration Authority may revoke a WidePoint PIV SSP Subscriber's certificate for cause as specified in Section 4.9.1 of this WidePoint PIV SSP CPS or at the direction of an external agency, organization, relying party or court of competent jurisdiction if proof can be provided that the WidePoint PIV SSP Subscriber violated the terms of the Subscriber Agreement they acknowledged and signed. The WidePoint PIV SSP will maintain a list of authorized parties that includes persons appointed by the FPKIPA who may request revocation of any WidePoint PIV SSP Subscriber or WidePoint PIV SSP CA certificate. Revocation requests made by the FPKIPA are final and not subject to appeal or arbitration requests by the WidePoint PIV SSP Subscriber to whom the revocation requests apply.

Additionally, a WidePoint PIV SSP Local Registration Authority may perform a revocation request on behalf of a WidePoint PIV SSP Subscriber or for the organization to whom the WidePoint PIV SSP Subscriber is or was affiliated. The WidePoint PIV SSP Local Registration Authority will collect from the WidePoint PIV SSP Subscriber or from the WidePoint PIV SSP Point of Contact for the organization a signed message or documentation stating the reason and circumstances for the revocation request. The WidePoint PIV SSP LRA will send a revocation request on behalf of the WidePoint PIV SSP Subscriber or the WidePoint PIV SSP Point of Contact for the organization to a WidePoint PIV SSP Registration Authority via a signed message or signed documentation using their own WidePoint PIV SSP certificate that asserts a certificate policy equal to or greater than the certificate policy of the WidePoint PIV SSP Subscriber certificate for which revocation is requested.

3.5 Identification and Authentication for Key Recovery Request

3.5.1 Third-Party Key Recovery Request

Third Parties, described as any entity other than the WidePoint PIV SSP Subscriber to whom the associated certificate of an escrowed key has been issued, may request recovery of escrowed keys from the WidePoint PIV SSP. All third-party requests will be coordinated through a WidePoint PIV SSP Registration Authority. The WidePoint PIV SSP Registration Authority who receives the third-party recovery request will validate the authorization of the requestor in consultation with the WidePoint Chief Security Officer, the WidePoint Corporate Security Auditor, legal counsel retained by the WidePoint PIV SSP and the FPKIMA as appropriate.

The third-party requestor will establish their identity to the WidePoint PIV SSP RA either through use of their own WidePoint PIV SSP certificate or federal certificate that is cross-certified with Common Policy (i.e. PIV, CAC, PIV-I) in the form of a digitally signed message that is signed by a valid and trusted certificate asserting a certificate policy equal to or greater than the certificate policy in the associated certificate of the escrowed key or by using the procedures specified for in-person authentication of identity as specified in Section 3.2.3.1 of this WidePoint PIV SSP CPS. Additionally, the FPKIPA may request recovery of an escrowed key on behalf of a third party which may have cause to remain anonymous. In such cases, the FPKIPA shall notify a WidePoint PIV SSP Registration Authority of the intended key recovery through the same methods stipulated in this paragraph.

Third-party requestors may be a WidePoint PIV SSP PKI Point of Contact for organizations wishing to recover the escrowed keys of WidePoint PIV SSP Subscribers that have asserted an affiliation to their organization, a court of competent jurisdiction pursuant to a court order, or the FPKIPA with no stipulation. Other third-party requestors may be identified in the future but are subject to the opinion of their validity by the WidePoint Chief Security Officer, the WidePoint Corporate Security Auditor, legal counsel retained by the WidePoint PIV SSP and the FPKIPA prior to any recovery being permitted.

3.5.2 WIDEPOINT PIV SSP SUBSCRIBER KEY RECOVERY REQUEST

The WidePoint PIV SSP securely stores all encryption private keys issued by WidePoint PIV SSP CAs to all WidePoint PIV SSP Subscribers. Only private keys associated with certificates that assert the key usage of key encipherment and represent a human entity are escrowed by the WidePoint PIV SSP. Escrow of the private key occurs at the time of issuance of the certificate bound to that private key.

WidePoint PIV SSP Subscribers are authorized to request the recovery of their own escrowed encryption keys from the WidePoint PIV SSP. This recovery facilitates the ability of the WidePoint PIV SSP Subscriber to decrypt data that has been encrypted by that encryption key which may no longer be accessible to the WidePoint PIV SSP Subscriber.

WidePoint PIV SSP Subscribers may authenticate to the WidePoint PIV SSP CA with their valid WidePoint PIV SSP certificate to request the recovery of their escrowed keys. The WidePoint PIV SSP Subscriber must present their certificate that asserts a certificate policy equal to or greater than the certificate policy in the associated certificate of the escrowed key.

Alternatively, WidePoint PIV SSP Subscribers may request recovery through a WidePoint PIV SSP Registration Authority by establishing their identity either through use of their WidePoint PIV SSP certificate in the form of a digitally signed message that is signed by a valid WidePoint PIV SSP certificate asserting a certificate policy equal to or greater than the certificate policy in the associated certificate of the escrowed key or by using the procedures specified for in-person authentication of identity as specified in Section 3.2.3.1 of this WidePoint PIV SSP CPS.

3.5.3 KEY RECOVERY AGENT AUTHENTICATION

WidePoint PIV SSP Key Recovery Agents authenticate to a WidePoint PIV SSP Key Encryption Database or a WidePoint PIV SSP Data Decryption Server using a public key certificate issued by a WidePoint PIV SSP Certificate Authority. When a public key certificate is used, it must be on a FIPS 140 level 2 or higher validated hardware cryptographic module. The assurance level of the certificate must be the same as or greater than that of the certificate whose corresponding private key is being recovered.

3.5.4 KEY RECOVERY OFFICIAL AUTHENTICATION

A WidePoint PIV SSP Key Recovery Official does not have access privileges to any WidePoint PIV SSP Key Encryption Database or a WidePoint PIV SSP Data Decryption Server. A WidePoint PIV SSP Key Recovery Official may request key recovery for any WidePoint PIV SSP Subscriber that they have been authorized for (i.e. a key recovery official for a particular organization or agency) but shall use their WidePoint PIV SSP Subscriber certificate that is at an assurance level equivalent to or greater than the WidePoint PIV SSP Subscriber certificate for which they are requesting recovery.

3.5.5 WIDEPOINT PIV SSP DATA DECRYPTION SERVER

A WidePoint PIV SSP Data Decryption Server or agency Data Decryption Server authenticates to a WidePoint PIV SSP KED directly using a public key certificate issued by the WidePoint PIV SSP. The assurance level of the certificate issued to a WidePoint PIV SSP Data Decryption Server or agency Data Decryption Server shall be issued with the certificate policy OID of **id-fpki-common-devicesHardware** and protected as specified in Section 6.2.1 Cryptographic Module Standards and Controls and shall be greater than the assurance levels of the certificate protected in a WidePoint PIV SSP Key Encryption Database or a WidePoint PIV SSP Data Decryption Server or agency Data Decryption Server.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

The WidePoint PIV SSP offers certificates that may assert any of the certificate policies identified in Section 1.2 of this WidePoint PIV SSP CPS. WidePoint PIV SSP CAs are configured with certificate profiles for each of the certificate policy types. Each certificate profile on each WidePoint PIV SSP CA is configured as specified in Section 7 and populated with values for each certificate type as specified in Section 10 of this WidePoint PIV SSP CPS. The certificate policies identified in Section 1.2 of this WidePoint PIV SSP CPS are encoded in the certificate profile of each WidePoint PIV SSP CA and cannot be overwritten by any certificate policy asserted in the certificate request. Certificate requests by Applicants and WidePoint PIV SSP Subscribers are submitted against a particular profile on the WidePoint PIV SSP CAs and cannot be transferred to a different profile.

The WidePoint PIV SSP CAs only recognizes WidePoint PIV SSP issued certificates for accomplishing tasks associated with the configuration, operation, and maintenance of a WidePoint PIV SSP CA. Each WidePoint PIV SSP CA is configured with an internal trust list that includes the trust chain of only WidePoint PIV SSP CAs. No external roots or certificate authorities are trusted in the internal trust store of the WidePoint PIV SSP CAs other than the roots associated with the Common Policy CA or internal roots that may be required by the certificate authority software. A WidePoint PIV SSP Subscriber can only present a WidePoint PIV SSP issued certificate to any WidePoint PIV SSP CAs under this configuration. Additional access control lists internal to the WidePoint PIV SSP CAs will grant a user with a WidePoint PIV SSP certificate privileges to the WidePoint PIV SSP CA if the WidePoint PIV SSP Subscriber's certificate is in the access control list. <REDACTED>

The WidePoint PIV SSP is not authorized to certify other certificate authorities. The WidePoint PIV SSP is not authorized to issue certificates to either a WidePoint PIV SSP subordinate certificate authority or a WidePoint PIV SSP subordinate certificate authority to an external entity or organization.

4.1.1 WHO CAN SUBMIT A CERTIFICATE APPLICATION

The WidePoint PIV SSP only accepts certificate applications from Applicants or WidePoint PIV SSP Subscribers for WidePoint PIV SSP certificate types as identified in Section 1.4.1 that will assert one of the certificate policies identified in Section 1.2 of this WidePoint PIV SSP CPS except **id-fpki-common-piv-contentSigning** and **id-fpki-common-pivi-contentSigning**. Applicants and WidePoint PIV SSP Subscribers may not submit requests for another human Applicant or WidePoint PIV SSP Subscriber but may submit requests for devices for which they are the designated WidePoint PKI Point of Contact for that device.

Certificate application requests for **id-fpki-common-devices** or **id-fpki-common-devicesHardware** are made by Applicants or WidePoint PIV SSP Subscribers who have met the obligations of a WidePoint PIV SSP PKI Sponsor as specified in Section 1.3.7.2 of this WidePoint PIV SSP CPS and will act as the human subscriber for the device for which the certificate is requested.

A WidePoint PIV SSP PKI Sponsor for a device certificate asserting a certificate policy **id-fpki-common-devices** or **id-fpki-common-devicesHardware** must accept and abide by the responsibilities of a WidePoint PIV SSP Subscriber for the certificate of the device.

The WidePoint PIV SSP does not permit certificate requests made by a WidePoint Registration Authority or WidePoint PIV SSP Trusted Agent on behalf of an Applicant or a WidePoint PIV SSP Subscriber.

Only WidePoint CAAs are authorized to request OCSP responder certificates. WidePoint does not delegate OCSP responses.

4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES

The following section describes the enrollment process for various certificates and credential types for the WidePoint PIV SSP.

4.1.2.1 WidePoint PIV SSP PIV and PIV-I Credential Enrollment Process and Responsibilities

WidePoint PIV SSP CMSs and WidePoint PIV SSP CMS workstations are used to manage the enrollment process for Applicants or WidePoint PIV SSP Subscribers who are requesting WidePoint PIV SSP PIV or PIV-I credentials.

Applicants or WidePoint PIV SSP Subscribers asserting an organizational affiliation must be authorized by a WidePoint PIV SSP PKI Point of Contact for that organization. Applicants or WidePoint PIV SSP Subscribers asserting no organization affiliation will have an organization value of "Unaffiliated" registered in all locations where an organization name value is required.

Applicants or WidePoint PIV SSP Subscribers requesting WidePoint PIV SSP PIV-I credentials are required to appear in-person before a WidePoint Registrar, as shown in the figure below, at a WidePoint Registrar Workstation for identity-proofing, in accordance with Section 3.2.3.1 of this WidePoint PIV SSP CPS to complete the enrollment process.

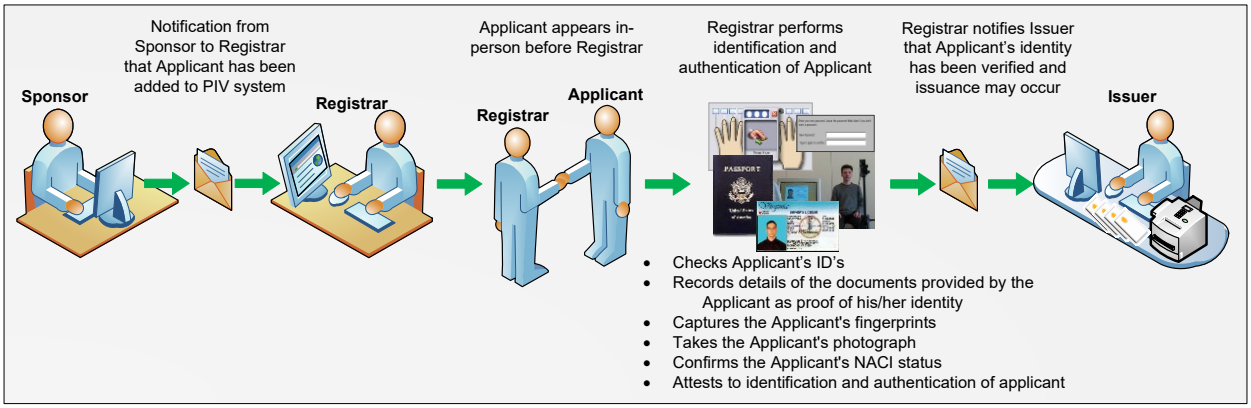

Figure 5 – WidePoint PIV SSP PIV or PIV-I Workflow

The WidePoint Registrar uses the workstation to access the WidePoint CMS having first authenticated via VPN to the WidePoint firewall with a certificate on their PIV Card, then logging into the CMS over HTTPS. The WidePoint Registrar, upon identity verification, will capture the following from the Applicant or WidePoint PIV SSP Subscriber if it has not already been preloaded by the WidePoint PIV SSP PKI Point of Contact into the WidePoint CMS:

- Validity period requested (max 3 years);
- Organization name
- First name
- Middle name or initial
- Last name
- Email address
- Location (either United States or non-United States); and,
- Contact phone information.

Additionally, the WidePoint Registrar captures the biometrics of the Applicant or WidePoint PIV SSP Subscriber. These biometrics include:

- Fingerprints of both index fingers (substitution of fingers are allowed); and,
- Digital photo of the Applicant or Subscriber
- Hair color - optional
- Eye color - optional.

Upon confirmation of the information provided and capture of the Applicant or WidePoint PIV SSP Subscriber's biometrics, the WidePoint Registrar will approve the Applicant or WidePoint PIV SSP Subscriber's request for a WidePoint PIV SSP PIV or PIV-I credential. This action asserts that the WidePoint Registrar has vetted and gathered the necessary information for the Applicant or WidePoint PIV SSP Subscriber and that the WidePoint Registrar has

certified that the Applicant or WidePoint PIV SSP Subscriber may move to the issuance process controlled by the WidePoint Issuer.

4.1.2.2 WidePoint PIV SSP Derived Certificate Enrollment Process and Responsibilities

Applicants and WidePoint PIV SSP Subscribers requesting certificates that assert a certificate policy OID of **id-fpki-common-derived-pivAuth** or **id-fpki-common-derived-pivAuth-hardware** present their current and valid PIV card which contains their certificate that asserts the certificate policy OID of **id-fpki-common-authentication (PIV authentication)** to the WidePoint PIV SSP Derived Credential Enrollment Server. The WidePoint PIV SSP Derived Credential Enrollment Server challenges the Applicant or WidePoint PIV SSP Subscriber for their PIN in order to access the PIV Authentication certificate on the card. Upon receipt of the correct PIN, the WidePoint PIV SSP Derived Credential Enrollment Server reads the card and generates a Quick Response (QR) Code, which is presented over HTTPS within a browser. The Applicant or WidePoint PIV SSP Subscriber scans the QR code using a mobile app. A certificate request is generated and sent to a WidePoint PIV SSP Certificate Authority, which processes the request and issues a certificate to the mobile device.

4.1.2.3 WidePoint PIV SSP CA signing certificate request process and Responsibilities

Requests for new WidePoint PIV SSP CA signing certificates are submitted to the FPKIPA using the contact designated in Section 1.5.3 of this WidePoint PIV SSP CPS and are accompanied by a current version of this WidePoint PIV SSP CPS.

WidePoint PIV SSP CAs only issue certificates asserting the certificate policies defined in Section 1.2 of this WidePoint PIV SSP CPS only after authorization from the FPKIPA and then only within the constraints imposed by the FPKIPA or its designated representatives.

4.1.2.4 Device Enrollment Process and Responsibilities

The WidePoint PIV SSP Sponsor requesting certificates that assert a certificate policy OID of **id-fpki-common-devices** or **id-fpki-common-devicesHardware** are required to appear in person before a WidePoint Registration Authority, a WidePoint Local Registration Authority, or a Trusted Agent, as defined in Section 1.3 of this WidePoint PIV SSP CPS for Initial Identity Validation, in accordance with Section 3.2 for Identity Proofing within the United States or Section 11 for Identity Proofing Outside the United States. The WidePoint PIV SSP Sponsor acts as the WidePoint PIV SSP Subscriber for the device for which they are requesting a certificate.

Upon acceptance by the WidePoint PIV SSP Sponsor of the Component Obligations, the WidePoint PIV SSP Sponsor will submit the certificate request with their component specific information and their user information in accordance with Section 3.1.1 of this WidePoint PIV SSP CPS. This information will include:

- Validity period requested (max 3 years).
- Component specific information (Server SSL including Multi-SAN, Domain Controller and Device Identity).
- PKCS 10 formatted request string.
- Server DNS name.
- Server IP (optional)
- Global Unique Identifier (GUID) – for Domain Controller and Device Identity
- Other unique Component identification – depending upon requirements of the device to be credentialed
- WidePoint PIV SSP Sponsor specific information:
    - First name
    - Middle name or initial
    - Last name
    - Organization name
    - Email address
    - Citizenship
    - Location (either United States or Non-United States)
    - Contact phone information

The WidePoint PIV SSP Sponsor submits the PKCS#10 formatted request and the data entered for Component and Subscriber information to the WidePoint PIV SSP for processing. The WidePoint PIV SSP, upon receiving the WidePoint PIV SSP Sponsor's Component request data, will verify and process the request and return a request confirmation form populated with the request information that is to be printed by the WidePoint PIV SSP Sponsor, completed and taken either to a WidePoint Registration Authority or a Trusted Agent as specified in Section 1.3.7.1 for identity verification as described in Section 3.2.3.1 of this WidePoint PIV SSP CPS.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

All certificate requests will be validated through the authentication procedures defined in Section 3 of this WidePoint PIV SSP CPS. The Applicant or WidePoint PIV SSP Subscriber is responsible for presenting the required information for identity verification to the WidePoint Registration Authority, WidePoint Local Registration Authority or Trusted Agent for certificates that will assert a certificate policy OID of **id-fpki-common-policy**, **id-fpki-common-hardware**, **id-fpki-common-devices**, or **id-common-devicesHardware** or a WidePoint Registrar in the case of WidePoint PIV SSP PIV or PIV-I credentials. For certificate requests for certificate requests that will assert a certificate policy OID of **id-fpki-common-derived-pivAuth** or **id-fpki-common-derived-pivAuth-hardware** shall accept the presentation of the Applicant or WidePoint PIV SSP Subscriber's current and valid PIV Credential and their certificate that asserts a certificate policy OID of **id-fpki-common-authentication** as their identity verification.

Upon receipt of a complete certificate request and identity validation package from the Applicant or WidePoint PIV SSP Subscriber, a WidePoint Local Registration Authority will verify that the identity validation procedure has been correctly and completely followed as appropriate for the certificate policy requested and as stipulated in Section 3 of this WidePoint PIV SSP CPS. The verifying WidePoint PIV SSP Local Registration Authority will send a digitally signed message to a WidePoint Registration Authority approving the Applicant or WidePoint PIV SSP Subscriber's certificate request and providing a copy of the DN, the subject alternate name, hereafter referred to as SAN, if applicable, the certificate request unique identifier, and the certificate policy for which the Applicant or WidePoint PIV SSP Subscriber identity was authenticated. In no case will WidePoint PIV SSP certificates be issued prior to proper identity authentication.

4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

Identification and authentication procedures will be performed as detailed in Section 3 and Section 4.2.1.

No certificates will be issued prior to proper authentication. A WidePoint PIV SSP Registration Authority or a WidePoint PIV SSP Local Registration Authority will deny issuance if:

- the WidePoint PIV SSP Registration Authority or WidePoint PIV SSP Local Registration Authority does not send a digitally signed issuance request email; or,
- the email is missing any of the requisite information or the email is signed with a lower assurance certificate than that being requested, as listed in Section 4.2.1 of this WidePoint PIV SSP CPS; or,
- the Applicant or WidePoint PIV SSP Subscriber fails to provide documentation verifying their name, citizenship, or organizational affiliation.

If the certificate request is denied, the WidePoint PIV SSP will not sign the requested certificate, and will work, within good reason, with the Applicant or the WidePoint PIV SSP Subscriber to resolve the problem.

For the WidePoint PIV SSP PIV-I credentials, the WidePoint PIV SSP will deny issuance if the documents presented to the WidePoint Issuer are different from those recorded by the WidePoint Registrar. The WidePoint PIV SSP will also deny issuance if the WidePoint Issuer cannot verify the identity and citizenship of the Applicant or WidePoint PIV SSP Subscriber based on the documentation provided, as specified in Section 3.2.3.1 of this WidePoint PIV SSP CPS.

The WidePoint PIV SSP CA is configured to enforce requirements specified by NIST SP 800-89 and NIST SP 800-56A.

4.2.3 Time to Process Certificate Applications

The entire process from Applicant or WidePoint PIV SSP Subscriber appearing before a WidePoint Registration Authority, a WidePoint PIV SSP Local Registration Authority, or a Trusted Agent for identity verification to certificate issuance will take no more than 90 days. All certificate requests are verified by a WidePoint Local Registration Authority prior to issuance to confirm that the issuance would be within the 90-day window described above and reject any requests that are received beyond 90 days from date of identity verification.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

<REDACTED>

In the case of WidePoint PIV SSP PIV or PIV-I credential issuance, the WidePoint PIV SSP Issuer accesses a WidePoint PIV SSP CMS workstation by authenticating with their WidePoint PIV SSP PIV or PIV-I credential to the WidePoint PIV SSP CMS. The WidePoint PIV SSP CMS workstation is comprised of a desktop or laptop and various peripherals, as shown below in Figure 8.

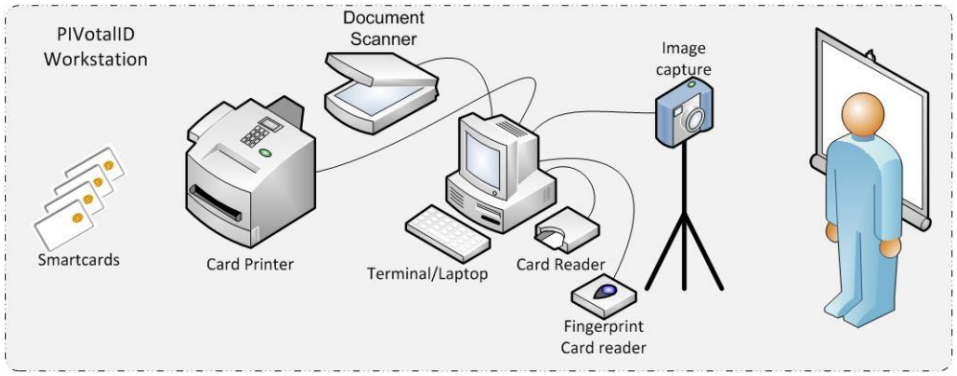

Figure 8 – WidePoint PIV SSP CMS Workstation Components

The Applicant or WidePoint PIV SSP Subscriber must appear in person before a WidePoint PIV SSP Issuer at a WidePoint PIV SSP CMS workstation. A WidePoint PIV SSP Issuer will compare the identity documentation provided by the Applicant or the WidePoint PIV SSP Subscriber against the identity documentation presented and recorded during the registration process described in Section 4.1.2.3. Upon successful verification of the identity documentation, the WidePoint PIV SSP Issuer will print the Subscriber's PIV or PIV-I credential. After the card has been successfully printed, the Applicant or WidePoint PIV SSP Subscriber will authenticate with one of the fingerprints captured during the registration process and create a numeric PIN as specified in Section 6.4.1. Upon successful fingerprint match and setting of PIN, the Applicant or WidePoint PIV SSP Subscriber's card begins the activation process. Upon successful completion of the WidePoint PIV SSP PIV or PIV-I Credential Activation, the Applicant or WidePoint PIV SSP Subscriber must attest to the WidePoint PIV SSP Subscriber Obligations as detailed in Section 9.6.4 of this WidePoint PIV SSP CPS.

Upon acceptance by the Applicant or WidePoint PIV SSP Subscriber of the WidePoint PIV SSP Subscriber Obligations, the WidePoint PIV SSP Issuer will release the activated PIV or PIV-I credential to the Subscriber.

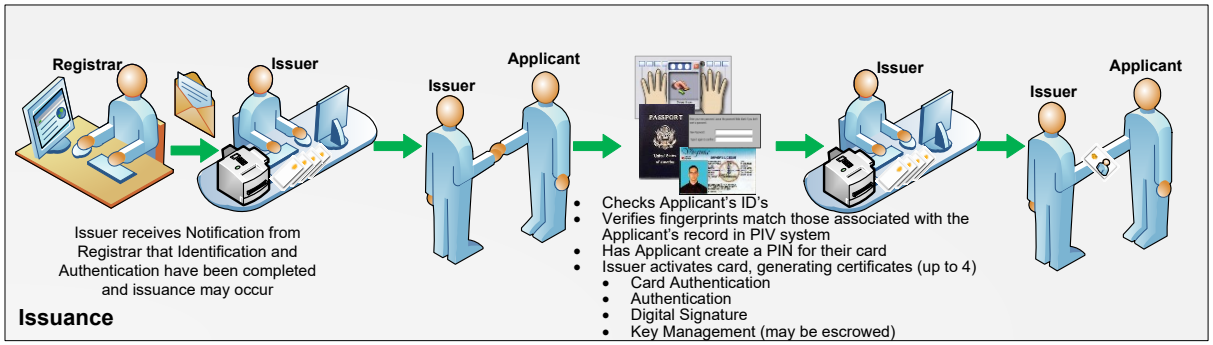

Figure 9 – WidePoint PIV SSP Issuer Workflow

For **id-fpki-common-devices**, **id-fpki-common-devicesHardware**, **id-fpki-common-derived-pivAuth**, **id-fpki-common-derived-pivAuth-hardware**, upon successful completion of the subscriber identification and authentication process in accordance with Section 3.2.3, Authentication of Individual Identity, of this WidePoint PIV SSP CPS, WidePoint creates the requested certificate, notifies the applicant thereof, and, after ensuring that the Subscriber has formally acknowledged his/her obligations in accordance with Section 9.6.3, Subscriber Representations and Warranties, makes the certificate available to the applicant.

For **id-fpki-common-derived-pivAuth**, a WidePoint PIV SSP RA issues the certificate by clicking on a button at the WidePoint PIV SSP DCE site.

WidePoint PIV SSP does not accept or allow for additional authorization or attribute information from Applicants for inclusion in certificates.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

For all certificate types except WidePoint PIV SSP PIV or PIV-I credentials, WidePoint PIV SSP Registration Authorities will notify the WidePoint PIV SSP Subscriber of certificate issuance through electronic mail. The notification will include the URL that the WidePoint PIV SSP Subscriber will use to receive the approved certificate. The WidePoint PIV SSP uses a delivery template Certificate Issuance Notification (CIN) email which contains a URL to download the WidePoint PIV SSP Subscriber's issued certificate based on the issuing WidePoint PIV SSP CA and WidePoint PIV SSP Subscriber's certificate serial number. The WidePoint PIV SSP will verify possession of the WidePoint PIV SSP Subscriber's private key at the time the WidePoint PIV SSP Subscriber accepts the issued certificate, as described in Section 3.2.1 of this WidePoint PIV SSP CPS.

The notification will inform the WidePoint PIV SSP Subscriber of the creation of a certificate, direct the WidePoint PIV SSP Subscriber to the certificate contents page, and reaffirm their responsibilities. The notification will inform the WidePoint PIV SSP Subscriber that the private key for their encryption certificate has been escrowed if applicable.

The WidePoint PIV SSP Subscriber will import their certificate(s) from the WidePoint PIV SSP CA. The WidePoint PIV SSP CA will perform a proof of possession test to ensure the public key of the certificate requested is paired with the correct private key. Successful importation of the certificate by the WidePoint PIV SSP Subscriber constitutes acceptance. Additionally, the WidePoint PIV SSP logs the acceptance of the certificate by the WidePoint PIV SSP Subscriber.

For device certificates, the WidePoint PIV SSP Sponsor of the certificate will act as the WidePoint PIV SSP Subscriber.

For WidePoint PIV SSP PIV or PIV-I credentials, the WidePoint PIV SSP Issuer authorizes the WidePoint PIV SSP CMS to authenticate to the WidePoint PIV SSP CA with its internal connector certificate that is a trusted user on the WidePoint PIV SSP CA. The WidePoint PIV SSP CA creates all certificates for the WidePoint PIV SSP PIV or PIV-I credentials, generates, and escrows the encryption private key and recovers any previous encryption keys

escrowed for the WidePoint PIV SSP Subscriber. This process is conducted in the presence of the WidePoint PIV SSP Subscriber and the Subscriber is notified as part of the Certificate Acceptance process as defined in Section 4.4 Certificate Acceptance below.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

A handwritten or digital signature by the WidePoint PIV SSP Subscriber or the WidePoint PIV SSP Sponsor obtained during the WidePoint PIV SSP certificate application process and lack of objection to published certificate constitutes certificate acceptance by the WidePoint PIV SSP Subscriber or the WidePoint PIV SSP Sponsor. The WidePoint PIV SSP Subscriber or WidePoint PIV SSP Sponsor signature is collected prior to the issuance of any WidePoint PIV SSP certificate in accordance with the procedures specified in this WidePoint PIV SSP CPS and before the WidePoint PIV SSP Subscriber or the WidePoint PIV SSP Sponsor can make effective use of the private key associated with the certificate issued by the WidePoint PIV SSP. As part of the issuance process of WidePoint PIV SSP PIV or PIV-I credentials, the WidePoint PIV SSP Subscriber accepts the issued certificate during the issuance process by accepting the Subscriber obligations prior to completion of the PIV or PIV-I issuance completion. This acceptance requires the Subscriber to provide their PIN that protects the PIV or PIV-I credential. This PIN was selected by and is only known by the WidePoint PIV SSP Subscriber.

4.4.2 Publication of the Certificate by the WidePoint PIV SSP

The WidePoint PIV SSP CA certificates and WidePoint PIV SSP Subscriber certificates are published to the WidePoint PIV SSP repositories as defined in Section 2.1 and whose contents are defined by Section 2.2 of this WidePoint PIV SSP CPS. Certificates that contain the FASC-N and/or UUID in the subject alternative name extension, such as PIV or PIV-I Authentication Certificates, are not to be distributed via public repositories as described in Section 2 of this WidePoint PIV SSP CPS.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The WidePoint PIV SSP will notify the FPKIPA at least two weeks prior to a request for the issuance of a new WidePoint PIV SSP CA certificate from the Common Policy CA or for subordinate Certificate Authorities issued by the WidePoint PIV SSP for customer agencies. In addition, notification will be provided to the FPKIPA when the new WidePoint PIV SSP CA or Subordinate CA certificates are published and activated.

The WidePoint PIV SSP does not issue CA certificates to other organizations. All issued CA certificates (including subordinates) are hosted at WidePoint.

4.5 Key Pair and Certificate Usage

4.5.1 WidePoint PIV SSP Subscriber Private Key and Certificate Usage

The WidePoint PIV SSP Subscriber and the WidePoint PIV SSP Sponsor in the case of device certificates attest to their obligations as specified in Section 9.6.3 of this WidePoint PIV SSP CPS. These obligations do not permit use of private signature keys once the associated certificate has been revoked, restrict use of encryption private keys to only decrypt previously encrypted information after the associated certificate has been revoked or has expired, and limit the use of private key to the stated uses in the key usage extension of the associated certificate as well as the extended key usage extension if it is present and implies any further limitation.

4.5.2 Relying Party Public Key and Certificate Usage

The WidePoint PIV SSP will publicly post a summary of this WidePoint PIV SSP CPS on the WidePoint PIV SSP Repositories as specified in Section 2.1 to provide Relying Parties information regarding the expectation of the WidePoint PIV SSP and use of certificates issued to WidePoint PIV SSP Subscribers. Relying Parties shall ensure that a public key in a certificate is used only for the purposes indicated by the key usage extension, if the extension is present, as well as any implied limitation asserted in the extended key usage extension, if any is present, in the WidePoint PIV SSP issued certificate. Additional Relying Party obligations are stipulated in Section 9.6.4 of this WidePoint PIV SSP CPS.

4.6 CERTIFICATE RENEWAL

WidePoint PIV SSP Subscribers are notified 30 days prior to expiration of their certificate via an automated email from the WidePoint PIV SSP. A follow up expiration notice is sent to the WidePoint PIV SSP Subscriber 15 days prior to expiration via automated email. The automated email to the WidePoint PIV SSP Subscriber provide a link to a client authenticated TLS webpage, hereafter referred to as the WidePoint PIV SSP Renewal Portal, where the WidePoint PIV SSP Subscriber may submit a certificate renewal request.

The WidePoint PIV SSP Renewal Portal accepts electronic authentication for certificate renewal using currently valid WidePoint PIV SSP Subscriber digital certificates that assert a certificate policy of **id-fpki-common-hardware**. The WidePoint PIV SSP Renewal Portal prompts the WidePoint PIV SSP Subscriber to present a digital certificate for renewal and checks that:

- The certificate presented was issued by the WidePoint PIV SSP.
- The certificate presented has a private key associated with it.
- The certificate presented is a digital signature certificate.
- The certificate is not expired.
- The certificate is within 30 days of its expiration date; and,
- The certificate is currently valid and does not appear on the CRL of the WidePoint PIV SSP CA that issued the certificate.

Upon successful authentication and validation of the above conditions, the WidePoint PIV SSP captures data elements from the WidePoint PIV SSP Subscriber's presented certificate to include:

- The WidePoint PIV SSP CA that issued the certificate.
- The DN of the certificate being renewed.
- The certificate policy object identifier asserted in the certificate; and,
- The certificate serial number.

The WidePoint PIV SSP Renewal Portal searches the WidePoint PIV SSP Repository for the original request tied to the WidePoint PIV SSP Subscriber certificate presented and retrieves that information for use in the WidePoint PIV SSP Subscriber's renewal submittal form. Additionally, the WidePoint PIV SSP Renewal Portal searches the WidePoint PIV SSP Repository for the currently valid encryption certificate that has been issued to the WidePoint PIV SSP Subscriber. The WidePoint PIV SSP Renewal Portal retrieves the original request information for the encryption certificate for use in the WidePoint PIV SSP Subscriber's renewal submittal form.

The WidePoint PIV SSP Renewal Portal captures the certificate policy from the certificate presented by the WidePoint PIV SSP Subscriber. The certificate policy from the presented certificate is used to verify that the next in-person authentication date, as specified in Section 3.3.1, will not be exceeded or that the number of renewals permitted without in-person authentication by the issuance of a renewed certificate will not be exceeded for the certificate policy asserted in the WidePoint PIV SSP Subscriber certificate presented. The WidePoint PIV SSP Renewal Portal accomplishes this by checking flag fields in the WidePoint PIV SSP Subscriber's entry in the WidePoint PIV SSP Repository that are set during the WidePoint PIV SSP Subscriber's first certificate issuance. This flag field has values of 0, 1, 2 or 3 to denote the number of renewals performed by the Subscriber without in-person authentication. A value of 3 denotes that the user has performed three (3) renewals without in-person authentication and will not be allowed to complete the renewal process and be directed to the in-person authentication process to obtain new keys and certificates. If the value of the flag field is 0, 1 or 2, the WidePoint PIV SSP Subscriber may submit renewal requests for their digital signature and encryption (if applicable) certificates at this time.

In the case of a certificate presented for renewal that asserts a certificate policy object identifier of **id-fpki-common-hardware**, the WidePoint PIV SSP Renewal Portal will check the validity period of the certificate to be renewed. If the validity period of the certificate to be renewed is 3 years, the WidePoint PIV SSP Subscriber will not be allowed to complete the renewal process and will be directed to the process for in-person authentication for a new certificate. Similarly, if the certificate presented for renewal that assert **id-fpki-common-hardware** to be renewed has a current validity of 1 or 2 years, the WidePoint PIV SSP Renewal Portal will only allow the WidePoint

PIV SSP Subscriber to request a renewal validity period such that the total validity period of the original certificate and its renewal certificate does not exceed 3 years.

WidePoint PIV SSP Subscriber renewal requests are then pre-populated with the information from the previous requests and issued certificates and are unalterable by the WidePoint PIV SSP Subscriber. This information will include:

- The certificate policy of the certificate to be renewed is contained in the original request retrieved by the WidePoint PIV SSP. This retrieved record contains the profile information on the WidePoint PIV SSP that created the certificate presented during electronic authentication and the renewal request is submitted against that same profile. The WidePoint PIV SSP Subscriber is unable to change the certificate policy during the renewal process.
- The DN of the certificate to be renewed which contains the WidePoint PIV SSP Unique Identification String previously assigned.
- All data in certificate that can be used to provide authentication information such as email address, Public Key Information and Subject Key Information.
- Validity period submitted by the WidePoint PIV SSP Subscriber of the renewal request cannot exceed the maximum key life determined by this WidePoint PIV SSP CPS and Common Policy for the certificate policy requested. The maximum validity period that the WidePoint PIV SSP Subscriber can request is 3 years; and,
- A unique request ID number assigned by the WidePoint PIV SSP.

When a successful renewal request is made, the WidePoint PIV SSP Renewal Portal presents a request form to the WidePoint PIV SSP Subscriber. The WidePoint PIV SSP Subscriber is directed to print the request form for each renewal certificate requested. Each printed form includes the unique request number for each renewal certificate requested (i.e., a unique request number for the identity certificate and a unique request number for the encryption certificate). The WidePoint PIV SSP Subscriber then transmits the renewal request form to a WidePoint PIV SSP Registration Authority or WidePoint PIV SSP Local Registration Authority. If the renewal request form is transmitted to a WidePoint PIV SSP Local Registration Authority, the WidePoint PIV SSP Local Registration Authority will send a digitally signed email requesting that the renewal certificates be issued. The WidePoint PIV SSP Local Registration Authority then sends a digitally signed email that includes the request ID numbers to the WidePoint PIV SSP Registration Authority requesting issuance of the renewal certificate(s) based on the WidePoint PIV SSP Subscriber's electronic authentication when making the renewal request as described in Section 4.3.1. This procedure for certificate renewal, thereby, parallels the procedure for initial certificate issuance except that identity verification is not performed and key generation is not witnessed, since no keys are generated.

Upon receipt of the printed WidePoint PIV SSP Subscriber Certificate renewal request forms from the WidePoint PIV SSP Subscriber, or a digitally-signed email containing certificate renewal request information (including the request ID number) from an approved WidePoint PIV SSP Local Registration Authority for the organization for which the certificate has been issued and is requested, a WidePoint PIV SSP Local Registration Authority performs a manual search of the WidePoint PIV SSP Repository for both the CN value of the certificate to be renewed and for the desired CN value of the new certificate. The WidePoint PIV SSP Local Registration Authority examines all prior certificate issuances to the named WidePoint PIV SSP Subscriber. Since the renewed public portion of the WidePoint PIV SSP Subscriber certificate will only import into the FIPS 140-3 Level 2 secure container (i.e., a cryptographic token or a smart card) that protects the corresponding private key, only that secure container may ever hold either the WidePoint PIV SSP Subscriber's expiring or renewed certificate. When the WidePoint PIV SSP Subscriber's renewed certificate is imported into the secure container, the WidePoint PIV SSP Subscriber's expiring public certificate is overwritten. Only one version of the WidePoint PIV SSP Subscriber's certificate can be present on the secure container. When the WidePoint PIV SSP Subscriber's renewed certificate is imported, the WidePoint PIV SSP Subscriber's expiring certificate is destroyed. Therefore, a WidePoint PIV SSP Subscriber cannot be in possession of both the old certificate (eligible for renewal) and the new (renewed) certificate at the same time. If a renewal certificate issuance has occurred within the previous 30 days, the WidePoint PIV SSP Local Registration Authority will not forward the request for issuance, the WidePoint PIV SSP LRA will contact the WidePoint PIV SSP Subscriber to ensure the proper importation of the previously renewed WidePoint PIV SSP Subscriber certificate. This procedure ensures that a WidePoint PIV SSP Subscriber certificate is not further renewed or rekeyed.

In all cases, the WidePoint PIV SSP may request additional information or verification if deemed necessary to confirm the requestor's identity. A WidePoint Local Registration Authority will contact the Subscribers via phone or email.

4.6.1 Circumstances for Certificate Renewal

The WidePoint PIV SSP accepts requests for certificate renewal pursuant to the following circumstances:

- The public key of the WidePoint PIV SSP Subscriber certificate presented has not reached the end of its validity.
- The WidePoint PIV SSP Subscriber certificate presented has not been revoked.
- The total lifetimes of certificate issued to the WidePoint PIV SSP Subscriber (including the renewal requested) for that public key has not exceeded the next in-person identity proofing date required by the certificate policy asserted.
- The associated private key of the WidePoint PIV SSP Subscriber certificate presented has not been compromised; and,
- The WidePoint PIV SSP Subscriber name and attributes in the current valid certificate have not changed.

WidePoint PIV SSP Subscribers are notified via automated email, 30 days prior to expiration and again 15 days prior to expiration, that their certificates will soon expire. The automated email to the WidePoint PIV SSP Subscriber provides a link to the WidePoint PIV SSP Renewal Portal where WidePoint PIV SSP Subscribers may submit certificate renewal requests.

4.6.2 Who May Request Renewal

All WidePoint PIV SSP Subscribers who have certificates that assert a certificate policy of **id-fpki-common-hardware** may submit requests to have their certificates renewed.

4.6.3 Processing Certificate Renewal Requests

The WidePoint PIV SSP Subscriber certification renewal process is in accordance with the certificate issuance process described in Section 4.3 of this WidePoint PIV SSP CPS. Identity validation is in accordance with either Section 3.2.3.1 or Section 3.2.3.2 of this WidePoint PIV SSP CPS.

4.6.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2 of this WidePoint PIV SSP CPS.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

See Section 4.4.1 of this WidePoint PIV SSP CPS.

4.6.6 Publication of the Renewal Certificate by the CA

See Section 4.4.2 of this WidePoint PIV SSP CPS.

4.6.7 Notification of Certificate Issuance by the CA to other Entities

See Section 4.4.3 of this WidePoint PIV SSP CPS.

4.7 Certificate Re-Key

The WidePoint PIV SSP only accepts electronic authentication for certificate re-key for currently valid digital WidePoint PIV SSP Subscriber certificates issued by the WidePoint PIV SSP that assert a certificate policy of **id-fpki-common-policy**. The WidePoint PIV SSP does not offer certificate re-key for WidePoint PIV SSP Subscribers certificates that assert any other certificate policy as described in Section 1.2 of this WidePoint PIV SSP CPS but may renew those certificates if they meet the requirements as specified in Section 4.6 of this WidePoint PIV SSP CPS. WidePoint PIV SSP Subscriber certificate re-key follows the same process as defined in Section 4.6 with the exception that a new key-pair is generated for the WidePoint PIV SSP Subscriber certificate instead of using the previous existing key-pair. Once a certificate has been re-keyed, the old certificate may or may not be revoked, but shall not be reused for requesting further renewals, re-keys, or modifications.

4.7.1 Circumstances for Certificate Re-Key

The WidePoint PIV SSP accepts requests for certificate re-key pursuant to the following circumstances:

- The WidePoint PIV SSP Subscriber certificate can no longer be renewed, as stipulated in Section 4.6.
- The WidePoint PIV SSP Subscriber certificate has not been revoked.
- Total lifetime of certificates issued to the WidePoint PIV SSP Subscriber (including new certificate) for that public key has not exceeded the next in-person identity proofing date.
- The WidePoint PIV SSP Subscriber's name and attributes in the current valid certificate remain the same.

WidePoint PIV SSP Subscribers are notified via automated email, 30 days prior to expiration and again 15 days prior to expiration, that their certificates will soon expire. The automated email to the WidePoint PIV SSP Subscriber provide a link to the WidePoint PIV SSP Renewal Portal where WidePoint PIV SSP Subscribers may submit certificate re-key requests.

The WidePoint PIV SSP does not re-key WidePoint PIV SSP Certificate Authorities or subordinate Certificate Authorities.

Section 6.3.2, Certificate Operational Periods and Key Pair Usage Periods, defines usage periods for private keys.

4.7.2 Who May Request Certification of a New Public Key

All WidePoint PIV SSP Subscribers who have certificates that assert a certificate policy of **id-fpki-common-policy** may submit requests to have their certificates re-keyed.

4.7.3 Processing Certificate Re-Keying Requests

The WidePoint PIV SSP Subscriber certificate re-keying process is in accordance with the certificate issuance process described in Section 4.3 of this WidePoint PIV SSP CPS. Identity validation may be in accordance with either Section 3.2.3.1 or Section 3.2.3.2 of this WidePoint PIV SSP CPS.

WidePoint PIV SSP Subscriber requests for certificate re-key are marked as a certificate renewal request.[2] A WidePoint PIV SSP LRA will search the WidePoint PIV SSP Repository for the WidePoint PIV SSP Subscriber's current and valid certificate to confirm eligibility to re-key as specified in Section 4.7 of this WidePoint PIV SSP CPS. Upon confirmation, the WidePoint PIV SSP LRA sends a digitally signed email to a WidePoint PIV SSP RA similar to the email sent for initial registration but containing the current and valid certificate's pending expiration date. Prior to issuance, a WidePoint PIV SSP RA performs a manual search of the WidePoint PIV SSP Repository for the CN value of the WidePoint PIV SSP Subscriber certificate to be re-keyed. The new WidePoint PIV SSP Subscriber certificate is based on new key pairs, generated in accordance with Section 6.1.1 of this WidePoint PIV SSP CPS. The new WidePoint PIV SSP Subscriber certificate is issued with a validity start date one day prior to the expiration date of the expiring certificate allowing the WidePoint PIV SSP Subscriber one (1) day to transition from the expiring certificate(s) to the new certificate(s). No WidePoint PIV SSP Subscriber certificate may be re-keyed after expiration. Additionally, the WidePoint PIV SSP will not issue a certificate such that the WidePoint PIV SSP Subscriber would have more than one current and valid certificate asserting the same certificate policy OID. If a WidePoint PIV SSP Subscriber should make such a certificate request, the WidePoint PIV SSP Registration Authority would revoke any certificate that would otherwise lead to a WidePoint PIV SSP Subscriber possessing more than one valid certificate at one time. Such situations can arise when a WidePoint PIV SSP Subscriber experiences technical issues and has failed to make operational copies of their certificates where permissible. The WidePoint PIV SSP does not revoke the certificate in the case where a certificate nearing expiration is re-keyed to produce a certificate that becomes valid as the old certificate expires.

Identity validation for the WidePoint PIV SSP Subscriber is performed in accordance with Section 3.3 of this WidePoint PIV SSP CPS.

[2] The use of the term "renewal" is used for simplification on the part of the subscriber so as not to confuse between renew and re-key. This is done for internal use only.

4.7.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

See Section 4.4.1.

4.7.6 Publication of the Re-Keyed Certificate by the CA

See Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.8 Certificate Modification

Updating a WidePoint PIV SSP Subscriber certificate means creating a new certificate that has a different subject public key, a different serial number, and differs in one or more other fields, from the old certificate. For example, the WidePoint PIV SSP may choose to update a certificate of a WidePoint PIV SSP Subscriber who mistyped their email address. The old certificate is revoked, and therefore cannot be further re-keyed, renewed, or updated.

The WidePoint PIV SSP will authenticate the validity of any authorizations using the same means as for the initial authorization or means of equal or greater security and assurance.

When certificate modification becomes necessary and is allowed, a WidePoint PIV SSP RA or LRA searches the WidePoint PIV SSP Repository for both the CN value of the certificate to be modified and for the desired CN value of the new certificate. In the case of certificate modification, the modified certificate is issued with the same public key as the original certificate. WidePoint issues the modified certificate with the same validity dates as the original certificate, but with a new serial number. Modifications do not extend the life of the certificate.

The WidePoint PIV SSP does not accept modification for certificates that assert a certificate policy of **id-fpki-common-hardware, id-fpki-common-authentication, id-fpki-common-cardAuth, id-fpki-common-pivi-authentication, id-fpki-common-pivi-cardAuth, id-fpki-common-piv-contentSigning** or **id-fpki-common-pivi-contentSigning**. If a certificate that asserts a certificate policy of **id-fpki-common-authentication**, **id-fpki-common-cardAuth**, **id-fpki-common-pivi-authentication**, or **id-fpki-common-pivi-cardAuth**, requires modification a new WidePoint PIV SSP PIV or PIV-I Credential is created, and new certificates are issued.

4.8.1 Circumstances for Certificate Modification

WidePoint PIV SSP Certificate Authority and WidePoint PIV SSP Certificate Status Services certificates whose characteristics have changed (e.g., assert new policy OID) may be modified.

A WidePoint PIV SSP Subscriber certificate may be modified if some of the information, such as the e-mail address, has changed.

If the WidePoint PIV SSP Subscriber's name has changed, the WidePoint PIV SSP Subscriber must undergo the initial registration process.

4.8.2 Who May Request Certificate Modification

A WidePoint PIV SSP Subscriber may request certificate modification by contacting their WidePoint PIV SSP Agency PKI Point of Contact. The WidePoint PIV SSP Agency PKI Point of Contact will validate any changes in the WidePoint PIV SSP Subscriber's authorizations reflected in the certificate such as email address, or length of validity period 1, 2, or 3 years. The WidePoint PIV SSP Agency PKI Point of Contact confirms the desired modification and forwards the modification request to agency staff serving as WidePoint PIV SSP Registration Authority.

4.8.3 Processing Certificate Modification Requests

WidePoint PIV SSP Subscribers may submit requests for certificate modification in writing, via email, or via help-desk requests. WidePoint PIV SSP personnel may verify the need for the modification and gather the necessary certificate data as identified in Section 4.8.2 to pass on to a WidePoint PIV SSP RA or LRA. WidePoint PIV SSP

personnel may gather data and make recommendations but do not have a trusted role in the process. Information gathered by and sent from WidePoint PIV SSP personnel is sent by email or recorded in a help desk application. The request for certificate modification is assigned to a WidePoint PIV SSP LRA for processing. The WidePoint PIV SSP LRA reviews the requested modification and all records related to the certificate issuance. Upon successful review, the WidePoint PIV SSP LRA will forward the certificate modification request to the WidePoint PIV SSP RA for issuance. The WidePoint PIV SSP LRA may contact the WidePoint PIV SSP Subscriber to gather amplifying information and evidence or reject the request if sufficient information and evidence cannot be obtained. A modified certificate will use a different subject public key from the original certificate. Proof of all subject information changes is required.

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2

4.8.5 Conduct Constituting Acceptance of a Modified Certificate

See Section 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

See Section 4.4.2.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

A WidePoint PIV SSP Subscriber, or the Sponsoring Organization (where applicable), is responsible for promptly requesting revocation of any WidePoint PIV SSP Subscriber certificate for any of the reasons listed below. WidePoint PIV SSP Subscriber certificates will only be revoked in the following circumstances:

- The certificate holder requests that the certificate be revoked.
- The certificate holder can be shown to have violated the WidePoint PIV SSP Subscriber Obligations, including non-payment of any required fees.
- The certificate holder is no longer authorized to hold the certificate (e.g., termination of employment, change in responsibilities);
- The information in the certificate is no longer accurate so that identifying information needs to be changed (e.g., change of name or privilege attributes asserted in the Subscriber's certificate are reduced).
- The WidePoint PIV SSP Subscriber's employer or organization requests revocation.
- The certificate was obtained by fraud or mistake.
- The certificate was not correctly requested, issued, or accepted.
- The certificate contains incorrect information, is defective or creates a possibility of incorrect reliance or usage.
- Certificate private key compromise is suspected; and,
- The certificate holder fails to make a payment or other contractual obligations related to the certificate.

Whenever any of the above circumstances occur, the associated certificate will be revoked and placed on the CRL for the WidePoint PIV SSP CA that issued the certificate. In addition, if it is determined subsequent to issuance of new certificates that a private key used to sign requests for one or more additional certificates may have been compromised at the time the requests for additional certificates were made, all certificates authorized via that compromised key from the date of known compromise forward will be revoked, as detailed in Section 4.9.12. WidePoint PIV SSP certificates will remain on the CRL of the WidePoint PIV SSP CA that issued the certificates until they expire. Revoked WidePoint PIV SSP certificates are removed from the respective CRL upon their expiration but must at least appear in one CRL.

WidePoint PIV SSP Subscribers leaving the organization that sponsored their participation are required to surrender to their organization's WidePoint PIV SSP PKI Point of Contact through any accountable mechanism all cryptographic hardware tokens that were issued, under the sponsoring organization, prior to leaving the organization. The sponsoring organization is responsible for taking possession of all cryptographic hardware tokens containing WidePoint PIV SSP certificates and issued under the sponsoring organization. The PKI PoC must zeroize or destroy the token promptly upon surrender and must protect the token from malicious use from the time of surrender. In all cases, regardless of certificate assurance level, the organization must promptly notify a WidePoint PIV SSP LRA to revoke the certificate, providing the WidePoint PIV SSP Subscriber's:

- Name
- Organization name
- Email address; and,
- Issuer Distinguished Name (i.e., the name of the WidePoint PIV SSP CA that issued the certificate).

The WidePoint PIV SSP LRA searches the WidePoint PIV SSP Repository for certificates issued to the WidePoint PIV SSP Subscriber and identifies certificates by verifying the submitted information. The WidePoint PIV SSP LRA then notes the serial number(s) and date of issuance of every current certificate issued to that WidePoint PIV SSP Subscriber and sends a request to the WidePoint PIV SSP RA for revocation of those certificates. The organization must also attest to the disposition of the credential (if applicable), via a digitally signed e-mail. Cryptographic hardware tokens can be identified by their unique 'serial number' (often a CUID number on the chip) and/or by the certificates on the cryptographic hardware token.

For all WidePoint PIV SSP Subscriber that express an organizational affiliation, the organization's WidePoint PKI Point of Contact must inform the WidePoint PIV SSP of any changes in a WidePoint PIV SSP Subscriber's affiliation through a digitally signed email or through a digitally signed transaction through the WidePoint PIV SSP CMS. If the Affiliated Organization no longer authorizes the affiliation of a WidePoint PIV SSP Subscriber, the WidePoint PIV SSP will revoke any certificates issued to that WidePoint PIV SSP Subscriber containing the organization affiliation. If an Affiliated Organization terminates its relationship with the WidePoint PIV SSP such that it no longer provides updates to organizational affiliation information, the WidePoint PIV SSP will revoke all certificates containing that Affiliated Organization's information.

4.9.2 WHO CAN REQUEST A REVOCATION

The following authorized parties may request a revocation of a WidePoint PIV SSP certificate:

- Any WidePoint PIV SSP Subscriber may request revocation of their own certificate(s).
- WidePoint PIV SSP PKI Points of Contact may submit requests for any WidePoint PIV SSP Subscriber that is affiliated with their organization or may notify a WidePoint PIV SSP LRA or WidePoint PIV SSP RA to request revocation of the WidePoint PIV SSP Subscriber affiliated with their organization.
- The WidePoint PIV SSP RA may revoke any WidePoint PIV SSP Subscriber certificate for reasons identified in this WidePoint PIV SSP CPS, and.
- Persons appointed by the FPKIPA to request revocation of any WidePoint PIV SSP Subscriber or WidePoint PIV SSP CA certificate.

Relying parties can find information on revocations at https://orc.widepoint.com/certificate-revocation/.

If any individual has reason to believe that a WidePoint PIV SSP issued certificate private key has been compromised, that individual is required to notify the WidePoint PIV SSP of the compromise suspicion. It is the responsibility of the WidePoint PIV SSP, in particular a WidePoint PIV SSP RA, to investigate the information and determine if certificate revocation is warranted, based on communications with either the WidePoint PIV SSP Subscriber that is identified by the suspected compromised certificate or an organization representative such as the WidePoint PIV SSP PKI Point of Contact for that organization or an employee of the organization who has been duly appointed as a WidePoint PIV SSP LRA for the WidePoint PIV SSP Subscriber's organization. The WidePoint PIV SSP RA will verify the WidePoint PIV SSP Subscriber Name, Organization and email address associated with the certificate to be revoked. If there is ambiguity, the WidePoint PIV SSP will investigate for additional information to ensure accuracy.

If the revocation request has been deemed as appropriate and warranted by the WidePoint PIV SSP, the WidePoint PIV SSP RA will document the reasons for the revocation and revoke the certificates identified in the revocation request. The WidePoint PIV SSP will send a written notice and brief explanation for the revocation to the WidePoint PIV SSP Subscriber unless directed otherwise by the FPKIPA or a court of competent jurisdiction.

The WidePoint PIV SSP reserves the right to revoke any WidePoint PIV SSP issued certificate at its discretion.

4.9.3 PROCEDURE FOR REVOCATION REQUEST

Revocation requests of human or device WidePoint PIV SSP Subscriber certificates can be made through the WidePoint PIV SSP Help Desk or directly to a WidePoint PIV SSP RA or LRA via any process that sufficiently ensures identity validation of the party making the request, a clear explanation of the reason for revocation and also the confirmation of the identity of the certificate to be revoked (e.g. certificate CN, certificate serial number, name, email address, organizational affiliation, issuer DN, date of issue). If a revocation request is made via a WidePoint PIV SSP Help Desk call, the revocation request will be forwarded to a WidePoint PIV SSP RA for verification and processing. WidePoint PIV SSP Help Desk personnel will send a digitally signed email with the information identified above to the WidePoint PIV SSP RA or LRA. A revocation request may also be submitted in letter form through a signed letter delivered to the WidePoint PIV SSP to the address identified in Section 1.5.2 of this WidePoint PIV SSP CPS. A WidePoint PIV SSP Form Letter Revocation Request is available at the WidePoint PIV SSP website or can be provided via a help desk request.

Upon receipt of a revocation request, a WidePoint PIV SSP RA or LRA will validate the credentials of the party making the request, either through digital signature verification or hard-copy written request. If the WidePoint PIV SSP Subscriber who is the subject of a revocation request is affiliated with an organization, a written revocation request will be submitted on the organization's letterhead from the organization's WidePoint PIV SSP PKI Point of Contact or an organization executive with approval authority if the WidePoint PIV SSP PKI Point of Contact is unavailable for any reason including a revocation request submitted against their own WidePoint PIV SSP Subscriber certificate. If the named WidePoint PIV SSP Subscriber is requesting revocation of their own certificate, the WidePoint PIV SSP, typically a WidePoint PIV SSP RA or LRA, will validate the revocation requestor using the procedures outlined for initial certificate request validation as specified in Section 3.2.3.1 or Section 3.2.3.2 of this WidePoint PIV SSP CPS. If a WidePoint PIV SSP RA chooses to revoke a certificate because of sufficient evidence of noncompliance with this WidePoint PIV SSP CPS, the WidePoint PIV SSP RA will document the reason for certificate revocation and will notify the WidePoint PIV SSP Subscriber unless directed otherwise by the FPKIPA or a court of competent jurisdiction.

If the WidePoint PIV SSP RA or WidePoint PIV SSP Issuer determines there is a need to revoke the certificate once an authorized request is received, the WidePoint PIV SSP RA or WidePoint PIV SSP Issuer will revoke the certificate by accessing the certificate management system and selecting the "revoke certificate" option, which then places the serial number and certificate revocation date on a CRL. The WidePoint PIV SSP RA or WidePoint PIV SSP Issuer will also remove the certificate from the primary directory and any replicated directories.

Whenever the reason for revocation is due to key compromise or suspected fraudulent use, both the WidePoint PIV SSP Subscriber and the WidePoint indicates that reason in their respective revocation request email.

WidePoint PIV SSP Subscribers, who have received cryptographic tokens such as needed for a WidePoint PIV SSP PIV or a WidePoint PIV SSP PIV-I credential and are leaving the organization that sponsored their participation in the WidePoint PIV SSP, must surrender to their organization's WidePoint PIV SSP PKI Point of Contact (through any accountable mechanism) all cryptographic hardware tokens that were issued, under the sponsoring organization, prior to leaving the organization. The WidePoint PIV SSP PKI Point of Contact will zeroize (only if token reuse is desired and allowed, and if token unlock code is known) or destroy the token promptly upon surrender and will protect the token from malicious use between surrender and zeroization or destruction. The WidePoint PIV SSP PKI Point of Contact will send a signed email to a WidePoint PIV SSP RA requesting revocation. Upon receipt of the Revocation request, the WidePoint PIV SSP RA will revoke the certificates assigned to that token. WidePoint PIV SSP Subscriber credentials (cryptographic tokens) are the responsibility of the sponsoring organization, including procurement and final disposition. If a WidePoint PIV SSP Subscriber leaves an affiliated organization and the

WidePoint PIV SSP Subscriber credentials (cryptographic tokens) cannot be obtained from the WidePoint PIV SSP Subscriber, then all WidePoint PIV SSP Subscriber certificates associated with the un-retrieved tokens will be revoked for the reason of key compromise.

4.9.4 REVOCATION REQUEST GRACE PERIOD

WidePoint PIV SSP Subscriber certificates will be revoked upon request as soon as the need can be verified. There is no grace period. A WidePoint PIV SSP Subscriber, or their sponsoring organization's WidePoint PIV SSP PKI Point of Contact or an organization executive with approval authority if the WidePoint PIV SSP PKI Point of Contact is unavailable for any reason, FPKIPA personnel, and WidePoint PIV SSP personnel must request revocation from the WidePoint PIV SSP as soon as the need for revocation has been determined.

4.9.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

All WidePoint PIV SSP CAs process revocation requests as quickly as practicable upon receipt of an authenticated revocation request as will be but as an operating practice within two hours of receipt. The WidePoint PIV SSP Subscriber, or their sponsoring organization, must request revocation from WidePoint PIV SSP as soon as the need for revocation has been determined. Revocation requests for WidePoint PIV SSP PIV or PIV-I credentials are processed immediately upon receipt by the WidePoint PIV SSP or approved agency Card Management System which then authenticates to the appropriate WidePoint PIV SSP Certificate Authority and revokes the certificates associated with the WidePoint PIV SSP PIV or PIV-I credential. All revocations requests received prior to two hours before the next CRL is published will be processed. The CRL issuance frequency for each WidePoint PIV SSP CA is addressed in Section 4.9.7 of this WidePoint PIV SSP CPS.

The WidePoint PIV SSP maintains a continuous 24x7 ability to respond internally to high-priority problem reports through the WidePoint First Responder teams which are comprised of at least one WidePoint Certificate Authority Administrator, a WidePoint System Administrator and a WidePoint Registration Authority who are trained in the policies and practices of this WidePoint PIV SSP CPS, the WidePoint System Security Plan and subordinate and related plans such as the WidePoint Incident Response Plan and the WidePoint Contingency Plan, and where appropriate, the WidePoint PIV SSP shall forward such a complaint to law enforcement authorities, and/or revoke a certificate that is the subject of such a complaint.

Routine WidePoint Certificate Authority or Subordinate Certificate Authority certificate revocation shall be completed within an agreed time following receipt of an authenticated revocation request. If the revocation is due to a compromise or emergency, the time to revoke shall adhere to the requirements of Section 4.9.12.

4.9.6 REVOCATION CHECKING REQUIREMENTS FOR RELYING PARTIES

It is the responsibility of the Relying Party to verify that WidePoint PIV SSP Subscriber certificates have not been revoked and are expected to verify the validity of these certificates in accordance with and as specified in [RFC 5280]. WidePoint PIV SSP Subscriber certificates may be stored locally by a Relying Party but should be validated at least daily before use. The Relying Party must always check a WidePoint PIV SSP Subscriber certificate against the Certificate Revocation List, hereafter referred to as CRL, of the WidePoint PIV SSP CA that issued the WidePoint PIV SSP Subscriber certificate and that the CRL is current, valid and has not expired. If the Relying Party is unable to or it is temporarily infeasible to obtain revocation information, the Relying Party must either reject use of the WidePoint PIV SSP Subscriber certificate or make an informed decision to accept the risk, responsibility, and consequences for using a WidePoint PIV SSP Subscriber certificate whose authenticity cannot be guaranteed to the standards of this WidePoint PIV SSP CPS and Common Policy.

The following text is included in the WidePoint PIV SSP Subscriber Agreement and posted on the WidePoint PIV SSP website:

Use of revoked certificates could have damaging or catastrophic consequences in certain applications. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party and the system accreditor. If it is temporarily infeasible to obtain revocation information, then the Relying Party must either reject use of the certificate, or make an informed decision to accept the risk, responsibility, and consequences for using a certificate whose authenticity cannot be guaranteed to the standards of this policy.

4.9.7 CRL Issuance Frequency

Each WidePoint PIV SSP CA is required to issue CRLs every 18 hours. As a general rule, WidePoint PIV SSP CAs issue a new CRL every 6 hours but in all cases WidePoint PIV SSP CAs will issue a new CRL prior to the expiration of its current CRL. WidePoint PIV SSP CA CRLs are issued with a maximum validity period of 48 hours. New CRLs for WidePoint PIV SSP Cas are issued even if there are no changes or updates to be made, i.e., no certificate has been revoked since the creation of the last CRL or no certificate that was revoked has since expired. The "nextUpdate" field in the CRL will be no more than 48 hours from "thisUpdate" field of the CRL. If a revocation request is granted for the reason of key compromise, a new CRL will be generated as quickly as is feasible and will be posted within 12 hours of receipt of the request. Each new CRL for each WidePoint PIV SSP CA is published to the pointer location designated in the CRL Distribution Point Field of each certificate issued by that WidePoint PIV SSP CA and as described in Section 2 of the WidePoint PIV SSP CPS. Each superseded CRL for each WidePoint PIV SSP CA is archived to a folder by year and month on the WidePoint PIV SSP Repository to ensure a complete CRL history for each WidePoint PIV SSP CA.

CRLs are posted to webservers that use the HTTP protocol. CRL locations for each WidePoint PIV SSP CA is embedded in each certificate issued by that WidePoint PIV SSP CA in the Certificate Revocation List Distribution Point (CRLDP) field.

CRL location information is provided to Subscribers during certificate request or issuance and is made readily available to any potential Relying Party via the WidePoint PIV SSP website.

The WidePoint PIV SSP will notify the FPKIPA and any externally certified Certificate Authorities immediately in the event of any WidePoint PIV SSP CA revocation for any reason.

4.9.8 Maximum Latency for CRLs

Each WidePoint PIV SSP Certificate Authority is configured to auto-issue a CRL every 6 hours. CRLs issued by each WidePoint PIV SSP Certificate Authority are posted to the location that corresponds to the value embedded in the Certificate Revocation List Distribution Point (CRLDP) extension for each certificate issued by that WidePoint PIV SSP Certificate Authority. Each CRL is posted upon generation, but within no more than four hours after generation. Each WidePoint PIV SSP CA is configured to publish to the CRLDP upon issuance of the CRL. In the event of publishing failure, automated monitoring scripts verify the current CRL on the WidePoint PIV SSP CA versus the publicly available CRL found at the CRLDP. If the CRL on the WidePoint PIV SSP CA is more recently published than the publicly available CRL, the scripts pull the newer CRL and replace the publicly available CRL with the more recent CRL.

4.9.9 Online Revocation/Status Checking Availability

The WidePoint PIV SSP Certificate Status Services (WidePoint PIV SSP CSSs), which are OCSP responders, ensure that:

- An accurate and up to date CRL, from each WidePoint PIV SSP CA, is used to provide the revocation status of the certificates issued by that WidePoint PIV SSP CA;
- Latency of certificate status information meets or exceeds the requirements for CRL issuance as stated in Section 4.9.7;
- WidePoint PIV SSP CSSs processes requests and provides responses compliant with x.509 Internet Public Key Infrastructure Online Certificate Protocol [RFC 6960]; and,
- Each WidePoint PIV SSP Certification Authority issues an OCSP Responder certificate according to the profile stipulated in Section 10.13.

All WidePoint PIV SSP CSS keys that sign OCSP responses are unique and issued by the WidePoint PIV SSP CA for which they will provide signed OCSP revocation responses. All WidePoint PIV SSP CSS keys are protected by a FIPS 140-3 level 2 hardware security module as specified in Section 6.1.1. WidePoint PIV SSP CSS certificates that sign OCSP responses for certificates issued by a WidePoint PIV SSP CA assert all certificate policies that the WidePoint PIV SSP CA asserts as identified in Section 1.2. The algorithm of each WidePoint PIV SSP CSS signing certificate is consistent with the algorithm of the WidePoint PIV SSP CA certificate for which it is signing an OCSP response.

WidePoint PIV SSP CSSs are configured to retrieve the CRL from each WidePoint PIV SSP CA every 15 minutes. WidePoint PIV SSP CSSs will only retrieve the CRL if the CRL is different from the CRL it currently has for that WidePoint PIV SSP CA.

WidePoint PIV SSP CSS is configured such that no scheduled downtime is required due to component redundancy.

WidePoint disclaims any liability for loss due to use of any validation information relied on by any party that does not comply with this stipulation.

4.9.10 Online Revocation Checking Requirements

Relying Parties may optionally use on-line status checking. Since some relying parties may not be able to accommodate on-line communications, the WidePoint PIV SSP supports CRLs. Client software using on-line revocation checking need not obtain CRLs.

Relying parties, including all components of the WidePoint PIV SSP CMA, will only rely upon OCSP Responders approved in accordance with the requirements of Common Policy and this WidePoint PIV SSP CPS.

WidePoint PIV SSP CSSs have been evaluated and found to be in compliance with and approved for use by relying parties for WidePoint PIV SSP certificate revocation status checking.

4.9.11 Other Forms of Revocation Advertisements Available

Each WidePoint PIV SSP CA generates, issues, and publishes CRLs. The WidePoint PIV SSP also provides OCSP responder service through the WidePoint PIV SSP CSSs. The WidePoint PIV SSP does not support any other forms of revocation advertisement.

4.9.12 Special Requirements Related to key Compromise

The WidePoint PIV SSP uses reason codes that specify the reason that a certificate has been revoked as part of the CRL created by each WidePoint PIV SSP CA and has the ability to transition any reason code to compromise. The process is a manual process that must be accomplished by a WidePoint Certificate Authority Administrator accompanied by a WidePoint System Administrator directly on the internal database managing the respective WidePoint PIV SSP CA.

4.9.13 Circumstances for Suspension and Restoration

The WidePoint PIV SSP does not support certificate suspension for Certificate Authorities covered by this WidePoint PIV SSP CPS. WidePoint PIV SSP Subscriber certificates may be suspended and restored from suspension for circumstances and reasons defined in Sections 4.9.14, 4.9.15, and 4.9.16. In addition, WidePoint PIV SSP CMSs are configured to require a reason code for the suspension of a certificate, as well as the reason code for revocation of a certificate for key compromise. Others reason codes relevant to end entity certificates may be populated but are not required.

Practice Note: Certificate suspension should only be used in circumstances where there is a reasonable possibility that the certificate will need to be restored (e.g., suspension while background investigation outcome is appealed). It is not recommended to use certificate suspension as a mechanism to enforce access controls on a temporary basis or to circumvent account deprovisioning. Additionally, a certificate must be permanently revoked if it meets the circumstances stated in Section 4.9.1.

4.9.14 WHO CAN REQUEST SUSPENSION AND RESTORATION

Only WidePoint Registration Authorities are permitted to request suspension and restoration of a WidePoint PIV SSP Subscriber certificate.

4.9.15 PROCEDURE FOR SUSPENSION REQUESTS

All requests for certificate suspension shall be directed to WidePoint Registration Authorities who will authorize the suspension through WidePoint PIV SSP Card Management Systems or authorized agency Card Management Systems for certificates that have been issued as part of the PIV/PIV-I credential issuance process and include the certificate policy of **id-fpki-common-authentication**, **id-fpki-common-cardAuth**, **id-fpki-common-hardware,** or **id-fpki-common-policy** in the case of a PIV credential or **id-fpki-common-pivi-authentication**, **id-fpki-common-pivi-cardAuth**, **id-fpki-common-hardware,** or **id-fpki-common-policy policy** in the case of a PIV-I credential or authorize the suspension directly through the WidePoint PIV SSP Certificate Authority that issued the certificate for WidePoint PIV SSP Subscriber certificates that were not issued through the WidePoint PIV SSP Card Management System or approved agency Card Management Systems and that assert a certificate policy of **id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-devices,** or **id-fpki-common-devicesHardware.** WidePoint PIV SSP issued certificates asserting a certificate policy of **id-fpki-common-piv-contentSigning** or **id-fpki-common-pivi-contentSigning** shall never be placed on suspension for any reason or any amount of time. All WidePoint PIV SSP Subscriber certificates that are suspended will have their serial numbers populated on a full CRL within a timeframe specified in Section 4.9.7. The reason code CRL entry extension will be populated with "certificateHold." WidePoint PIV SSP Subscriber certificate serial numbers that have been restored from suspension will not be present on the next full CRL published by the WidePoint PIV SSP Certificate Authority that issued the WidePoint PIV SSP Subscriber certificate.

Practice Note: A certificate is considered restored only if its status at the time of CRL generation is neither suspended nor revoked.

A request to suspend or restore a certificate will include:

- authentication of the requestor,
- identification of the certificate to be suspended or restored, and
- explanation of the reason for suspension or restoration.

In all cases, a signed email by the requestor that identifies the certificate to be suspended or restored and the explanation of the reason for suspension or restoration shall be sent to a WidePoint Registration Authority and shall be retained by the WidePoint PIV SSP as proof of request and retained in accordance with the archive requirements as identified in Section 5.5.2 of this WidePoint PIV SSP CPS. In the case of WidePoint PIV SSP Subscriber certificates that have been issued as part of the PIV/PIV-I credential issuance process and include the certificate policy of **id-fpki-common-authentication**, **id-fpki-common-cardAuth**, **id-fpki-common-hardware,** or **id-fpki-common-policy** in the case of a PIV credential or **id-fpki-common-pivi-authentication**, **id-fpki-common-pivi-cardAuth**, **id-fpki-common-hardware,** or **id-fpki-common-policy** in the case of a PIV-I credential documentation of request shall be recorded by the WidePoint Card Management System or approved agency Card Management System that is processing the request.

If a WidePoint PIV SSP Subscriber is requesting restoration of their suspended certificate, the identity of the WidePoint PIV SSP Subscriber shall be re-established before restoring the certificate. The WidePoint PIV SSP Subscriber's identity shall be re-established using processes defined in Section 3.2.3.1 of this WidePoint PIV SSP CPS, through the use of biometrics on file through the chain of trust defined in [FIPS 201], or by the use of another private signature key of equivalent or greater assurance level issued to the WidePoint PIV SSP Subscriber.

The private key associated with any suspended WidePoint PIV SSP Subscriber certificate will not be used to authenticate the identity of the certificate subject.

4.9.16 Limits on Suspension Period

A certificate may remain in a suspended state until the CMS either reinstates it, revokes it, or the certificate expires. Department of Transportation uses a PIV enabled website where an authorized user may suspend a card holder. A start, stop date, reason and alert message are required for this process. This process is logged and emails are generated to requestor and PIV Management when a card holder is suspended or reinstated. This website is monitored by PIV Management to see if a card holder should be unsuspended or stop date should be modified. In all cases, certificate suspension will not exceed one year. The WidePoint PIV SSP CA is configured to remove expired certificates from a CRL.

Practice Note: In order to mitigate the threat of unauthorized person removing the certificate from hold, the identity of the Registration Authority or authorized individual removing the suspension should be authenticated using a mechanism equivalent or higher than the assurance level of the certificate being unsuspended.

4.10 Certificate Status Services

The WidePoint PIV SSP operates Certificate Status Services (CSSs) using OCSP responders that provides revocation status (see section 4.9.9, Online Revocation/Status Checking Availability).WidePoint PIV SSP CSSs practices include:

- Conformance to the stipulations of Common Policy, applicable Internet Standards, and this WidePoint PIV SSP CPS.
- Ensuring that certificate and revocation information is accepted only from valid WidePoint PIV SSP Certificate Authorities.
- Only valid and appropriate responses.
- Maintaining evidence that due diligence is exercised in validating certificate status.
- WidePoint PIV SSP CSS certificates that conform to the OCSP Responder Certificate profile as specified in Section 10.13.
- WidePoint PIV SSP CSS certificates that are valid for a maximum of thirty (30) days and renewed every seven (7) days.
- Not issuing pre-signed OCSP responses; and,
- Not issuing nonce-based OCSP responses.

WidePoint PIV SSP does not currently support SCVP.

4.10.1 Operational Characteristics

WidePoint PIV SSP CSSs will comply with the requirements of this WidePoint PIV SSP CPS and Common Policy, as detailed in Section 4.10.

4.10.2 Service Availability

WidePoint PIV SSP CSSs maintain service availability through redundancy of equipment and redundancy of network services by striving to operate at 99% up-time annually. This redundancy precludes the need for scheduled downtime.

4.10.3 Optional Features

WidePoint PIV SSP CSSs do not currently operate any optional features beyond those specified by the OCSP protocol.

4.11 End of Subscription

Subscription to the WidePoint PIV SSP is synonymous with the validity period of the WidePoint PIV SSP Subscriber's certificate issued by a WidePoint PIV SSP CA. The subscription ends when the WidePoint PIV SSP Subscriber's certificate expires, i.e., the current date has passed the validity period end date or has been revoked.

4.12 KEY ESCROW AND RECOVERY

4.12.1 KEY ESCROW AND RECOVERY POLICY AND PROCEDURES

WidePoint PIV SSP Certificate Authority or Subordinate Certificate Authority private keys are never escrowed.

WidePoint PIV SSP Human Subscriber key management keys are escrowed to provide key recovery. Escrowed keys are maintained within a WidePoint PIV SSP Key Encryption Database for a minimum of one year after the expiration of the associated public key certificate.

WidePoint PIV SSP Subscriber signature keys are never escrowed.

4.12.1.1 Key Escrow Process and Responsibilities

<REDACTED>

Escrowed keys are maintained throughout the life of the WidePoint PIV SSP. If the WidePoint PIV SSP issued certificate associated with the key is renewed or modified without changing the key, the escrowed key shall be maintained within the WidePoint PIV SSP Key Encryption Database for a minimum of one year after the expiration date of the renewed or modified WidePoint PIV SSP issued certificate associated with the key. Escrowed keys shall be archived as described in Section 5.5 of this WidePoint PIV SSP CPS. Security audit requirements are specified in Section 5.4 of this WidePoint PIV SSP CPS.

As part of the key escrow process, all Applicants and WidePoint PIV SSP Subscribers for whom the WidePoint PIV SSP escrows keys are notified that the private keys associated with their encryption certificates are being escrowed as part of the request and issuance process.

4.12.1.2 Key Recovery Process and Responsibilities

WidePoint PIV SSP Subscribers must use electronic means to request their own escrowed keys from the WidePoint PIV SSP. The WidePoint PIV SSP Subscriber may submit the request to a designated WidePoint Key Recovery Agent or a WidePoint Key Recovery Official. The WidePoint PIV SSP Subscriber will digitally sign the request using a WidePoint PIV SSP issued signature certificate of assurance level equal to or greater than that of the escrowed key.

WidePoint PIV SSP Subscribers may submit a request signed by hand to a WidePoint PIV SSP Agency PKI Point of Contact. The WidePoint PIV SSP Agency PKI Point of Contact forwards the request via a digitally signed email to a WidePoint Key Recovery Agent. The WidePoint Key Recovery Agent confirms that the WidePoint PIV SSP Subscriber name and e-mail address in the request match a record for an escrowed key to be recovered prior to approving the request. Upon validation of the recovery request, the escrowed key will be recovered by two (2) WidePoint Key Recovery Agents.

One WidePoint Key Recovery Agent will authenticate to the WidePoint PIV SSP CA that holds the requested private key in escrow. The key recovery process requires the creation of a password to protect the key after recovery. A second WidePoint Key Recovery Agent generates this password and provides it at the CA but does not share it with the first WidePoint Key Recovery Agent. The first WidePoint Key Recovery Agent completes the portion of the key recovery process at the CA by recovering the key to a file encrypted in p12 format. This p12 file is protected by the aforementioned strong password provided by the second WidePoint Key Recovery Agent. The first WidePoint Registration Authority/Key Recovery Agent is responsible for securely providing that cryptographic token to the WidePoint PIV SSP Subscriber via hand delivery or through certified mail. The password, which is generated in accordance with Section 6.4.1 of this WidePoint PIV SSP CPS by the second WidePoint Registration Authority/Key Recovery Agent is securely delivered to the requestor via hand delivery or through certified mail. No WidePoint Registration Authority/Key Recovery Agent may have simultaneous possession or control of the cryptographic token that contains the recovered private key of the WidePoint PIV SSP Subscriber and the password that protects the recovered private key. A WidePoint Key Recovery Witness Statement is prepared that documents the date and time, WidePoint PIV SSP Subscriber that is subject to the request, the WidePoint Registration Authorities/Key Recovery Agents performing the recovery, their signatures, and the role they performed (i.e. recovery and protecting via password or protecting the chain of custody for the token and delivery to the requestor). The WidePoint Key Recovery Witness Statement is scanned in and digitally signed by both participating WidePoint

Registration Authority/Key Recovery Agent and securely stored in the archive as specified in Section 5.5 of this WidePoint PIV SSP CPS.

WidePoint PIV SSP Subscribers who have a WidePoint PIV SSP PIV or PIV-I credential and who have either lost or are renewing their credential after expiration will have their previously escrowed encryption keys of their past WidePoint PIV SSP PIV or PIV-I credential issuances recovered to their new WidePoint PIV SSP PIV or PIV-I credential (as described in section 4.12.1.5, "Key Recovery During Token Issuance").

Third party requestors must use electronic means to request the WidePoint PIV SSP Subscribers' escrowed keys. The requestor will submit the request to a designated WidePoint Registration Authority or a Trusted Agent, digitally signing the request using a Common Policy CA or a federal bridge cross certified authentication or signature certificate of an assurance level equal to or greater than that of the escrowed key. Written requests signed by hand and notarized may be accepted on a case-by-case basis. Upon validation of the recovery request by a WidePoint Key Recovery Agent, the escrowed key will be recovered by two WidePoint Key Recovery Agents as described above.

Third party requestors shall be bound, by legal means and the stipulations of this WidePoint PIV SSP CPS and Common Policy, to the key protection and other provisions described herein. The requestor shall sign a document prepared by the requestor, which includes the following statement: "I hereby state that I have legitimate and official need to recover this key in order to obtain (recover) the encrypted data that I have authorization to access. I acknowledge receipt of a recovered WidePoint PIV SSP encryption key associated with the WidePoint PIV SSP Subscriber identified here. I certify that I have accurately identified myself to the WidePoint Registration Authority and truthfully described all reasons that I require access to data protected by the recovered key. I acknowledge my responsibility to use this recovered key only for the stated purposes, to protect it from further exposure, and to destroy all key materials or return them to the WidePoint PIV SSP Registration Authority or WidePoint PIV SSP Key Recovery Official when no longer needed. I understand that I am bound by subscriber's organization policies, applicable laws and Federal regulations concerning the protection of the recovered key and any data recovered using the key."

4.12.1.3 Key Recovery Through WidePoint PIV SSP Key Recovery Agent

WidePoint PIV SSP Subscribers may submit a request signed by hand to a WidePoint Registration Authority or a WidePoint PIV SSP Key Recovery Official. The WidePoint Registration Authority or WidePoint PIV SSP Key Recovery Official must validate the identity of the requestor. WidePoint PIV SSP Key Recovery Official shall forward the request via a digitally signed email to a WidePoint Registration Authority. The WidePoint Registration Authority must authenticate the information in the request prior to approving the request. Upon validation of the recovery request by a WidePoint Registration Authority, the escrowed key will be recovered by two WidePoint Registration Authorities or WidePoint Key Recovery Agents who are WidePoint Registration Authorities but are only designated to perform key recovery. One WidePoint Registration Authority/Key Recovery Agent will authenticate using their WidePoint PIV SSP PIV-I credential to the WidePoint PIV SSP CA that holds the requested private key in escrow. The recovered keys are encrypted in p12 format and recovered to a cryptographic token. The p12 file is protected by a strong password provided by the second WidePoint Registration Authority/Key Recovery Agent who secures this password without the knowledge of the first WidePoint Registration Authority/Key Recovery Agent. The first WidePoint Registration Authority/Key Recovery Agent is responsible for protecting the cryptographic token that houses the recovered key in p12 format and is responsible for securely providing that cryptographic token to the WidePoint PIV SSP Subscriber via hand delivery or through certified mail. The password, which is generated in accordance with Section 6.4.1 of this WidePoint PIV SSP CPS by the second WidePoint Registration Authority/Key Recovery Agent is securely delivered to the requestor via hand delivery or through certified mail. No WidePoint Registration Authority/Key Recovery Agent may have simultaneous possession or control of the cryptographic token that contains the recovered private key of the WidePoint PIV SSP Subscriber and the password that protects the recovered private key. A WidePoint Key Recovery Witness Statement is prepared that documents the date and time, WidePoint PIV SSP Subscriber that is subject to the request, the WidePoint Registration Authorities/Key

Recovery Agents performing the recovery, their signatures, and the role they performed (i.e. recovery and protecting via password or protecting the chain of custody for the token and delivery to the requestor). The WidePoint Key Recovery Witness Statement is scanned in and digitally signed by both participating WidePoint Registration Authority/Key Recovery Agent and securely stored in the archive as specified in Section 5.5 of this WidePoint PIV SSP CPS.

Practice Note: Subscriber notification of key management key recovery is not necessary and may be prohibited in certain use cases (e.g., Counterintelligence or Law Enforcement investigations).

4.12.1.4 Automated Self-Recovery

This service is not implemented at this time.

4.12.1.5 Key Recovery During Token Issuance

When a WidePoint PIV SSP Subscriber is issued a new certificate on a hardware token, private key management keys for the WidePoint PIV SSP Subscriber can be recovered as part of the issuance process by authenticating to the appropriate WidePoint PIV SSP Key Encryption Database that holds the past encryption keys for the WidePoint PIV SSP Subscriber. This is done using the Global Platform Secure Channel Protocol as part of the WidePoint PIV SSP Subscriber PIV or PIV-I issuance process to inject the key history onto the hardware token directly. The previously escrowed encryption keys will be recovered and each placed into a separate container of the newly issued WidePoint PIV SSP PIV or PIV-I credential, namely the "Retired X.509 Certificate for Key Management 1" as specified in NIST SP 800-73-5 Interfaces for Personal Identity Verification – Part 1: PIV Card Application Namespace, Data Model and Representation and incremented per number of encryption keys that need to be recovered. Current WidePoint PIV SSP PIV or PIV-I credentials will hold up to five previously escrowed encryption keys from WidePoint PIV SSP PIV or PIV-I credentials. PIV or PIV-I Card stock may be acquired that could recover up to twenty (20) previously escrowed keys from WidePoint PIV SSP PIV or PIV-I credentials. Note: the issuance process for WidePoint PIV SSP PIV or PIV-I credentials is controlled and secured by a WidePoint PIV SSP CMS and only permits recovery of encryption keys issued through a WidePoint PIV SSP CMS issuance process.

4.12.1.6 Key Recovery by Data Decryption Server

Not Applicable.

4.12.1.7 Who can Submit a Key Recovery Application

WidePoint PIV SSP Subscribers may request recovery of their own escrowed keys by contacting a WidePoint KRA.

WidePoint KRAs may request recovery of escrowed keys on behalf of the WidePoint PIV SSP Subscriber as part of the re-key or re-issuance process.

Internal and external requestors may request recovery of escrowed keys via a WidePoint KRA.

An Internal requestor is the WidePoint PIV SSP PKI Point of Contact for the organization or a requestor who is in the supervisory chain of the organization to which the WidePoint PIV SSP Subscriber is or was affiliated. The intent of this WidePoint PIV SSP Certification Practice Statement is not to change the policy and procedures of the organization.

An External Requestor is an investigator or someone outside the WidePoint PIV SSP Subscribers' organization with authorized court order to obtain the decryption private key of the WidePoint PIV SSP Subscriber.

4.12.1.8 Requestor Authorization Validation

WidePoint PIV SSP Subscribers are authorized to request recovery of their escrowed keys.

WidePoint PIV SSP PKI Agency Points of Contact are authorized to request recovery of escrowed keys for WidePoint PIV SSP Subscribers in their organization.

Third-party requests from law enforcement are referred to WidePoint Corporate Legal Counsel for consideration.

Third-party requests from organizations other than the subscribing agency are referred to that agency's WidePoint PIV SSP PKI Agency Point of Contact.

Nothing in this document is intended to change the current procedures for obtaining information about individuals in connection with such requests

4.12.1.9 WidePoint PIV SSP Subscriber Authorization Validation

Current WidePoint PIV SSP Subscribers are authorized to recover their own escrowed key material through authentication with their WidePoint PIV SSP Subscriber authentication certificate.

Using the card management system, the key recovery agent reviews the list of certificates issued to the Subscriber and available for recovery for the Subscriber.

4.12.1.10 WidePoint PIV SSP Key Recovery Agent Authorization Validation

The WidePoint PIV SSP Key Encryption Database verifies that the individual WidePoint PIV SSP Key Recovery Agent PIV or PIV-I is still valid upon authenticating to the WidePoint PIV SSP Key Encryption Database and that the individual has the appropriate Key Recovery Agent group permissions within the WidePoint PIV SSP Key Encryption Database access control list.

4.12.1.11 WidePoint PIV SSP Key Recovery Official Authorization Validation

A WidePoint PIV SSP Key Recovery Agent shall verify that the WidePoint PIV SSP Key Recovery Official has been authorized to request keys for the identified WidePoint PIV SSP Subscriber. WidePoint PIV SSP Key Recovery Officials may only make requests on behalf of their organization. WidePoint PIV SSP Key Recovery Officials do not have access privileges on WidePoint PIV SSP Key Encryption Databases.

4.12.1.12 Data Decryption Server Authorization Validation

A WidePoint PIV SSP Key Encryption Database shall verify that a WidePoint PIV SSP or an agency Data Decryption Service recovery request is limited to the organization from which the WidePoint PIV SSP or an agency Data Decryption Service was established.

4.12.2 SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES

The WidePoint PIV SSP does not support session key encapsulation and recovery.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

The WidePoint PIV SSP consists of equipment dedicated to the operations of all WidePoint PIV SSP CAs, WidePoint PIV SSP CMSs, WidePoint PIV SSP RA workstations, WidePoint PIV SSP CSSs, WidePoint PIV SSP Hardware Security Modules, hereafter referred to as WidePoint PIV SSP HSMs, and WidePoint PIV SSP Firewall and Networking Equipment. WidePoint PIV SSP Equipment is dedicated for the sole purpose of performing functions in accordance with the issuance, revocation, life-cycle maintenance, protection, and operations of the WidePoint PIV SSP in accordance with this WidePoint PIV SSP CPS and Common Policy. Databases and directories located on WidePoint PIV SSP equipment will not be accessible to Applicants, WidePoint PIV SSP Subscribers or Relying Parties.

WidePoint PIV SSP CMS equipment is dedicated for the sole purpose of issuance of WidePoint PIV SSP PIV or PIV-I credentials.

<REDACTED>

5.1.1 SITE LOCATION AND CONSTRUCTION

<REDACTED>

5.1.2 PHYSICAL ACCESS

<REDACTED>

5.1.2.1 Physical Access for WidePoint PIV SSP Certificate Authority Equipment

<REDACTED>

5.1.2.2 Physical Access for WidePoint PIV SSP Registration Authority Equipment

<REDACTED>

5.1.2.3 Physical Access for WidePoint PIV SSP Certificate Status Services Equipment

<REDACTED>

5.1.2.4 Physical Access for WidePoint Key Encryption Database Equipment

<REDACTED>

5.1.2.5 Physical Access for WidePoint PIV SSP or agency Data Decryption Server Equipment

<REDACTED>

5.1.2.6 Physical Access for WidePoint PIV SSP Key Recovery Agent Equipment

<REDACTED>

5.1.3 POWER AND AIR CONDITIONING

<REDACTED>

5.1.4 WATER EXPOSURE

<REDACTED>

5.1.5 FIRE PREVENTION AND PROTECTION

<REDACTED>

5.1.6 MEDIA STORAGE

<REDACTED>

5.1.7 WASTE DISPOSAL

<REDACTED>

5.1.8 OFF-SITE BACKUP

<REDACTED>

5.2 PROCEDURAL CONTROLS

5.2.1 TRUSTED ROLES

WidePoint defines a trusted role as one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. As part of this determination of the impact of roles, WidePoint assigns each role a risk designation as described in the WidePoint System Security Plan Personnel Security Control Family Control PS-2 Position Risk Designation following the principles described in 5 Code of Federal Regulations 731-106. Each role is assigned a Risk Designation category of "High" for roles that can directly impact the system configuration of WidePoint PIV SSP systems, "Moderate" for roles that can act as gateways that enable "High" risk roles to interact with the WidePoint PIV SSP systems, or "Low" for roles that do not interact with any of the WidePoint PIV SSP systems.

<REDACTED>

5.2.1.1 WidePoint Certificate Authority Administrator

<REDACTED>

5.2.1.2 WidePoint Registration Authority

<REDACTED>

5.2.1.3 WidePoint System Administrator

<REDACTED>

5.2.1.4 WidePoint Corporate Security Auditor

<REDACTED>

5.2.1.5 Other Trusted Roles

5.2.1.5.1 WidePoint Local Registration Authorities

<REDACTED>

5.2.2 NUMBER OF PERSONS REQUIRED FOR TASK

<REDACTED>

5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

<REDACTED>

5.2.4 ROLES REQUIRING SEPARATION OF DUTIES

<REDACTED>

5.3 PERSONNEL CONTROLS

5.3.1 QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS

<REDACTED>

5.3.2 Background Check Procedures

WidePoint Certificate Authority Administrators, WidePoint System Administrators, WidePoint Registration Authorities, and WidePoint Corporate Security Auditors will either hold a United States Department of Defense security clearance at a level of Secret or higher or receive a thorough background check covering the past seven years performed by a qualified investigator, including, but not limited to:

- A criminal history check must show no misdemeanor or felony conviction.
- A credit history check must show that person has not committed any fraud or is otherwise financially trustworthy.
- Employment verification must demonstrate that the person is competent, reliable and trustworthy.
- Professional references must demonstrate that the person is competent, reliable, and trustworthy.
- Education verification of highest or most relevant degree.
- Place of residence.
- Social Security trace must show that the person has a valid social security number; and,
- Verification of authorization to work in the United States.

Adjudication of the background investigation is performed by the screening company whose agents/adjudicators are trained on State and Fair Credit Reporting Act rules and use of a client matrix to score a risk associated with a background investigation, has a process consistent with [Executive Order 12968], or equivalent. The results of these checks will not be released except as required by Section 9.4.4 of this WidePoint PIV SSP CPS and Common Policy.

For Federal employees and cleared contractors who fulfill trusted roles:

- a national security eligibility (i.e., Confidential, or above) is granted after positive adjudication of a Tier 3 or Tier 5 investigation,
- a suitability determination is granted after positive adjudication of a Tier 2 or Tier 4 investigation, and
- a PIV credential eligibility is granted after a positive adjudication of a Tier 1 investigation.

An active national security eligibility, suitability determination, or PIV credential eligibility fulfills the background check procedure requirements and continued maintenance of those determinations fulfills any reinvestigation requirements.

In all cases, the reinvestigation period for a Trusted Role background check must not exceed 10 years. If a Trusted Role's national security eligibility, suitability determination, or PIV eligibility is ever suspended or revoked during their appointment, all CA accesses must be revoked until the security eligibility, suitability determination, or PIV eligibility is reinstated or a separate investigation is completed and adjudicated. In the case of federal employees and cleared contractors, the requirements of this section are to be performed by the department or agency for whom the federal employee or cleared contractor is employed.

Practice Note: For Federal organizations, continuous evaluation (CE) processes, where utilized, replace the need for periodic reinvestigations. Currently, CE is in use for national security eligibility recipients and are planned for inclusion of the other determination types.

5.3.3 Training Requirements

<REDACTED>

5.3.4 Retraining Frequency and Requirements

<REDACTED>

5.3.5 Job Rotation Frequency and Sequence

<REDACTED>

5.3.6 Sanctions for Unauthorized Actions

<REDACTED>

5.3.7 Independent Contractor Requirements

<REDACTED>

5.3.8 Documentation Supplied to Personnel

<REDACTED>

5.4 Audit Logging Procedures

<REDACTED>

5.4.1 Types of Events Recorded

<REDACTED>

5.4.2 Frequency of Processing Log

<REDACTED>

5.4.3 Retention Period for Audit Log

<REDACTED>

5.4.4 Protection of Audit Log

<REDACTED>

5.4.5 Audit Log Backup Procedures

<REDACTED>

5.4.6 Audit Collection System (Internal vs. External)

<REDACTED>

5.4.7 Notification to Event-Causing Subject

<REDACTED>

5.4.8 Vulnerability Assessments

<REDACTED>

5.5 RECORDS ARCHIVAL

<REDACTED>

5.5.1 TYPES OF EVENTS ARCHIVED

<REDACTED>

5.5.2 RETENTION PERIOD FOR ARCHIVE

<REDACTED>

5.5.3 PROTECTION OF ARCHIVE

<REDACTED>

5.5.4 ARCHIVE BACKUP PROCEDURES

<REDACTED>

5.5.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS

<REDACTED>

5.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)

<REDACTED>

5.5.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION

<REDACTED>

5.6 KEY CHANGEOVER

<REDACTED>

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

<REDACTED>

5.7.2 COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED

<REDACTED>

5.7.3 ENTITY PRIVATE KEY COMPROMISE PROCEDURES

5.7.3.1 CA Private Key Compromise Procedures

<REDACTED>

5.7.3.2 KRS Private Key Compromise Procedures

<REDACTED>

5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

<REDACTED>

5.8 CA OR RA TERMINATION

<REDACTED>

5.8.1 WIDEPOINT PIV SSP CERTIFICATE AUTHORITY CESSATION OF OPERATION

<REDACTED>

5.8.2 WIDEPOINT PIV SSP TERMINATION

<REDACTED>

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

This WidePoint PIV SSP CPS does not preclude any source of key that has been generated in accordance with the stipulations of this WidePoint PIV SSP CPS, Common Policy, and local security requirements. Key generation shall be performed using a FIPS approved method or equivalent international standard. Key generation events shall use the configuration that was the basis of the FIPS or other approved standard (e.g., FIPS mode). If the required keys cannot be generated while in an approved configuration, the specific configuration and reason for use of a different method should be documented by the WidePoint PIV SSP. The WidePoint PIV SSP does not currently use any non-FIPS approved configurations.

6.1.1.1 WidePoint PIV SSP Certificate Authority Key Pair Generation

<REDACTED>

6.1.1.2 WidePoint PIV SSP Subscriber Key Pair Generation

<REDACTED>

6.1.1.3 WidePoint PIV SSP Certificate Status Services Key Pair Generation

<REDACTED>

6.1.1.4 WidePoint PIV Content Signing Key Pair Generation

<REDACTED>

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER

In accordance with this WidePoint PIV SSP CPS, in all cases except encryption, the key is generated directly on the WidePoint PIV SSP Subscriber's token. The WidePoint PIV SSP Subscriber is in possession and control of the private key from the time of generation or benign transfer.

In the case of encryption keys, the WidePoint PIV SSP generates the private key in the hardware security module of the WidePoint PIV SSP CA and stores and encrypts the key in a WidePoint PIV SSP Key Encryption Database.

The delivery of escrowed encryption keys retrieved from the WidePoint PIV SSP is described in Section 4.12.2.3 of this WidePoint PIV SSP CPS.

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

<REDACTED>

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

The WidePoint PIV SSP will deliver the Common Policy CA and WidePoint PIV SSP CA public keys via a web interface to a protected server using SSL. The WidePoint PIV SSP CA issues the web server its certificate. The public key will be stored such that it is unalterable and not subject to substitution. Protection of the Common Policy CA and WidePoint PIV SSP CA public keys is accomplished by:

- Blocking access to the machines hosting the web servers via SSH on the firewall.
- Disabling access to any webpage admin pages/ports
- Placing the Common Policy CA and WidePoint PIV SSP CA public certs in read-only directories
- Adherence to standard webserver lockdown procedures to prevent unauthorized access to the site with permissions other than read only

Relying Parties must contact the help desk to receive the official certificate hashes to compare them with the certificates downloaded from the site. In addition, during in-person authentication as described in Section 3.2.3.1

of this WidePoint PIV SSP CPS, the WidePoint PIV SSP will provide the Common Policy CA to WidePoint PIV SSP Subscribers.

6.1.5 KEY SIZES

WidePoint PIV SSP Subscriber certificates asserting certificate policy OIDs identified in Section 1.2 of this WidePoint PIV SSP CPS that have an expiration date after December 30, 2008, will use a 2048-bit modulus at a minimum and SHA-256 algorithm or stronger. WidePoint PIV SSP Subscriber certificates asserting certificate policy OIDs identified in Section 1.2 of this WidePoint PIV SSP CPS which expire after December 31, 2030, will contain either RSA public keys that are 3072 bits at a minimum or Elliptic Curve that are 256 at a minimum and SHA-256 hash algorithm or stronger. Trusted Certificates that expire on or after January 1, 2031, shall contain subject public keys of at least 3072 bits for RSA and 256 for Elliptic Curve and a hash algorithm of SHA-256 or greater and be signed with the corresponding private key.

All WidePoint PIV SSP CAs sign CRLs using the same key size and hash algorithms as are used to sign their signing certificates.

WidePoint PIV SSP CSSs sign OCSP responses using 2048-bit RSA and SHA-256 or stronger algorithms until 12/31/2030. After 12/31/2030, WidePoint PIV SSP CSSs will sign responses using 3072-bit RSA and SHA-384 or stronger algorithms.

WidePoint PIV SSP CMSs that sign content for WidePoint PIV SSP PIV or PIV-I credentials sign content using the SHA-256 algorithm.

WidePoint PIV SSP KED and WidePoint PIV SSP DDS keys shall be equal to or stronger than the keys being escrowed.

Use of Transport Layer Security (TLS) protocol or another protocol providing similar security to accomplish the requirements of this WidePoint PIV SSP CPS and Common Policy uses, at a minimum, AES (128 bits) or equivalent for the symmetric key, at least 2048 bit RSA or equivalent for the asymmetric keys, and SHA-256 for certificates expiring on or before December 31, 2030 and at least 3072 bit RSA and SHA-384 for after December 31, 2030. In addition, cryptographic protocols such as TLS, CMS, S/MIME use a cipher suite at least as strong as any keys transported using the protocol.

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

The requirements in this section apply to all entities generating WidePoint PIV SSP key pairs whose public components are to be certified by the WidePoint PIV SSP. All RSA key pairs, including the prime numbers, must be generated in accordance with the Digital Signature Standard [FIPS 186-3], including primality tests. RSA public exponent is in the range specified in [FIPS 186-4], (e.g., public exponent will be at least $2^{16} + 1$ (65537). Additionally, the WidePoint PIV SSP Certificate Authorities perform partial key validation as specified in NIST SP 800-89 (section 5.3.3).

For WidePoint PIV SSP Certificate Authorities that use ECC, public keys will fall within curves defined in Section 7.1.3 of this WidePoint PIV SSP CPS. Additionally, the WidePoint PIV SSP Certificate Authorities confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine as specified in NIST SP 800-56A (Sections 5.6.2.3.3, or 5.6.2.3.4).

6.1.7 KEY USAGE PURPOSES (AS PER X.509 V3 KEY USAGE FIELD)

The use of a specific key is constrained by the Key Usage extension in the X.509 certificate.

All WidePoint PIV SSP issued certificates will assert a critical Key Usage Extension. The dataEncipherment, encipherOnly, and decipherOnly bits of the Key Usage Extension will not be asserted in any certificates issued under this WidePoint PIV SSP CPS.

- WidePoint PIV SSP certificates to be used for authentication only set the digitalSignature bit of the Key Usage Extension.
- WidePoint PIV SSP certificates to be used by Human Subscribers only for digital signatures must set the digitalSignature and nonRepudiation bits of the Key Usage Extension.

- WidePoint PIV SSP certificates that have the nonRepudiation bit set, must not have keyEncipherment bit or keyAgreement bit set of the Key Usage Extension.
- WidePoint PIV SSP certificates to be used for encryption (RSA) must set the keyEncipherment bit of the Key Usage Extension.
- WidePoint PIV SSP certificates to be used for key agreement (ECC) must set the keyAgreement bit of the Key Usage Extension.

WidePoint PIV SSP CA certificates only set the cRLSign and keyCertSign bits of the Key Usage Extension.

Keys associated with WidePoint PIV SSP CA certificates are only used for signing certificates and CRLs.

Keys associated with Human Subscriber certificates must be used only for digital signature (including authentication) or encryption, but not both.

Certificates that assert **id-fpki-common-authentication, id-fpki-common-pivi-authentication, id-fpki-common-derived-pivAuth- hardware, id-fpki-common-derived-pivAuth, id-fpki-common-cardAuth**, or **id-fpki-common-pivi-cardAuth** are used solely for authentication.

Keys associated with WidePoint PIV SSP Subscriber device certificates may be used for digital signature (including authentication), encryption, or both. WidePoint PIV SSP device certificates must not assert the nonRepudiation bit of the Key Usage Extension.

For all WidePoint PIV SSP Subscriber certificates issued after June 30, 2019, the Extended Key Usage extension must always be present.

For all WidePoint PIV SSP Subscriber certificates, Extended Key Usage OIDs will be consistent with key usage bits asserted. The Extended Key Usage extension does not contain anyExtendedKeyUsage {2.5.29.37.0} or id-kpcodeSigning {1.3.6.1.5.5.7.3.3}.

WidePoint PIV SSP certificates that assert **id-fpki-common-piv-contentSigning** include the critical Extended Key Usage extension that asserts only id-PIV-content-signing {2.16.840.1.101.3.6.7} (see [CCP-PROF]).

WidePoint PIV SSP certificates that assert **id-fpki-common-pivi-contentSigning** must include a critical Extended Key Usage extension that asserts only **id-fpki-pivi-content-signing** {2.16.840.1.101.3.8.7} (see [CCP-PROF]).

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The relevant standard for all cryptographic modules for use with the WidePoint PIV SSP is FIPS140-3 Security Requirements for Cryptographic Modules. All WidePoint PIV SSP keys are generated using the associated FIPS 140-3 method inherent within the respective FIPS validated device (e.g., browser, HSM).

Applicants and WidePoint PIV SSP Subscribers must use cryptographic modules that have been validated to meet at least the criteria specified for FIPS 140-3 Level 1 for use with WidePoint PIV SSP issued certificates at the Medium Assurance level as defined in Section 1.4.1.4 and throughout this WidePoint PIV SSP CPS. The browser-based process for requesting Medium Assurance certificates from the WidePoint PIV SSP website performs a check of the Applicant or WidePoint PIV SSP Subscriber's browser to ensure a compliant browser is being used. If an Applicant or a WidePoint PIV SSP Subscriber is using a non-compliant browser, a message notifies the Applicant or WidePoint PIV SSP Subscriber that the browser they are using is not compliant with FIPS 140-3 Level 1 and suggests the current acceptable browsers that they may use. WidePoint PIV SSP certificates that are issued for this level may only assert a certificate policy object identifier of **id-fpki-common-policy** or **id-fpki-common-devices**.

Applicants and WidePoint PIV SSP Subscribers may procure from the WidePoint PIV SSP FIPS 140-3 Level 2 hardware cryptographic modules (or bring their own) for use with WidePoint PIV SSP issued certificates that assert a certificate policy OID value of **id-fpki-common-hardware**. The browser-based process for requesting certificates from the WidePoint PIV SSP website performs a check of the Applicant or WidePoint PIV SSP Subscriber's cryptographic certificate browser to ensure a compliant browser is being used that represent **id-fpki-common-hardware**. If an Applicant or WidePoint PIV SSP Subscriber possesses or procures their hardware cryptographic module from a source other than the WidePoint PIV SSP, WidePoint Local Registration Authorities must verify,

prior to processing the Applicant or WidePoint PIV SSP Subscriber's request, that the token use for key generation is a FIPS 140-3 Level 2 token by checking the FIPS-approved products website. WidePoint PIV SSP identity certificates that are issued for these levels may only assert a certificate policy object identifier commensurate with the assurance level of vetting that was completed and the key generation that was performed. WidePoint PIV SSP encryption certificates may only assert a certificate policy object identifier of **id-fpki-common-policy**.

WidePoint PIV SSP PIV and PIV-I Credentials are only issued using card stock that has been tested and approved by the Personal Identity Verification (PIV) of Federal Employees and Contractors, FIPS 201 Evaluation Program and listed on the GSA Approved Products List (APL). Any card stock that has been removed from the APL may only be used for issuance of new WidePoint PIV SSP PIV-I Credentials for up to one year after GSA approved replacement card stock is available. WidePoint PIV SSP PIV-I Credentials issued using a card stock that has been deprecated may continue to be used until the current WidePoint PIV SSP Subscriber certificates expire unless otherwise notified by the Federal PKI Policy Authority or the DoD FPKIPA. On an annual basis, each WidePoint PIV SSP CMS will one sample WidePoint PIV SSP PIV-I Credential that has been issued through its configuration and shall submit the sample WidePoint PIV SSP PIV-I Credential to the FIPS 201-3 Evaluation Program for testing. Findings of the testing will be distributed to all trusted roles of the WidePoint PIV SSP and incorporated into the necessary documentation.

WidePoint PIV SSP CMSs protects their individual content signing keys and master keys in hardware security modules validated to FIPS 140-3 Level (or higher). Protection of "card diversified keys" is accomplished through the combination of protections inherent in the hardware security module (HSM), hardware tokens, and each WidePoint PIV SSP CMS. The hardware security modules and hardware tokens used by WidePoint have attained FIPS 140-3 Level 2 validation.

All WidePoint PIV SSP issued certificates will be signed by a WidePoint PIV SSP CA whose signing key is protected by a hardware cryptographic module that has been validated to meet and operates FIPS 140-3 Level 3.

WidePoint PIV SSP CSS private keys are protected by a hardware security module validated at FIPS 140-3 Level 2, at a minimum.

WidePoint PIV SSP Certificate Authority Administrators, WidePoint Registration Authorities, and WidePoint PIV SSP Local Registration Authorities are issued WidePoint PIV SSP PIV-I Credentials whose private keys are protected by cryptographic hardware tokens validated at FIPS 140-3 Level 2. WidePoint Issuers and WidePoint Registrars are issued WidePoint PIV SSP PIV or PIV-I Credentials whose card stock that has been tested and approved by the Personal Identity Verification (PIV) of Federal Employees and Contractors, , FIPS 201 Evaluation Program and listed on the GSA Approved Products List (APL). WidePoint PIV SSP PIV or PIV-I credentials issued using deprecated card stock may continue to be used until the current WidePoint PIV SSP Subscriber certificates expire, unless otherwise notified by the FPKIPA/FPKIMA.

All cryptographic modules are operated such that the private asymmetric cryptographic keys are never being output in plaintext. No private key will appear unencrypted outside a WidePoint PIV SSP CA, WidePoint PIV SSP CMS or a WidePoint PIV SSP CSS equipment.

No one will have access to a private signing key but the WidePoint PIV SSP Subscriber. Private encryption keys will be held by the WidePoint PIV SSP Subscriber and by parties authorized to request recovery as specified in Section 4.12.2.2 of this WidePoint PIV SSP CPS. All key recovery requestors will protect recovered keys as described in Section 4.12.2.3 of this WidePoint PIV SSP CPS.

Note that Section 6.1.1 of this WidePoint PIV SSP CPS stipulates cryptographic module requirements for key generation.

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

Private Key	FIPS 140 Level

WidePoint PIV SSP Certificate Authorities WidePoint Key Encryption Database WidePoint Data Decryption Service	3
WidePoint Certificate Status Services	2
WidePoint PIV SSP PIV and PIV-I Content Signing ➢ id-fpki-common-piv-contentSigning ➢ id-fpki-common-pivi-contentSigning	2
WidePoint PIV SSP Subscriber Hardware Signature and Authentication ➢ id-fpki-common-authentication ➢ id-fpki-common-derived-pivAuth-hardware ➢ id-fpki-common-cardAuth ➢ id-fpki-common-hardware ➢ id-fpki-common-pivi-authentication ➢ id-fpki-common-pivi-cardAuth	2
WidePoint PIV SSP Subscriber Hardware Key Management ➢ id-fpki-common-hardware	2
WidePoint PIV SSP Subscriber Hardware Device ➢ id-fpki-common-devicesHardware	2
WidePoint PIV SSP Subscriber Software Signature and Authentication ➢ id-fpki-common-policy ➢ id-fpki-common-derived-pivAuth	1
WidePoint PIV SSP Subscriber Software Key Management ➢ id-fpki-common-policy	1
WidePoint PIV SSP Subscriber Software Key Management ➢ id-fpki-common-devices	1

6.2.2 PRIVATE KEY (N OUT OF M) MULTI-PERSON CONTROL

Activation of WidePoint PIV SSP CA signature keys, WidePoint PIV SSP CSS signature keys, the WidePoint CMS content signer key and the CMS Master keys or access to any cryptographic security module containing the complete WidePoint PIV SSP CA or WidePoint PIV SSP CSS private signing keys procedurally requires two-person control as described in the WidePoint System Security Plan Physical and Environmental Protection Control Family Control PE-3: Physical Access Control Part C for physical access to the WidePoint PIV SSP system Access Control Family Control AC-2 Account Management for logical access. Access to WidePoint PIV SSP Certification Authorities signature keys and the WidePoint PIV SSP CSS signature keys backed up for disaster recovery requires the same two-person control as the operational WidePoint PIV SSP CA signature keys and the WidePoint PIV SSP CSS signature keys.

WidePoint PIV SSP Subscriber private encryption keys requested by anyone other than the WidePoint PIV SSP Subscriber or the WidePoint PIV SSP PKI Point of Contact may only be extracted from the WidePoint PIV SSP CA key recovery databases under two-person control as specified in in Section 4.12.2.3 of this WidePoint PIV SSP CPS, namely one WidePoint Key Recovery Agent and one WidePoint Key Recovery Official. WidePoint PIV SSP Subscribers are permitted to back up their own encryption keys where possible but not their signature keys. The

names of personnel and their roles relating to the operations of the WidePoint PIV SSP, and this WidePoint PIV SSP CPS are maintained on the WidePoint First Responders document and will be made available for inspection during compliance audits.

Access to an escrowed private key as part of the key recovery and subsequent delivery to a third party requestor is under two-party control as described in Section 4.12.2.3 of this WidePoint PIV SSP CPS.

6.2.3 PRIVATE KEY ESCROW

WidePoint PIV SSP Certificate Authority private keys are never escrowed. Additionally, under no circumstances will a non-repudiation signature key be escrowed or held in trust by a third party other than the WidePoint PIV SSP Subscriber.

All WidePoint PIV SSP Human Subscriber key management keys are escrowed as described in Section 4.12 of this WidePoint PIV SSP CPS. Separately, WidePoint PIV SSP Device Subscriber key may be escrowed if the device has a separate key management key certificate

The method, procedures and controls which apply to the storage, request for, extraction and/or retrieval, delivery, protection, and destruction of the requested copy of an escrowed key are described in Section 4.12 of this WidePoint PIV SSP CPS.

6.2.4 PRIVATE KEY BACKUP

For WidePoint PIV SSP Subscriber certificates that assert a certificate policy OID of **id-fpki-common-authentication**, **id-fpki-common-derived-pivAuth-hardware**, **id-fpki-common-cardAuth**, **id-fpki-common-hardware**, **id-fpki-common-pivi-authentication**, or **id-fpki-common-pivi-cardAuth**, WidePoint PIV SSP Subscribers are notified that private signature keys may not be backed up or copied.

For WidePoint PIV SSP Subscriber certificates that assert a certificate policy OID of **id-fpki-common-policy** the WidePoint PIV SSP recommends to WidePoint PIV SSP Subscribers that they make an operational copy of their software-based encryption private keys (but not signature) and will provide recommended procedures. The backup private keys must be stored on a removable media and cannot be kept online.

WidePoint PIV SSP Subscribers are also advised that backup of private signature keys for the sole purpose of key recovery may not be made.

WidePoint PIV SSP Subscribers are permitted to make operational copies of private keys residing in software cryptographic modules for each of the WidePoint PIV SSP Subscriber's applications or locations that require the key in a different location or format. However, private keys stored in each of these applications or locations must be in cryptographic modules that have been validated at [FIPS140] Level 1 and must be held in the WidePoint PIV SSP Subscriber's control and protected from unauthorized access by a password whose strength is equal to or greater than the original password created during the request process.

All key transfers must be done from an approved cryptographic module, and the key must be encrypted during the transfer. The WidePoint PIV SSP Subscriber or WidePoint PIV SSP PKI Sponsor is responsible for ensuring that all copies of private keys, including those that might be embedded in component backups, are protected, including protecting any workstation on which any of its private keys reside.

WidePoint PIV SSP CA and WidePoint PIV SSP CSS private signature keys and WidePoint PIV SSP CMS Master Keys are backed up following the same multi-person control as the original signature key. When such a backup is made, only a single copy is kept at the primary location, and a second copy will be kept at the WidePoint PIV SSP Secondary (or Alternate) Site. No more than two backup copies will be made. The backup module must also meet the cryptographic module requirements for WidePoint PIV SSP CAs, WidePoint PIV SSP CSSs and WidePoint PIV SSP CMSs.

The previous text for this section is summarized in the following table:

Private Key	Backup

WidePoint PIV SSP Certificate Authorities WidePoint Key Encryption Database WidePoint Data Decryption Service	Required
WidePoint Certificate Status Authorities	Optional
WidePoint PIV SSP PIV and PIV-I Content Signing ➢ id-fpki-common-piv-contentSigning ➢ id-fpki-common-pivi-contentSigning	Optional
WidePoint PIV SSP Subscriber Hardware Signature and Authentication ➢ id-fpki-common-authentication ➢ id-fpki-common-derived-pivAuth-hardware ➢ id-fpki-common-cardAuth ➢ id-fpki-common-hardware ➢ id-fpki-common-pivi-authentication ➢ id-fpki-common-pivi-cardAuth	Not Permitted
WidePoint PIV SSP Subscriber Hardware Key Management ➢ id-fpki-common-hardware	Required
WidePoint PIV SSP Subscriber Hardware Device ➢ id-fpki-common-devicesHardware	Optional
WidePoint PIV SSP Subscriber Software Signature and Authentication ➢ id-fpki-common-policy ➢ id-fpki-common-derived-pivAuth	Optional *
WidePoint PIV SSP Subscriber Software Key Management ➢ id-fpki-common-policy	Required
WidePoint PIV SSP Subscriber Software Device ➢ id-fpki-common-devices	Optional

* WidePoint PIV SSP Subscriber Software Signature and Authentication private signature keys may be backed up or copied but must be held and maintained in the WidePoint PIV SSP Subscriber's control.

6.2.5 Private Key Archival

WidePoint PIV SSP Certificate Authority private signature keys and WidePoint PIV SSP Subscriber private signature keys are not to be archived.

WidePoint PIV SSP Certificate Authorities that retain WidePoint PIV SSP Subscriber private encryption keys for business continuity purposes archive the escrowed WidePoint PIV SSP Subscriber private keys, so that they can be recovered for as long as the business continuity purposes require. Archives of escrowed private keys are protected in accordance with Sections 4.12, 5.1, 5.2, and 6.2 of this WidePoint PIV SSP CPS.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

Private keys are generated by and in a cryptographic module using the FIPS 140-3 approved method inherent within the respective cryptographic module. For WidePoint PIV SSP CAs, the cryptographic module must be a FIPS 140-3 Level 3 module (or higher). For WidePoint PIV SSP CSSs and WidePoint PIV SSP CMSs, the cryptographic module must be a FIPS 140-3 Level 2 module (or higher). For WidePoint PIV SSP Subscriber certificates that assert a certificate policy OID of **id-fpki-common-authentication**, **id-fpki-common-derived-pivAuth-hardware**, **id-fpki-**

common-cardAuth, id-fpki-common-hardware, id-fpki-common-pivi-authentication, or **id-fpki-common-pivi-cardAuth**, the cryptographic module must be a FIPS 140-3 Level 2 module (or higher). For WidePoint PIV SSP Subscriber certificates that assert a certificate policy OID of **id-fpki-common-policy**, the cryptographic module must be a FIPS 140-3 Level 1 module (or higher).

At no time are WidePoint PIV SSP CMS Master Keys and Diversified Keys exposed in plaintext outside of the hardware security module or the WidePoint PIV SSP PIV-I Credential associated with the key. WidePoint PIV SSP hardware security modules is designed with security world technology to ensure that keys remain secure throughout their life cycle. Every key in the security world is always protected by another key, even during recovery and replacement operations. Because the security world is built around key-management modules, keys are never available in plain text on the hardware security module or in the operating system.

All hardware security module keys are copied using their approved FIPS 140-3 method, following the manufacturer documentation. Specifically, the WidePoint stores encrypted key material and related data in files within the remote file system on each WidePoint PIV SSP CA.

Backup of WidePoint PIV SSP hardware security modules is handled through the WidePoint PIV SSP monthly backup process. Backups are encrypted in accordance with the WidePoint System Security Plan System and Communications Protection Control Family Control SC-28(1) Protection of Information at Rest | Cryptographic Protection.

6.2.7 Private Key Storage on Cryptographic Module

WidePoint PIV SSP private keys stored in the cryptographic modules are protected from unauthorized access and use in accordance with the FIPS 140-3 requirements applicable for that module.

6.2.8 Method of Activating Private Key

<REDACTED>

Certificate Policy Asserted	Activation Requirements
➢ id-fpki-common-authentication ➢ id-fpki-common-derived-pivAuth-hardware ➢ id-fpki-common-derived-pivAuth ➢ id-fpki-common-policy ➢ id-fpki-common-hardware ➢ id-fpki-common-pivi-authentication	Passphrases, PINs, or biometrics. When passphrases or PINs are used, they must be a minimum of six (6) characters. Entry of activation data must be protected from disclosure (i.e., the data should not be displayed while it is entered).
➢ id-fpki-common-devices ➢ id-fpki-common-devicesHardware	May be configured to activate the private key without requiring a human sponsor or authorized administrator to authenticate to the cryptographic token. The appropriate physical and logical access controls must be implemented for the device and its cryptographic token.
➢ id-fpki-common-piv-contentSigning ➢ id-fpki-common-pivi-contentSigning	May be configured to activate the private key without requiring a human sponsor or authorized administrator to authenticate to the cryptographic token. The appropriate physical and logical access controls must be implemented for content signing operations conformant with PIV issuance requirements (see [FIPS 201]).

	The strength of the security controls must be commensurate with the level of threat in the PIV credential issuance system's environment, and must protect the hardware, software, and the cryptographic token and its activation data from compromise.
➢ id-fpki-common-cardAuth ➢ id-fpki-common-pivi-cardAuth	None

6.2.9 Method of Deactivating Private key

<REDACTED>

6.2.10 Method of Destroying Private Key

<REDACTED>

6.2.11 Cryptographic Module Rating

Requirements for cryptographic modules are as stated above in Section 6.2.1 of this WidePoint PIV SSP CPS.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The public key is archived as part of the certificate archival.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

All WidePoint PIV SSP Certificate Authorities that issue WidePoint PIV SSP Subscriber certificates have a maximum key usage period of 10 years. WidePoint PIV SSP Certificate Authority private keys are used to sign CRLs and OCSP Responder certificates for their entire usage period and are configured at the Certificate Authority to not allow a WidePoint PIV SSP Subscriber certificate's expiration date and time to exceed the maximum lifetime allow by that certificate profile or to exceed the expiration date of the WidePoint PIV SSP Certificate Authority that is signing that certificate.

Key	Private Key	Certificate
WidePoint PIV SSP Subscriber Authentication	3 years	3 years
WidePoint PIV SSP Subscriber Signature	3 years	3 years
WidePoint PIV SSP Subscriber Encryption	Unrestricted	3 years
WidePoint PIV SSP Subscriber Card Authentication	3 years	3 years
WidePoint PIV SSP Content Signing	3 years	9 years *
WidePoint PIV SSP OCSP Responder	3 years	120 Days
WidePoint PIV SSP Device	3 years	3 years

* Expiration of WidePoint PIV SSP Content Signing certificates shall be later than the expiration of the WidePoint PIV SSP Subscriber certificates on the same PIV credential.

WidePoint PIV SSP Registration Authorities, WidePoint PIV SSP or Customer Agency Data Decryption Servers, WidePoint PIV SSP Key Recovery Agents and WidePoint PIV SSP Key Recovery Officers are considered WidePoint PIV SSP Subscribers.

6.3.3 Subscriber Private Key Usage Environment

WidePoint PIV SSP Subscribers affirm in the Subscriber agreement to use their private keys only on the machines that are protected and managed using commercial best practices.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

WidePoint PIV SSP Certificate Authority activation data may be user-selected (by each of the multiple parties trusted roles holding that activation data). The strength of WidePoint PIV SSP Certificate Authority activation data meets or exceeds the requirements for authentication mechanisms stipulated by FIPS 140-3 Level 3, see Section 6.2.1.

WidePoint PIV SSP Registration Authority certificates or credentials are protected by either a password or a PIN that is in compliance with FIPS 140-3 Level 2.

All WidePoint PIV SSP Registration Subscriber certificates or credentials activation data strength meets or exceeds the requirements for authentication mechanisms stipulated in [FIPS 140] for the associated cryptographic module level listed in Section 6.2.1.

The password will be in compliance with Section 6.2.8 of this WidePoint PIV SSP CPS. In addition, WidePoint PIV SSP Subscribers sign and return a subscriber advisory statement to help understand responsibilities for the use and control of the cryptographic module. The activation data password is generated by the Applicant or WidePoint PIV SSP Subscriber, as stipulated in the subscriber's agreement.

WidePoint PIV SSP Subscribers who receive WidePoint PIV SSP PIV or PIV-I credentials are directed to protect their credential with a PIN that must be 6-8 digits at a minimum. WidePoint PIV SSP Subscribers who receive WidePoint PIV SSP PIV or PIV-I credentials are instructed to select PINs that are not related to their personal identity, history, or environment. Sequences, repeated numbers, social security numbers, and date formats, or other easily guessed numbers are not to be used. For all WidePoint PIV SSP PIV or PIV-I credentials, in the event activation data can be reset by a WidePoint PIV SSP Issuer after the card is locked, authentication of the WidePoint PIV SSP PIV or PIV-I Subscriber is required. This authentication is conducted in accordance with FIPS 201, Section 2.9.3.

WidePoint PIV SSP Subscribers who receive end entity certificates other than WidePoint PIV SSP PIV-I credentials use passwords to protect the private keys of the WidePoint PIV SSP certificate. Requirements for password strength include an interspersed mix of eight 8 characters, including at least two (2) interspersed digits, password may not resemble dictionary words; differ from words or names by at least two characters that are not simple number-for-letter substitutions and do not consist of words or names followed by 1-4 digits. Sequences, repeated characters, date formats, or license plate formats may not be used. To the extent practicable, technical means are used to verify that the activation data meets all of the requirements in this section.

The WidePoint PIV SSP does not permit password or PIN generation by anyone other than the WidePoint PIV SSP Subscriber for whom the certificate or credential is being issued. Password or PIN assignment for the protection of the private key is performed prior to private key generation by the WidePoint PIV SSP Subscriber. The password or PIN is known only to the WidePoint PIV SSP Subscriber.

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

6.4.2 Activation Data Protection

Only WidePoint Certificate Authority Administrators are authorized to know and employ the signing key password for WidePoint PIV SSP CAs and WidePoint PIV SSP CSSs that is used to unlock the hardware cryptographic modules

that protect the respective signing keys. The activation password is stored in the WidePoint Certificate Authority Administrator's drawer of the WidePoint Primary Site SNOC Cage Safe and the WidePoint Secondary (or Alternate) Site Cage Safe. Only WidePoint Certificate Authority Administrators have access to the WidePoint Certificate Authority Administrator's drawer at each site.

The activation data protection mechanism for WidePoint PIV SSP CAs, WidePoint PIV SSP CMSs, and WidePoint PIV SSP CSSs is accomplished by distributing the functions of operations among several role so that any malicious activity requires collusion between at least two people and one from each role. Activation requires one WidePoint System Administrator to provide the hardware token that is stored in the WidePoint System Administrator drawer of the WidePoint Primary Site SNOC Cage Safe or WidePoint Secondary (or Alternate) Site Cage Safe while one WidePoint Certificate Authority Administrator provides the token password to activate the hardware security module for the WidePoint PIV SSP system being activated.

Activation data protection for WidePoint PIV SSP CAs includes the capability to temporarily lock the account, or terminate the application, after a maximum number of failed logon attempts (5) is reached. WidePoint PIV SSP CA activation data is protected from eavesdropping and replay by means of masking or completely hiding (nothing appears in window for keystrokes) activation data during input.

Activation data protection for WidePoint PIV SSP PIV or PIV-I includes the capability to temporarily lock the account, or terminate the application, after a maximum number of failed logon attempts (15) is reached. WidePoint PIV SSP Subscribers who have a PIV or PIV-I credential that is locked due to failed login attempts must appear before WidePoint Registration Authorities to perform a PIN reset.

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

6.4.3 Other Aspects of Activation Data

The activation data for WidePoint PIV SSP CAs, WidePoint PIV SSP CMSs, and WidePoint PIV SSP CSSs is changed no less than once every 84 days in accordance with the WidePoint System Security Plan Identification and Authentication Control Family Control IA-5(1) Authenticator Management | Password-Based Authentication. All WidePoint PIV SSP Certificate Authority Administrators, WidePoint System Administrators, and WidePoint Registration Authority personnel are required to change the login passwords no less than once every 84 days in accordance with the WidePoint System Security Plan Identification and Authentication Control Family Control IA-5(1) Authenticator Management | Password-Based Authentication.

For Medium Hardware PIV-I certificates, in the event activation data must be reset, a successful biometric 1:1 match of the WidePoint PIV SSP Subscriber against the biometrics collected in Section 3.2.3.1 of this WidePoint PIV SSP CPS is required. This biometric 1:1 match is conducted by a WidePoint Issuer or WidePoint Registrar.

Where a single cryptographic module has the private keys of more than one entity, remote activation requires authentication commensurate with the assurance of the certificate of the key being activated.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

<REDACTED>

6.5.2 Computer Security Rating

<REDACTED>

6.6 Life-Cycle Technical Controls

6.6.1 System Development Controls

<REDACTED>

6.6.2 Security Management Controls

<REDACTED>

6.6.3 Life-Cycle Security Controls

<REDACTED>

6.7 Network Security Controls

<REDACTED>

6.8 Time-Stamping

<REDACTED>

7 CERTIFICATE, CRL, AND OCSP PROFILES

Section 10 contains the formats for the various certificates and CRLs.

7.1 CERTIFICATE PROFILE

7.1.1 VERSION NUMBERS(S)

The WidePoint PIV SSP will issue X.509 Version 3 certificates.

7.1.2 CERTIFICATE EXTENSIONS

WidePoint PIV SSP certificate profiles are in accordance with the requirements of the certificate profiles described in Common Policy.

WidePoint PIV SSP Subscriber certificates always contain the Extended Key Usage extension, and that extension does not contain the anyExtendedKeyUsage {2.5.29.37.0} object identifier. Extended Key Usage object identifiers are consistent with key usage bits asserted.

Access control information may be carried in the subjectDirectoryAttributes non-critical extension.

7.1.3 ALGORITHM OBJECT IDENTIFIERS

Certificates issued by the WidePoint PIV SSP will use the following object identifiers for signatures.

sha-256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11} (1.2.840.113549.1.1.11)
sha-384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12} (1.2.840.113549.1.1.12)
sha-512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13} (1.2.840.113549.1.1.13)
Id-RSASSA-PSS	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10} (1.2.840.113549.1.1.10)
ecdsa-with-SHA384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3}
ecdsa-with-SHA256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2} (1.2.840.10045.4.3.4)
ecdsa-with-SHA384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3} (1.2.840.10045.4.3.3)
ecdsa-with-SHA512	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4} (1.2.840.10045.4.3.4)

The PSS padding scheme OID is independent of the hash algorithm. The hash algorithm is specified as a parameter (for details, see [PKCS#1]). Certificates issued under this CP must use the SHA-256 hash algorithm when generating RSASSA-PSS signatures. The following OID must be used to specify the hash in an RSASSA-PSS digital signature:

SHA-256	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1} (2.16.840.1.101.3.4.2.1)

Certificates under this Policy will use the following OIDs for identifying the algorithm for which the subject key was generated.

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-x9-62(10045) public key-type (2) 1}

For certificates that contain an elliptic curve public key, the parameters will be specified as one of the following named curves. In order to provide cryptographic separation for a closed community, when the subject public key is of the form id-ecDH, a private OID may be asserted to indicate a different base point on one of these curves.

ansip256r1	{iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7} (1.2.840.10045.3.1.7)
ansip384r1	{iso(1) identified-organization(3) certicom(132) curve(0) 34 } (1.3.132.0.34)

The WidePoint PIV SSP will certify only public keys associated with the crypto-algorithms identified above and will only use the signature crypto-algorithms described above to sign certificates, certificate revocation lists, and WidePoint PIV SSP CSS OCSP responses.

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

7.1.4 NAME FORMS

DNs will be used by the WidePoint PIV SSP in the issuer and in subject fields of the certificates. X.500 Directories use the DN for lookups. All Relying Parties will have the ability to process DNs. If communities request to use other names (e.g., certificates used to implement a hardware protocol, where device addresses are most useful and certificate lookup is not performed), then the WidePoint PIV SSP will define alternate name forms to be included in the subjectAltName extension and provide the alternative name form to the FPKIPA. Any name form defining GeneralName in [ISO9594-8] will be used, in accordance with the required profile (Section 7.1.2).

For attribute values other than domain component: The WidePoint PIV SSP encodes all WidePoint PIV SSP CA Distinguished Names (in various fields, e.g., Issuer, Subject, Subject Alternative Name, Name constraints) as printable strings. The WidePoint PIV SSP encodes all subscriber DN portions that name constraints apply to as printable strings. For other portions of the subscriber DN, the WidePoint PIV SSP encodes these values as printable strings, if possible. If a portion cannot be encoded as a printable string, then and only then will it be encoded using a different format and that format will be UTF8.

For domain component attribute values, the WidePoint PIV SSP encodes all domain component attribute values as an IA5 string.

7.1.5 NAME CONSTRAINTS

Name constraints may be asserted in WidePoint PIV SSP Certificate Authority and Subordinate Certificate Authority certificates.

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER

Certificates issued by the WidePoint PIV SSP will assert the certificate policy object identifier appropriate to the level of assurance with which it was issued.

Certificates that express the **id-fpki-common-cardAuth, id-fpki-common-pivi-cardAuth, id-fpki-common-piv-contentSigning,** or **id-fpki-common-pivi-contentSigning** certificate policy OID must not express any other certificate policy OIDs.

Delegated OCSP Responder certificates shall assert all certificate policy OIDs for which they are authoritative.

7.1.7 USAGE OF POLICY CONSTRAINTS EXTENSION

The WidePoint PIV SSP Certificate Authorities and Subordinate Certificate Authorities may assert policy constraints in their certificates. When this extension appears, at least one of requireExplicitPolicy or inhibitPolicyMapping must be present. When present, this extension may be marked critical.

7.1.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS

Certificates issued by the WidePoint PIV SSP may contain the following policy qualifiers: WidePoint PIV SSP CPS pointer.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

The WidePoint PIV SSP will not set the certificate policies extension to be critical. Relying Parties whose client software does not process this extension do so at their own risk.

7.1.10 Inhibit Any Policy Extension

The WidePoint PIV SSP Certificate Authorities and Subordinate Certificate Authorities may assert InhibitAnyPolicy in CA certificates. When present, this extension may be marked critical. Skip certs must be set to 0 since certificate policies are required in the Federal PKI.

7.2 CRL Profile

7.2.1 Version Number(s)

CRLs issued under this WidePoint PIV SSP CPS assert a version number as described in the X.509 standard [ISO9594-8]. CRLs will assert Version 2.

7.2.2 CRL and CRL Entry Extensions

Detailed CRL profiles covering the use of each extension are described in Section 10 and are in accordance with [CCP-PROF]. The WidePoint PIV SSP supports CRL Distribution Points (CRL DP) in all End Entity certificates.

7.3 OCSP Profile

Section 10 contains the format (profile) for OCSP requests and responses.

7.3.1 Version Number(s)

See OCSP request and response profiles in Section 10.

7.3.2 OCSP Extensions

See OCSP request and response profiles in Section 10.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The WidePoint PIV SSP operating under this WidePoint PIV SSP CPS and the Common Policy CP are subject to an annual review by the FPKIPA to ensure their policies and operations remain compliant with the Common Policy CP.

WidePoint PIV SSP Certificate Authorities operating under this WidePoint PIV SSP CPS and the Common Policy CP must have a compliance audit mechanism in place to ensure that the requirements of this WidePoint PIV SSP CPS are being implemented and enforced. The WidePoint PIV SSP Program Manager, as defined in Section 1.5.2, is responsible for ensuring annual audits are conducted for all PKI functions regardless of how or by whom the PKI components are managed and operated.

Customer Agencies must ensure they have appropriate authority to operate, in accordance with [FIPS 201] and [NIST SP 800-79] Guidelines for the Accreditation of PIV Card Issuers and Derived PIV Credential Issuers (DPCI). Customer Agencies must also ensure annual PKI compliance audits are conducted for all PKI operations for which they are responsible.

8.1 FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT

The WidePoint PIV SSP has compliance audits performed annually of all CMA operations to validate that CMAs are operating in accordance with the security practices and procedures described in this WidePoint PIV SSP CPS. The WidePoint PIV SSP acknowledges the requirement for subsequent periodic or aperiodic inspection or compliance audit of its support facilities as determined necessary by the FPKIPA.

The WidePoint PIV SSP acknowledges the FPKIPA's right to require periodic and aperiodic inspections and compliance audits of the WidePoint PIV SSP CMA facility to validate that the WidePoint PIV SSP CMAs are operating in accordance with the security practices and procedures set forth in this WidePoint PIV SSP CPS.

The WidePoint PIV SSP and FPKIPA will state the reason(s) for any aperiodic compliance audit.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The WidePoint PIV SSP engages the services of an external independent auditor that is competent in the field of security compliance audits of Information Technology systems and is thoroughly familiar with the WidePoint PIV SSP CPS and performs CA or IT system compliance audits as a primary responsibility. In all cases, the selected external independent auditor will have experience in information security, cryptography, and PKI.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The external independent auditor is an independent entity who has a contractual relationship with WidePoint PIV SSP to perform the compliance audit. The WidePoint PIV SSP also performs internal audits of all WidePoint PIV SSP systems to verify compliance with this WidePoint PIV SSP CPS and the WidePoint System Security Plan. The internal audits are conducted by a WidePoint Corporate Security Auditor.

8.4 TOPICS COVERED BY ASSESSMENT

The purpose of a compliance audit is to verify that the WidePoint PIV SSP has in place a system to assure the quality of the WidePoint PIV SSP services that it provides, and that it complies with all of the requirements of Comon Policy CP and this WidePoint PIV SSP CPS. All aspects of the WidePoint PIV SSP operation as specified in this WidePoint PIV SSP CPS are subject to compliance inspections.

Any discrepancies between a WidePoint PIV SSP operation and the stipulations of this CPS and the relevant policy will be noted. The FPKIPA will be immediately notified of all discrepancies. The FPKIPA will determine the appropriate remedy, and the FPKIPA and the WidePoint PIV SSP will determine the time for completion.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

When the external independent auditor or FIPS 201 Evaluation Program testing finds a discrepancy between the design, operation, or maintenance of the WidePoint PIV SSP and the stipulations of this WidePoint PIV SPP CPS or the Common Policy CP, the following actions will occur:

- The compliance auditor will note the discrepancy.
- The compliance auditor will notify the parties identified in Section 8.6 of the discrepancy.
- The WidePoint PIV SSP will propose a remedy, including expected time for completion, to the FPKIPA.

Any remedy may include permanent or temporary WidePoint PIV SSP cessation or termination of the WidePoint PIV SSP through revocation. However, several factors must be considered in this decision, including the severity of the discrepancy and the risks it imposes, and the disruption to the certificate using community.

Remedies will be defined by the FPKIPA and communicated to the WidePoint PIV SSP as soon as possible to limit the risks created. The FPKIPA and the WidePoint PIV SSP will determine a time for completion. The implementation of remedies will be coordinated between the FPKIPA and the WidePoint PIV SSP and subsequently communicated to the appropriate authority. A compliance audit, or FIPS 201 Evaluation Program testing, may be required to confirm the implementation and effectiveness of the remedy.

8.6 COMMUNICATIONS OF RESULTS

The results of any inspection or audit will be communicated, in whole, to the WidePoint PIV SSP and to the FPKIPA by the WidePoint PIV SSP. The WidePoint PIV SSP will determine appropriate remedies and will communicate the remedies to the FPKIPA as soon as possible to limit the risks created. The implementation of remedies will be communicated to the FPKIPA. A special audit may be required to confirm the implementation and effectiveness of the remedy.

If a WidePoint PIV SSP entity is found not to be in compliance with this WidePoint CPS, or the policy identified in Common Policy, the WidePoint PIV SSP will notify the FPKIPA immediately upon completion of the audit.

Each department or agency that participates in the WidePoint PIV SSP shall provide a Letter of Compliance signed by the external independent auditor to the WidePoint PIV SSP or directly to the FPKIPA.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 CERTIFICATE ISSUANCE OR RENEWAL FEES

A fee per validity year, unless otherwise negotiated, will be levied by the WidePoint PIV SSP to issue WidePoint PIV SSP certificates to WidePoint PIV SSP Subscribers for all credential and certificate types and profiles as described throughout this WidePoint PIV SSP CPS. Fees are published in WidePoint's GSA Schedule #47QTCA19D009F.

9.1.2 CERTIFICATE ACCESS FEES

All current WidePoint PIV SSP certificate information is available to all Relying Parties free of charge.

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEES

WidePoint PIV SSP CRL and OCSP Responses are provided free of charge to all Relying Parties.

9.1.4 FEES FOR OTHER SERVICES

No fee will be levied for on-line access to policy information about WidePoint PIV SSP. WidePoint will assess a fee from Relying Parties for providing archived revocation information. A reasonable fee to cover media reproduction and distribution costs may be levied for a physical media copy of this policy information. A fee per encryption certificate will be levied for the recovering of encryption keys. A consulting fee per hour will be levied for certificate support required in addition to the detailed instructions delivered with the notification of subscriber certificate issuance. This additional support includes documentation, telephone, and on-site support.

9.1.5 REFUND POLICY

No stipulation.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 INSURANCE COVERAGE

No stipulation.

9.2.2 OTHER ASSETS

No stipulation.

9.2.3 INSURANCE OR WARRANTY COVERAGE FOR END-ENTITIES

No stipulation.

9.2.4 FIDUCIARY RELATIONSHIPS

Issuance of certificates in accordance with this WidePoint PIV SSP CPS does not make any role associated with the WidePoint PIV SSP, an agent, fiduciary, trustee, or other representative of WidePoint PIV SSP Subscribers or relying parties. The relationship between the WidePoint PIV SSP or its designated authorities and WidePoint PIV SSP Subscribers and that between the WidePoint PIV SSP or its designated authorities and relying parties is not that of agent and principal. Neither WidePoint PIV SSP Subscribers nor relying parties have any authority to bind the WidePoint PIV SSP or its designated authorities, by contract or otherwise, to any obligation. The WidePoint PIV SSP and its designated authorities will make no representations to the contrary, either expressly, implicitly, by appearance, or otherwise.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 SCOPE OF BUSINESS CONFIDENTIAL INFORMATION

Not applicable. The WidePoint PIV SSP does not collect business confidential information.

9.3.2 Information Not Within the Scope of Business Confidential Information

Not applicable. The WidePoint PIV SSP does not collect business confidential information.

9.3.3 Responsibility to Protect Confidential Information

The WidePoint PIV SSP does not disclose non-certificate information to any third party unless authorized by this WidePoint PIV SSP Certification Practice Statement, the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, required by U.S. law, U.S. government rule or regulation, or order of a U.S. court of competent jurisdiction. The contents of the archives maintained by the WidePoint PIV SSP shall not be released except as required by this policy, required by U.S. law, U.S. government rule or regulation, or order of a U.S. court of competent jurisdiction.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The WidePoint PIV SSP protects all subscribers identifying information in accordance with the WidePoint System Security Plan Risk Assessment Control Family Control RA-8 Privacy Impact Assessments by conducting those assessments on an annual basis and by implementing the controls of the WidePoint System Security Plan Personally Identifiable Information Processing and Transparency Control Family All Controls. All Applicants and WidePoint EC Subscriber's identifying information will be maintained in accordance with the reference controls and applicable laws. Electronic Applicant and WidePoint PIV SSP Subscriber information is collected and maintained within the secure WidePoint PIV SSP environment as described in this WidePoint PIV SSP CPS and the WidePoint System Security Plan. Hard-copy Applicant and WidePoint PIV SSP Subscriber information is collected and maintained at the WidePoint PIV SSP facility in Fairfax, VA in secure containers. Archived hard-copy subscriber information is either maintained within the WidePoint PIV SSP facility Fairfax, VA facility or in an off-site storage facility as described in Section 5.5.2 of this WidePoint PIV SSP CPS.

9.4.2 Information Treated as Private

Information requested from Applicants or WidePoint PIV SSP Subscribers during the certificate issuance process other than that information, which is specifically included in the certificate, is withheld from release. This information may include personal information as described in Section 3.1 of this WidePoint PIV SSP CPS and is subject to the Privacy Act of 1974 {P.L. 093-579}. All information in the WidePoint PIV SSP record (not repository) is handled as Sensitive But Unclassified (SBU), and access will be restricted to those with official needs. Only WidePoint employees with assigned roles within the WidePoint PIV SSP have access to the information, which when not being reviewed or processed is maintained in locking file cabinets within WidePoint's secure suite.

Certificate private keys are considered sensitive, and access will be restricted to the certificate owner, except as stipulated in Section 4.12.2.2 of this WidePoint PIV SSP CPS . Private keys held by the WidePoint PIV SSP will be held in strictest confidence. Under no circumstances will any private key appear unencrypted outside the WidePoint PIV SSP hardware. Private keys held by the WidePoint PIV SSP will be released only to a trusted authority defined in Section 4.12.2.2 of this WidePoint PIV SSP CPS .

Audit logs and transaction records as a whole are considered sensitive and will not be made available publicly.

9.4.3 Information Not Deemed Private

No sensitive information will be held in certificates, as certificate information is publicly available in repositories. Information not considered sensitive includes the WidePoint PIV SSP Subscriber's name, electronic mail address, certificate public key, and certificate validity period. Information collected during the registration, issuance, or revocation process as described in this WidePoint PIV SSP CPS shall not be sold, exchanged in-kind, or given to any third party except as required by Section 9.4.6 Disclosure Pursuant to Judicial or Administrative Process of this WidePoint PIV SSP CPS.

9.4.4 Responsibility to Protect Private Information

The WidePoint PIV SSP will not disclose certificate-related information to any third party unless authorized by Common Policy, required by law, government rule or regulation, or order of a court of competent jurisdiction. The

WidePoint PIV SSP will authenticate any request for release of information. This does not prevent the WidePoint PIV SSP from disclosing the publicly available certificate and certificate status information (e.g., CRL, OCSP Requests and Responses, etc.).

9.4.5 Notice and Consent to Use Private Information

All notices will be in accordance with the applicable laws.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Sensitive data will be released to law enforcement officials only under a proper court order. The WidePoint PIV SSP will not disclose certificate or certificate-related information to any third party unless expressly authorized by Common Policy, required by criminal law, government rule or regulation, or order of a criminal court with jurisdiction. The WidePoint PIV SSP will authenticate such requests prior to disclosure. External requests must be made via the subscriber's organization, unless under court order.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

Unless otherwise agreed, property interests in the following security-related information materials and data are regarded as the property of the parties indicated below:

- Certificates and CRLs are the personal property of the WidePoint PIV SSP. Permission is granted to reproduce and distribute certificates issued by the WidePoint PIV SSP on a nonexclusive, royalty-free basis, provided that they are reproduced and distributed in full. Certificates and CRLs will not be published in any publicly accessible repository or directory without the express written permission of WidePoint.
- This WidePoint PIV SSP CPS is the sole property of WidePoint.
- Private keys are the personal property of the subscribers who rightfully use or are capable of using them (or their employer or principal), regardless of the physical medium within which they are stored and protected.
- Public keys are the personal property of subscribers (or their employer or principal), regardless of the physical medium within which they are stored and protected.
- WidePoint PIV SSP certificates issued to WidePoint personnel or WidePoint components/devices, including WidePoint PIV SSP public keys, are the property of WidePoint. WidePoint licenses relying parties to use such keys only in conjunction with FIPS 140-3 validated encryption modules.
- Distinguished names are the property of the individuals named or their employer.

9.6 Representations and Warranties

9.6.1 WidePoint PIV SSP CA Representations and Warranties

The WidePoint PIV SSP warrants that its procedures are implemented in accordance with this WidePoint PIV SSP CPS, and that any issued certificates that assert the certificate policy object identifiers identified in Section 1.2, are issued in accordance with the stipulations of this WidePoint PIV SSP CPS. The WidePoint PIV SSP warrants that CRLs issued, and keys generated by the WidePoint PIV SSP are in conformance with this WidePoint PIV SSP CPS.

The WidePoint PIV SSP will conform and operate in accordance with the stipulations of this WidePoint PIV SSP CPS, and that the WidePoint PIV SSP:

- Will provide to the FPKIPA this WidePoint PIV SSP CPS, as well as any subsequent changes, for conformance assessment.
- Will conform to the stipulations of Common Policy and this WidePoint PIV SSP CPS, upon approval.
- Ensures that registration information is accepted only from WidePoint Registration Authorities who understand and are obligated to comply with this WidePoint PIV SSP CPS and Common Policy.
- Includes only valid and appropriate information in the certificate and maintains evidence that due diligence was exercised in validating that information contained in the certificate.

- Ensures that obligations are imposed on WidePoint PIV SSP Subscribers in accordance with Section 9.6.3 of this WidePoint PIV SSP CPS and that WidePoint PIV SSP Subscribers are informed of the consequences of not complying with those obligations.
- Revokes the certificates of WidePoint PIV SSP Subscribers found to have acted in a manner counter to WidePoint PIV SSP Subscriber obligations.
- Notifies WidePoint PIV SSP Subscribers and makes public for the benefit of WidePoint PIV SSP Subscribers and Relying Parties any changes to the WidePoint PIV SSP operations that may impact interoperability or security. The WidePoint PIV SSP will post the notification of any change to the ssp.orc.com website.
- Operates or provides for the services of an on-line repository that satisfies the obligations under Section 9.6.5.2 of this WidePoint PIV SSP CPS; and,
- Posts certificates and CRLs to the repository.

The WidePoint PIV SSP KED that provides escrowed keys to Requestors under this policy must conform to the stipulations of this document. In particular, the following stipulations apply:

- The FPKIPA has approved the WidePoint PIV SSP CPS/KRPS prior to key escrow.
- The WidePoint PIV SSP KED operates in accordance with the stipulations of this WidePoint PIV SSP CPS/KRPS and the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework .
- The WidePoint PIV SSP CA/KED automatically notifies the subscribers when their private keys have been escrowed during the subscriber registration process (e.g., a dialog box may appear on a subscriber's screen during the certificate request process).
- The WidePoint PIV SSP KED monitors WidePoint PIV SSP Key Recovery Agent and WidePoint PIV SSP Key Recovery Official activity for patterns of potentially anomalous activity as indicators of possible problems in the infrastructure, and initiate inquiries or investigations as appropriate.

WidePoint PIV SSP Subscriber (applicant) organizations that authorize their employees to perform roles as stipulated in this WidePoint PIV SSP CPS, warrant that:

- Procedures are implemented in accordance with Common Policy and this WidePoint PIV SSP CPS.
- All actions are accomplished in accordance with this WidePoint PIV SSP CPS.
- They will operate in accordance with the applicable sections of this WidePoint PIV SSP CPS.
- They meet the personnel and training requirements stipulated in this WidePoint PIV SSP CPS.
- The applicant organization will cooperate and assist the WidePoint PIV SSP in monitoring and auditing that they are operating in accordance with the applicable sections of this WidePoint PIV SSP CPS; and,
- Network security controls are in accordance with the applicable sections of this WidePoint PIV SSP CPS.

The WidePoint PIV SSP does not warrant the actions of Notaries Public or other persons legally empowered to witness and certify the validity of documents and to take affidavits and depositions, as stipulated by the FPKIPA.

With respect to WidePoint PIV SSP Subscriber or Relying Party Agreements or obligations made by a U.S. Government entity by purchasing the services associated with this WidePoint PIV SSP CPS, agreement and interpretation will be governed by the Contracts Disputes Act of 1978 as amended (codified at 41 U.S.C. section 601).

9.6.2 WidePoint PIV SSP Registration Authorities and Key Recovery Agent/Key Recovery Official Representations and Warranties

9.6.2.1 WidePoint PIV SSP Registration Authorities Obligations

A WidePoint PIV SSP Registration Authority that performs registration functions as described in this WidePoint PIV SSP CPS must comply with the stipulations of this this WidePoint PIV SSP CPS that is approved by the FPKIPA for use with the FPKIPA Common Policy CP. A WidePoint PIV SSP Registration Authority who is found to have acted in a manner inconsistent with these obligations is subject to revocation of WidePoint PIV SSP Registration Authority responsibilities. A WidePoint PIV SSP Registration Authority supporting this policy must conform to the stipulations of this document, including:

- Maintaining its operations in conformance to the stipulations of this WidePoint PIV SSP CPS.

- Including only valid and appropriate information in certificate requests and maintaining evidence that due diligence was exercised in validating the information contained in the certificate.
- Ensuring that obligations are imposed on Subscribers in accordance with Section 9.6.3, and that Subscribers are informed of the consequences of not complying with those obligations.

WidePoint PIV SSP Registration Authorities are obligated to accurately represent the information prepared for the WidePoint PIV SSP and to process requests and responses in a timely and secure manner. WidePoint PIV SSP Registration Authorities may designate WidePoint Local Registration Authorities; however, WidePoint Local Registration Authorities may not designate other WidePoint Local Registration Authorities under this WidePoint PIV SSP CPS. WidePoint Registration Authorities under this WidePoint PIV SSP CPS are not authorized to assume any other WidePoint PIV SSP administration functions.

When validating subscriber requests for certificates issued under this WidePoint PIV SSP CPS, a WidePoint Registration Authority accepts the following obligations:

- Approve the issuance of certificates only when both the Applicant or WidePoint PIV SSP Subscriber's request and the trusted agent validation have been received.
- To validate the accuracy of all information contained in the Applicant or WidePoint PIV SSP Subscriber's certificate request.
- To validate that the named Applicant or WidePoint PIV SSP Subscriber actually requested the certificate.
- Revoke certificates with properly validated revocation requests.
- Notify the Applicant or WidePoint PIV SSP Subscriber through electronic mail or other means that the certificate request has or has not been granted in accordance with Section 4.3.2 of this WidePoint PIV SSP CPS.
- Notify a WidePoint PIV SSP Subscriber of certificate revocation in accordance with Section 4.9.2 of this WidePoint PIV SSP CPS (or delegate this action to another WidePoint Registration Authority or a WidePoint Local Registration Authority).
- To use the WidePoint Registration Authority certificate only for purposes associated with the WidePoint Registration Authority function.
- To immediately revoke one's own WidePoint Registration Authority certificate and report to the WidePoint PIV SSP CA if private key compromise is suspected.
- To immediately revoke a WidePoint Registration Authority , a WidePoint Local Registration Authority or a WidePoint PIV SSP Subscriber certificate and inform the WidePoint PIV SSP Subscriber if private key compromise is suspected.
- To revoke and approve reissue of WidePoint PIV SSP Subscriber certificates, if necessary, that were validated by a WidePoint Registration Authority or a WidePoint Local Registration Authority whose private key is suspected to be compromised.
- To inform trusted agents and the WidePoint PIV SSP of any changes in WidePoint Registration Authority status.
- To protect the WidePoint Registration Authority certificate private key from unauthorized access.
- Validating the credentials of WidePoint Registration Authorities and WidePoint Local Registration Authorities.
- Training of WidePoint Registration Authorities and WidePoint Local Registration Authorities in accordance with the WidePoint System Security Plan Awareness and Training Control Family Control AT-3 Role-Based Training; and,
- Posting certificates to the repository.

A WidePoint Registration Authority who is found to have acted in a manner inconsistent with these obligations is subject to revocation of WidePoint Registration Authority responsibilities.

9.6.2.2 WidePoint PIV SSP Key Recovery Agents Obligations

WidePoint PIV SSP Key Recovery Agents that submit requests as described in this WidePoint PIV SSP CPS shall comply with the stipulations of this WidePoint PIV SSP CPS. In particular, the following stipulations apply:

- WidePoint PIV SSP Key Recovery Agents shall keep a copy of the Common Policy CP and this WidePoint PIV SSP CPS.
- WidePoint PIV SSP Key Recovery Agents shall protect subscribers' escrowed keys from unauthorized disclosure, including the encrypted files and associated decryption keys.
- WidePoint PIV SSP Key Recovery Agents shall protect all information associated with key recovery, including the WidePoint PIV SSP Key Recovery Agent's own key(s), that could be used to recover subscribers' escrowed keys.
- WidePoint PIV SSP Key Recovery Agents shall release WidePoint PIV SSP Subscribers' escrowed keys only for properly authenticated and authorized requests from Requestor.
- WidePoint PIV SSP Key Recovery Agents may rely upon the WidePoint PIV SSP Key Recovery Officials for authentication and verification of the identity and authority of the Requestor. However, WidePoint PIV SSP Key Recovery Agents shall also authenticate the identity of the Requestor when the Requestor digital signature is available.
- WidePoint PIV SSP Key Recovery Agents shall authenticate the WidePoint PIV SSP Key Recovery Officials as described in Section 3.5.4.
- WidePoint PIV SSP Key Recovery Agents shall validate the authorization of the WidePoint PIV SSP Key Recovery Official by ensuring that the WidePoint PIV SSP Key Recovery Official is an authorized WidePoint PIV SSP Key Recovery Official for the Subscriber for whom key recovery has been requested.
- WidePoint PIV SSP Key Recovery Agents shall protect all information regarding all occurrences of key recovery.
- WidePoint PIV SSP Key Recovery Agents shall communicate knowledge of a recovery process only to the WidePoint PIV SSP Key Recovery Official and Requestor involved in the key recovery.
- WidePoint PIV SSP Key Recovery Agents shall not communicate any information concerning a key recovery to the Subscriber except when the WidePoint PIV SSP Subscriber is the Requestor.
- WidePoint PIV SSP Key Recovery Agents shall monitor WidePoint PIV SSP Key Recovery Official activity for patterns of potentially anomalous behavior as indicators of possible problems in the infrastructure, and initiate inquiries or investigations as appropriate.

9.6.2.3 WidePoint PIV SSP Key Recovery Official Obligations

A WidePoint PIV SSP Key Recovery Official initiates a key recovery request for a Requestor. When using the services of a WidePoint PIV SSP Key Recovery Official, the Requestor is generally a third party, but this policy does not preclude the WidePoint PIV SSP Subscriber from seeking the assistance of a WidePoint PIV SSP Key Recovery Official to recover the WidePoint PIV SSP Subscriber's private key.

- The WidePoint PIV SSP Key Recovery Official shall protect the WidePoint PIV SSP Subscribers' recovered keys from compromise.
- After providing the Requestor with the encrypted key, the WidePoint PIV SSP Key Recovery Official shall destroy the copy of the key in his/her system.
- The WidePoint PIV SSP Key Recovery Official shall request the Subscriber's keys only upon receipt of a request from an authorized Requestor.
- The WidePoint PIV SSP Key Recovery Official, as an intermediary for the WidePoint PIV SSP Key Recovery Agent, shall validate the identity of any Requestor seeking a key recovery.
- When the Requestor is authenticated on the basis of digital signature, the WidePoint PIV SSP Key Recovery Official shall forward the Requestor's digitally signed object to the WidePoint PIV SSP Key Recovery Agent in a form verifiable by the WidePoint PIV SSP Key Recovery Agent.
- In the case of persons other than the WidePoint PIV SSP Subscriber seeking a key recovery, the WidePoint PIV SSP Key Recovery Official shall ensure that the Requestor has the authority to request the WidePoint PIV SSP Subscriber's private decryption key.
- The WidePoint PIV SSP Key Recovery Official, as an intermediary for the WidePoint PIV SSP Key Recovery Agent, shall validate the authorization for the request, to include consultation with legal counsel when appropriate.

- The WidePoint PIV SSP Key Recovery Official shall protect all information associated with key recovery, including the WidePoint PIV SSP Key Recovery Official's own private key(s), that could be used to obtain the Subscriber's recovered private decryption key(s).
- The WidePoint PIV SSP Key Recovery Official shall protect all information regarding all occurrences of key recovery.
- The WidePoint PIV SSP Key Recovery Official shall communicate knowledge of any recovery process only to the Requestor
- The WidePoint PIV SSP Key Recovery Official shall not communicate any information concerning a key recovery to the Subscriber except when the WidePoint PIV SSP Subscriber is the Requestor.
- The WidePoint PIV SSP Key Recovery Official shall accurately represent himself when requesting key recovery services.
- The WidePoint PIV SSP Key Recovery Official shall keep records of all recovery requests and disposition, including acknowledgement of receipt by the Requestor.

9.6.2.4 LRA Representations and Warranties

WidePoint PIV SSP LRAs are obligated to accurately represent the information prepared for the WidePoint PIV SSP and to process requests and responses in a timely and secure manner. WidePoint LRAs may designate other LRAs or WidePoint Partner LRAs, however WidePoint Partner LRAs may not designate other LRAs under this CPS. LRAs under this CPS are not authorized to assume any other WidePoint PIV SSP administration functions.

When validating subscriber requests for certificates issued under this WidePoint PIV SSP CPS, a WidePoint Local Registration Authority accepts the following obligations:

- To operate in accordance with the stipulations of this WidePoint PIV SSP CPS.
- To validate the accuracy of all information contained in the Applicant or WidePoint PIV SSP Subscriber's certificate request.
- To validate that the named Applicant or WidePoint PIV SSP Subscriber actually requested the certificate.
- To verify to the WidePoint Registration Authority that the certificate request originated from the named Applicant or WidePoint PIV SSP Subscriber and that the information contained in the certificate request is accurate.
- To use private keys only on machines protected and managed using commercial best practices.
- To request revocation and verify reissue requirements of a WidePoint PIV SSP Subscriber's certificate upon notification of changes to information contained in the certificate.
- To request revocation of the certificates of WidePoint PIV SSP Subscribers found to have acted in a manner counter to subscriber obligations.
- To inform WidePoint PIV SSP Subscribers and the WidePoint Registration Authority of any changes in the WidePoint Local Registration Authority's status.
- To ensure that obligations are imposed on WidePoint PIV SSP Subscribers in accordance with the subscriber obligations; and,
- To inform Applicants and WidePoint PIV SSP Subscribers of the consequences of not complying with those obligations.

A WidePoint Local Registration Authority who is found to have acted in a manner inconsistent with these obligations is subject to revocation of WidePoint Local Registration Authority responsibilities.

9.6.3 Subscriber and Data Description Server Representations and Warranties

9.6.3.1 Subscriber Representations and Warranties

For all certificate issuances to WidePoint PIV SSP Subscribers or WidePoint PIV SSP Sponsor who function as a WidePoint PIV SSP Subscriber for a Medium Device or Medium Hardware Device certificate, the WidePoint PIV SSP Subscriber must acknowledge through hand-written or digital signature a set of obligations for participating in the WidePoint PIV SSP. The list of obligations may vary depending on the type of certificate or credential the WidePoint PIV SSP Subscriber has received.

WidePoint PIV SSP Subscribers receiving Medium or Medium Hardware certificates must acknowledge the following obligations:

- To operate in accordance with the stipulations of this WidePoint PIV SSP CPS.
- To accurately represent themselves in all communications with the WidePoint PIV SSP.
- To protect the WidePoint PIV SSP issued certificate private key from unauthorized access in accordance with Section 6.2 of this WidePoint PIV SSP CPS as stipulated in their certificate acceptance agreements, and local procedures;
- To immediately report to a WidePoint Registration Authority or a WidePoint Local Registration Authority and request certificate revocation if private key compromise of WidePoint PIV SSP issued certificate or credential is suspected.
- To use the WidePoint PIV SSP issued certificate only for authorized applications which have met the requirements of Common Policy and this WidePoint PIV SSP CPS.
- To use the WidePoint PIV SSP issued certificate only for the purpose for which it was issued, as indicated in the key usage extension of the certificate only on machines that are protected and managed using commercial best practices.
- To use private keys only on the machines that are protected and managed using commercial best practices.
- To report any changes to information contained in the WidePoint PIV SSP issued certificate to the appropriate WidePoint Registration Authority or a WidePoint Local Registration Authority for certificate reissue processing; and,
- Abide by all the terms, conditions, and restrictions levied upon the use of their private keys and WidePoint PIV SSP issued certificates.

These obligations are provided to the Subscriber during the registration process in the form of a Subscriber Agreement that the Subscriber must read and agree to prior to completing registration. Theft, compromise, or misuse of the private key may cause the Subscriber, Relying Party, and their organization legal consequences.

For Medium Device and Medium Hardware Device, WidePoint PIV SSP Sponsors (as described in Section 1.3.7.2) assume the obligations of WidePoint PIV SSP Subscribers for the certificates associated with their components and attest to the following Subscriber obligations:

WidePoint PIV SSP Sponsors receiving Medium Device or Medium Hardware Device certificates must acknowledge the following obligations:

- To operate in accordance with the stipulations of this WidePoint PIV SSP CPS.
- To accurately represent themselves in all communications with the WidePoint PIV SSP.
- To protect the WidePoint PIV SSP issued certificate private key from unauthorized access in accordance with Section 6.2 of this WidePoint PIV SSP CPS as stipulated in their certificate acceptance agreements, and local procedures.
- To immediately report to a WidePoint Registration Authority or a WidePoint Local Registration Authority and request certificate revocation if private key compromise of WidePoint PIV SSP issued certificate or credential is suspected.
- In the event of a WidePoint PIV SSP Sponsor change due to the verified individual having left the employ of the affiliated company or is no longer assigned as the WidePoint PIV SSP Sponsor for the WidePoint PIV SSP issued certificate(s), the affiliated organization must designate a new WidePoint PIV SSP Sponsor for the certificate(s). The new WidePoint PIV SSP Sponsor must complete a new identity verification.
- When renewing the certificate, the WidePoint PIV SSP Sponsor must complete a new identity verification.
- Confirm that the WidePoint PIV SSP Sponsor) is a current employee of the affiliated company and that you are authorized by the affiliated company to obtain Medium Device and Medium Device Hardware certificates for the company by completing and submitting the WidePoint PIV SSP Component/Server Authorization letter.
- That the component designated in the certificate request is the only system on which the certificate is to be installed.
- To use their private keys only on the machines that are protected and managed using commercial best practices.

- To use the certificate only for authorized applications which have met the requirements of this WidePoint PIV SSP CPS.
- To use the certificate only for the purpose for which it was issued, as indicated in the key usage extension of the certificate; and,
- To report any changes to information contained in the certificate to the appropriate WidePoint Registration Authority for certificate reissue processing.
- WidePoint PIV SSP Subscribers signify and guarantee that their application does not interfere with or infringe upon the rights of any others regarding their trademarks, trade names, or any other intellectual property. WidePoint PIV SSP Subscribers shall hold WidePoint and the WidePoint PIV SSP harmless for any losses resulting from any such act.
- As a result of issuing a certificate that identifies a person as an employee or member of an organization, the WidePoint PIV SSP does not represent that the individual has authority to act for that organization.

For Relying Parties: Use of REVOKED certificates could have damaging or catastrophic consequences in certain applications. The matter of how often new Revocation data should be obtained is a determination to be made by the relying party and the system accreditor. If it is temporarily infeasible to obtain Revocation information, then the relying party must either reject use of the certificate, or make an informed decision to accept the risk, responsibility, and consequences for using a certificate whose authenticity cannot be guaranteed to the standards of the WidePoint PIV SSP practice statement.

9.6.3.2 Group Encryption Certificate Sponsor and User Representations and Warranties

Sponsors of group encryption certificates must:

- Assign the subject DN and Subject Alternate Name (SAN) of the group encryption certificate, ensuring they reflect the correct group and do not identify nor imply a single individual,
- Maintain a list of individuals having access to the group encryption certificate and its associated private key,
- Maintain a record of the dates and times individual group members have access to a centrally managed hardware group encryption certificate and its associated private key,
- Maintain a Shared Key Usage Agreement for each group member,
- Coordinate revocation requests or key recovery requests with WidePoint PIV SSP Registration Authorities,
- Provide the group member list and Shared Key Usage Agreements to WidePoint PIV SSP Registration Authorities upon request or once the group encryption certificate expires or is revoked.

An individual with access to a shared key corresponding to a group encryption certificate must:

- Accurately represent themselves in all communications with the WidePoint PIV SSP and the group sponsor.
- Protect the shared private key(s) at all times, in accordance with this policy and locally defined processes and procedures.
- Promptly notify the group sponsor, or other designated individual, upon suspicion of loss, compromise, or inappropriate use of the shared private key(s). Such notification must be made directly or indirectly through mechanisms consistent with this WidePoint PIV SSP CPS.
- Abide by all the terms, conditions, and restrictions levied on the use of the shared private key(s) and certificate(s).

9.6.3.3 Data Decryption Server Representations and Warranties

Prior to the beginning of the operation of a Data Decryption Server by a Customer Agency of the WidePoint PIV SSP program, the Customer Agency shall formally acknowledge and agree to the obligations described here by signing a WidePoint PIV SSP Data Decryption Server Practice Statement document that contains the following obligations.

- The Customer Agency Data Decryption Server shall be protected in accordance with the physical and logical security controls as stipulated in this WidePoint PIV SSP CPS. The Customer Agency Data Decryption Server shall operate Data Decryption Server in accordance with NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations Revision 5 MODERATE Baseline.
- The Customer Agency Data Decryption Server shall ensure that the audit logging of the system is configured for the type of events described in Section 5.4.1 of this WidePoint PIV SSP CPS and the Audit and

Accountability Control Family of NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations Revision 5 MODERATE Baseline and that the audit logs generated are retained for the archival retention period as stated in Section 5.5 of this WidePoint PIV SSP CPS.

- The Customer Agency Data Decryption Server shall only request WidePoint PIV SSP Subscribers' encryption key(s) from Subscribers that are affiliated with and were authorized for issuance by the Customer Agency.
- The Customer Agency Data Decryption Server shall protect Subscribers' recovered key(s) from compromise.
- The Customer Agency Data Decryption Server shall destroy Subscribers' keys when no longer required (i.e., when the data has been recovered).
- The Customer Agency Data Decryption Server shall request the Subscriber's escrowed key(s) only upon receiving a request to decrypt subscriber data from an authenticated authorized Customer Agency Enterprise system (e.g., an e-mail Server).
- The Customer Agency Data Decryption Server must use the Subscriber's recovered keys only to recover Subscriber's data requested from an authenticated authorized Customer Agency Enterprise system.

The Customer Agency Data Decryption Server shall provide accurate identification and authentication information at the same or higher assurance level as required for issuing new WidePoint PIV SSP certificates at the assurance level of the key being requested.

9.6.4 Relying Party Representations and Warranties

The WidePoint PIV SSP will publicly post a summary of this WidePoint PIV SSP CPS to the repositories as identified in Section 2 of this WidePoint PIV SSP CPS to provide the relying party information regarding the expectation of the WidePoint PIV SSP. When accepting a certificate issued under this WidePoint PIV SSP CPS, a Relying Party accepts the following obligations:

- Perform a risk analysis to decide whether the level of assurance provided by the certificate is adequate to protect the Relying Party based upon the intended use.
- Use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension).
- Establish trust in the certificate using certification path validation procedures described in [RFC 5280] prior to reliance; and,
- Preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data. Note: data format changes associated with application upgrades may invalidate digital signatures and shall be avoided.

9.6.5 Representations and Warranties of Other Participants

9.6.5.1 Representations and Warranties

The WidePoint PIV SSP warrants that all procedures are implemented in accordance with this WidePoint PIV SSP CPS and Common Policy, and that any certificates issued that assert any certificate policy object identifiers detailed in Section 1.2 of this WidePoint PIV SSP CPS are issued in accordance with the stipulations of Common Policy.

The WidePoint PIV SSP warrants that WidePoint Registration Authorities or Trusted Agents operate in accordance with the applicable sections of this WidePoint PIV SSP CPS and Common Policy.

9.6.5.2 Repository Representations and Warranties

The WidePoint PIV SSP warrants that WidePoint PIV SSP Repositories which support WidePoint PIV SSP CAs in posting information as required by this WidePoint PIV SSP CPS will:

- Contain an accurate and current CRL for each WidePoint PIV SSP CA for use by Relying Parties.
- Be publicly accessible through a web server gateway using HTTPS and FIPS 140-3 approved encryption.
- Be maintained in accordance with the practices specified in this WidePoint PIV SSP CPS; and,
- Meet or exceed the requirement of 99% availability for all repository components within the control of the WidePoint PIV SSP. Communication failures as a result of Internet problems external to the operating organization will not count against this availability requirement.

The WidePoint PIV SSP maintains a copy of all certificates and CRLs for archiving. The WidePoint PIV SSP provides this information on a certificate accessed web server posted no later than 10 days after the end of the collection of the data.

9.6.5.3 Trusted Agent Representations and Warranties

Trusted Agents will perform Applicant and WidePoint PIV SSP Subscriber identity verification in accordance with this WidePoint PIV SSP CPS and in accordance with Common Policy.

9.6.5.4 CSS Representations and Warranties

WidePoint PIV SSP CSSs provide revocation status of WidePoint PIV SSP certificates issued by WidePoint PIV SSP CAs and that assert a certificate policy object identifier detailed in Section 1.2 of this WidePoint PIV SSP CPS. The WidePoint PIV SSP CSSs conform to the stipulations of this WidePoint PIV SSP CPS and Common Policy, including:

- Providing to the FPKIPA this WidePoint PIV SSP CPS, as well as any subsequent changes, for conformance assessment.
- Conforming to the stipulations of this WidePoint PIV SSP CPS and Common Policy.
- Ensuring that certificate and revocation information is accepted only from valid WidePoint PIV SSP CAs; and,
- Including only valid and appropriate response, and to maintain evidence that due diligence was exercised in validating the status of a WidePoint PIV SSP issued certificate.

9.6.5.5 PKI Point of Contact Representations and Warranties

Organizations of Applicants and WidePoint PIV SSP Subscribers are required to appoint a WidePoint PIV SSP PKI Point of Contact to provide a single trusted point of contact with the WidePoint PIV SSP. Organizations may assign more than one WidePoint PIV SSP PKI Point of Contact. The organization's WidePoint PIV SSP PKI Point of Contact must comply with the stipulations of this WidePoint PIV SSP CPS and Common Policy. The organization's WidePoint PKI Point of Contact may request revocation of certificates issued to WidePoint PIV SSP Subscribers within the WidePoint PIV SSP PKI Point of Contact's organization. The organization's WidePoint PIV SSP PKI Point of Contact may receive the hardware tokens issued to WidePoint PIV SSP Subscribers within their organization for zeroization and/or destruction.

A WidePoint PIV SSP PKI Point of Contact who is found to have acted in a manner inconsistent with the stipulations of this WidePoint PIV SSP CPS and Common Policy is subject to removal as a WidePoint PIV SSP PKI Point of Contact. Failure to address the deficiencies of the WidePoint PIV SSP PKI Point of Contact by the organization may result in the revocation of any or all WidePoint PIV SSP certificates issued to the organization.

9.6.5.6 Third-Party Key Requestor Representations and Warranties

Third-party key recovery Requestors must formally acknowledge and agree to the obligations described here, prior to receiving a recovered key:

- The Third-Party Requestor must protect WidePoint PIV SSP Subscribers' recovered key(s) from compromise. The Third-Party Requestor must use a combination of computer security, cryptographic, network security, physical security, personnel security, and procedural security controls to protect their keys and recovered Subscribers' keys.
- The Third-Party Requestor must destroy or surrender WidePoint PIV SSP Subscribers' keys when no longer required (i.e., when the data has been recovered).
- The Third-Party Requestor must request and use the WidePoint PIV SSP Subscriber's escrowed key(s) only to recover Subscriber's data they are authorized to access.
- The Third-Party Requestor must accurately represent themselves to all entities during any key recovery service.
- When the request is made, the Third-Party Requestor must provide accurate identification and authentication information at least to the same level required for issuing new PKI certificates at the level of the key being requested (e.g., the Third-Party Requestor sends a digitally signed request using the credential issued by the Entity PKI at the same or higher assurance level as the key being recovered).

- The Third-Party Requestor must protect information concerning each key recovery operation.
- Upon receipt of the recovered key(s), the Third-Party Requestor must sign an acknowledgement of agreement to follow the law and the subscriber's organization policies relating to protection and release of the recovered key. Such agreement should include the following attestations:
  - Third Party Requestor has accurately represented their identity to all key recovery entities,
  - Third Party Requestor has truthfully described the reason(s) for the key recovery request,
  - Third Party Requestor has a legitimate and official need to obtain the requested key(s),
  - Third Party Requestor has received the recovered key(s),
  - Third Party Requestor will use the recovered key(s) only for the stated purpose(s),
  - Third Party Requestor will protect the recovered key(s) from unauthorized access. When no longer required, the Third Party Requestor shall either destroy the key(s) and inform the organization of destruction per agency requirements, or return any recovered key(s) stored on hardware to the organization,
  - Third Party Requestor is bound by applicable laws and regulations concerning the protection of the recovered key(s) and any data recovered using the key(s).

9.7 Disclaimers of Warranties

Without limiting other WidePoint PIV SSP Subscriber obligations stated in this WidePoint PIV SSP CPS, all WidePoint PIV SSP Subscribers are liable for any misrepresentations they make in certificates to third parties who, having verified one or more digital signatures with the certificate, reasonably rely on the representations contained therein.

9.8 Limitations of Liability

9.8.1 Loss Limitation

WidePoint disclaims any liability for loss due to use of certificates issued by the WidePoint PIV SSP provided that the certificate was issued in accordance with Common Policy and this WidePoint PIV SSP CPS and that the relying party has used validation information that complies with Common Policy and this WidePoint PIV SSP CPS. WidePoint acknowledges professional liability with respect to the WidePoint PIV SSP or WidePoint Registration Authorities and its trusted agents. The limit for losses per transaction due to improper actions by the WidePoint PIV SSP or WidePoint Registration Authorities and its trusted agents is limited to $1,000 (U.S. Dollars). The limit for losses per incident due to improper actions by the WidePoint PIV SSP or WidePoint Registration Authorities and its trusted agents is $1 million (U.S. Dollars).

9.8.2 Other Exclusions

WidePoint PIV SSP Subscribers signify and guarantee that their application does not interfere with or infringe upon the rights of any others regarding their trademarks, trade names, or any other intellectual property. WidePoint PIV SSP Subscribers will hold the WidePoint PIV SSP and WidePoint harmless for any losses resulting from any such act.

As a result of issuing a certificate that identifies a person as an employee or member of an organization, the WidePoint PIV SSP does not represent that the individual has authority to act for that organization.

9.8.3 U.S. Federal Government Liability

In accordance with Common Policy, WidePoint PIV SSP Subscribers and Relying Parties will have no claim against the US Federal Government arising from use of the WidePoint PIV SSP Subscriber's certificate or a WidePoint PIV SSP determination to terminate (revoke) a certificate. In no event will the US Government be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any certificate issued or revoked by the WidePoint PIV SSP under this WidePoint PIV SSP CPS.

WidePoint will have no claim for loss against the FPKIPA, including but not limited to the revocation of any WidePoint PIV SSP CA certificate.

WidePoint PIV SSP Subscribers and Relying Parties will have no claim against the US Federal Government arising from erroneous certificate status information provided by the servers and services operated by the WidePoint PIV SSP and by the US Federal Government.

9.9 INDEMNITIES

Agents of the WidePoint PIV SSP (e.g., WidePoint Registration Authorities, WidePoint Issuer, WidePoint Registrar, WidePoint Local Registration Authorities, etc.) assume no financial responsibility for improperly used certificates issued by the WidePoint PIV SSP.

9.10 TERM AND TERMINATION

9.10.1 TERM

This WidePoint PIV SSP CPS will remain in effect until an updated WidePoint PIV SSP CPS supplants this CPS, or the WidePoint PIV SSP is terminated.

9.10.2 TERMINATION

This WidePoint CPS will survive any termination of the WidePoint PIV SSP. The requirements of this WidePoint CPS remain in effect through the end of the archive period for the last certificate issued.

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

The responsibilities for protecting business confidential and personal information, and for protecting WidePoint's intellectual property rights will survive termination of this WidePoint PIV SSP CPS.

Intellectual property rights will survive this WidePoint PIV SSP CPS, in accordance with the IP laws of the United States.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

The WidePoint PIV SSP will use commercially reasonable methods to communicate with all parties.

The WidePoint PIV SSP notifies the FPKIPA of any planned changes to the WidePoint PIV SSP infrastructure that have the potential to affect the FPKI operational environment. The WidePoint PIV SSP will notify the FPKI at least two weeks prior to the implementation. All new artifacts such as WidePoint PIV SSP Certificate Authority certificates, CRL DP locations, AIA locations, or other extensions that may contain location reference information such as Subject Information Access, etc., that are produced or modified as a result of the change will be provided to the FPKIPA within 24 hours following implementation as documented in the WidePoint System Change Request. Information not related to the WidePoint PIV SSP program and the system change or any Privacy Information(PII) may be redacted in the WidePoint System Change Request or other artifacts prior to transmission to the FPKIPA.

9.12 AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENT

WidePoint will notify the FPKIPA of any changes to this WidePoint PIV SSP CPS. WidePoint will also post notification of changes on the web site associated with the WidePoint PIV SSP operations as applicable to the WidePoint PIV SSP summary and other publicly available documentation. WidePoint will notify subscribers of any changes to subscriber obligations via posting to the WidePoint PIV SSP website. WidePoint will post a summary of this WidePoint PIV SSP CPS on its web site. WidePoint PIV SSP Subscriber obligation changes will be published within 7 days.

The FPKIPA will make the determination that this WidePoint PIV SSP CPS complies with the certificate policies identified in Section 1.2 of this WidePoint PIV SSP CPS.

9.12.2 Notification Mechanism and Period

The WidePoint PIV SSP will publish information (including this WidePoint PIV SSP CPS with sensitive data redacted) on the WidePoint PIV SSP web site.

9.12.3 Circumstances Under Which OID Must be Changed

A certificate policy object identifier will only change if the change in Common Policy results in a material change to the trust by the relying parties.

9.13 Dispute Resolution Provisions

The FPKIPA will be the sole arbiter of disputes over the interpretation or applicability of Common Policy.

With respect to Subscriber or Relying Party Agreements or Obligations made by an entity by purchasing the services associated with this WidePoint PIV SSP CPS an attempt will be made to resolve any dispute through an independent mediator, mutually agreed to by all disputing parties. If mediation is unsuccessful in resolving such a dispute, it will be resolved by arbitration in accordance with applicable statutes.

9.14 Governing Law

The laws of the United States of America will govern the enforceability, construction, interpretation, and validity of this WidePoint PIV SSP CPS with respect to the Common Policy and the Memorandum of Understanding between the FPKIPA and WidePoint, the provider of the WidePoint PIV SSP.

With respect to Subscriber or Relying Party Agreements or Obligations made by a US Government entity by purchasing the services associated with this WidePoint PIV SSP CPS, Agreement and interpretation will be governed by the Contracts Disputes Act of 1978 as amended (codified at 41 U.S.C. section 601). If the individuals or organizations purchasing the services associated with this WidePoint PIV SSP CPS are not within the jurisdiction of the US Government, the laws of the Commonwealth of Virginia will apply.

In the event of any conflict between Common Policy and this WidePoint PIV SSP CPS, the WidePoint PIV SSP CPS shall take precedence. Except to the extent prohibited by law, in the event of any conflict between this WidePoint PIV SSP CPS or Common Policy, on the one hand, and any WidePoint PIV SSP Subscriber or Subscriber Organization Agreement, or other document issued or agreement entered into by the WidePoint PIV SSP in connection with the performance of services under this WidePoint PIV SSP CPS, on the other hand, Common Policy, or this WidePoint PIV SSP CPS, respectively, shall take precedence. The provisions of this WidePoint PIV SSP CPS cannot be overridden, bypassed, or changed by any document issued or agreement entered into by the WidePoint PIV SSP in connection with the performance of services under this WidePoint PIV SSP CPS.

Various laws and regulations may apply, based on the jurisdiction in which a certificate is issued or used. It is the responsibility of the certificate holder, or user, to ensure adherence to all applicable laws and regulations.

9.15 Compliance with Applicable Law

No stipulation.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This WidePoint PIV SSP CPS shall constitute the entire understanding and agreement between the parties with respect to the transactions contemplated and supersedes any and all prior or contemporaneous oral or written representation, understanding, agreement, or communication concerning the subject matter hereof. No party is relying upon any warranty, representation, assurance, or inducement not expressly set forth herein and none shall have any liability in relation to any representation or other assurance not expressly set forth herein, unless it was made fraudulently. Without prejudice to any liability for fraudulent misrepresentation, no party shall be under any

liability or shall have any remedy in respect of misrepresentation or untrue statement unless and to the extent that a claim lies for breach of a duty set forth in this WidePoint PIV SSP CPS.

9.16.2 Assignment

Parties may not assign any of their rights or obligations under this WidePoint PIV SSP CPS or applicable agreements without the written consent of WidePoint.

9.16.3 Severability

Should it be determined that one section of this WidePoint PIV SSP CPS is incorrect or invalid, all other sections remain in effect until the policy is updated. Requirements for updating this policy are described in Section 9.12 of this WidePoint PIV SSP CPS. Responsibilities, requirements, and privileges of this document are transferred to the newer edition upon release of that newer edition.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

Neither Party will be liable for any failure or delay in performing an obligation under this WidePoint PIV SSP CPS that is due to any of the following causes, to the extent beyond its reasonable control: acts of God, accident, riots, war, terrorist act, epidemic, pandemic (including the COVID-19 pandemic), quarantine, civil commotion, breakdown of communication facilities, breakdown of web host, breakdown of internet service provider, natural catastrophes, governmental acts or omissions, changes in laws or regulations, national strikes, fire, explosion, or generalized lack of availability of raw materials or energy.

For the avoidance of doubt, Force Majeure shall not include (a) financial distress nor the inability of either party to make a profit or avoid a financial loss, (b) changes in market prices or conditions, or (c) a party's financial inability to perform its obligations hereunder.

9.17 Other Provisions

No stipulation.

10 CERTIFICATE AND CRL FORMATS

When used as URI, Universally Unique Identifier (UUID) used in WidePoint PIV SSP issued certificates conform to *UUID URN Namespace* [RFC 4122] requirement. When used as a Serial Number attribute, the UUID shall be encoded using the UUID string representation defined in Section 3 of RFC 4122 (e.g., "f81d4fae-7dec-11d0-a765-00a0c91e6bf6"). Since UUID is associated with a WidePoint PIV SSP PIV and PIV-I credential, when used, the same UUID shall be asserted in all applicable certificates and in all applicable other signed objects on a WidePoint PIV SSP PIV and PIV-I credential

None of the WidePoint PIV SSP issued certificates, WidePoint PIV SSP CRLs or OCSP Responses that are valid beyond 31 December 2030 will be signed using or contain 2048 bit or lower security RSA keys.

WidePoint PIV SSP certificates issued using profiles specified in the previous version of this WidePoint PIV SSP CPS and Common Policy may be used until expired. All new WidePoint PIV SSP issued certificates shall conform to these profiles.

The following certificate and CRL profiles are in compliance with the FPKIPA's Common Policy X.509 Certificate and Certificate Revocation List (CRL) Profiles, version 2.1 dated February 1, 2021.

10.1 ENCODING DATES IN CERTIFICATES AND CRLS

notBefore and notAfter fields in WidePoint PIV SSP issued certificates; thisUpdate and nextUpdate fields in CRLs; and revocation date in CRL entries are encoded using the following rules:

- Dates through 2049 shall be encoded as UTCTime; and,
- Dates from 2050 onwards shall be encoded as GeneralizedTime.

Invalidity Date, a CRL entry extension is always encoded as GeneralizedTime. producedAt, a field in OCSP response is always encoded as GeneralizedTime.

10.2 SUBJECT PUBLIC KEY INFORMATION (SPKI)

The subject public key information for WidePoint PIV SSP issue certificates contain one of the following values:

- 2048, 3072 or 4096 bit RSA using rsaEncryption {1 2 840 113549 1 1 1} algorithm OID.
- Uncompressed EC point using ecPublicKey {1 2 840 10045 2 1} algorithm OID and namedCurve P-384 {1 3 132 0 34} as the parameter

10.3 CERTIFICATE POLICY OIDS

This section describes the rules for including certificate policy object identifiers in the certificate policies extension of various types of WidePoint PIV SSP issued certificates including WidePoint PIV SSP CA certificates. WidePoint PIV SSP CSS certificates contain the certificate policy object identifiers for which the delegating WidePoint PIV SSP CA considers the WidePoint PIV SSP CSS to be authoritative.

WidePoint PIV SSP CA certificates and WidePoint PIV SSP Subscriber certificates other than WidePoint PIV SSP CSS certificates contain certificate policy object identifiers using the following rules:

- Hardware, software, or device certificate policy object identifier is determined by the type of cryptographic module in which the WidePoint PIV SSP Subscriber private key is stored.
- SHA-384 certificate policy object identifiers can be asserted in a WidePoint PIV SSP issued certificate if all of the following are true:
  - Hashing algorithm used to hash the contents of the certificate is SHA-384.
  - CA key pair used to sign the certificate is 3072 or 4096 bit RSA or EC P-384
  - Subject public key in the certificate is 3072 or 4096 bit RSA or EC P-384
- WidePoint PIV SSP PIV-I certificate policy object identifiers are only asserted in PIV-I Authentication certificate as listed in the certificate profiles later on in this WidePoint PIV SSP CPS.

A WidePoint PIV SSP certificate shall never contain higher assurance certificate policy object identifier as detailed in Section 1.2 of this WidePoint PIV SSP CPS than those determined using the above rules. A WidePoint PIV SSP certificate may contain lower assurance certificate policy object identifiers than those determined using the above rules. In order to maximize issuance flexibility, it is recommended that a WidePoint PIV SSP CA certificate contain the lower assurance certificate policy object identifiers than those determined using the above rules.

10.4 Signature Algorithm OIDs

A WidePoint PIV SSP issued certificate or CRL must contain one of the following values for the signature algorithm OID.

- Certificates and CRLs signed using 2048 bit RSA CA key pair are signed using SHA-256 hash and thus assert sha256WithRSAEncryption signature algorithm OID.
- Certificates and CRLs signed using 3072 or 4096 bit RSA CA key pair are signed using SHA-384 hash and thus assert sha384WithRSAEncryption signature algorithm OID.
- Certificates and CRLs signed using EC P-384 CA key pair are signed using SHA-384 hash and thus assert ecdsa-with-SHA384 signature algorithm OID.

10.5 Certificate Profiles

Distinguished Namess(DN) listed in these profiles are in LDAP display order, i.e., the RDNs are listed in reverse order from the actual RDNs in the certificate.

10.5.1 WidePoint PIV SSP Intermediate CA Certificate

Note: This certificate is issued to the WidePoint PIV SSP Intermediate Certificate Authority by the FPKI. Its purpose is to issue certificates to CA servers that will issue end entity certificates. The WidePoint PIV SSP Intermediate Certificate Authority does not issue certificates to end entities.

Field	Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Value per Section 10.4
Issuer Distinguished Name	CN = Federal Common Policy CA G2, OU=FPKI, O=U.S. Government,C=US
Validity Period	10 years or less from date of issue; Dates encoded per Section 10.1
Subject Distinguished Name	cn=WIDEPOINT PIV SSP INTERMEDIATE [UNIQUE NAME] <#>[3], o=ORC PKI c=US
Subject Public Key Information	Value per Section 10.2
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	Value per Section 10.4
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the Common Policy CA's public key information) authorityCertIssuer and authorityCertSerialNumber must not be populated.
Subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the Common Policy public key information)
key usage	c=yes; keyCertSign, cRLSign
Certificate policies	c=no; one or more of certificate policy object identifiers from Section 1.2 of this WidePoint PIV SSP CPS as appropriate and per Section 10.3; Policy Qualifier Id=CPS Qualifier: https://ssp.orc.com/WidePointPIVSSPCPS.pdf
Basic Constraints	c=yes; cA=True; path length constraint = 0

[3] The optional "UNIQUE NAME" field can be used to provide additional descriptive information about a CA (e.g., HW, SW, etc.).

Field	Certificate Value
Policy Constraints	c=yes; Required Explicit Policy Skip Certs=0 Inhibit Policy Mapping Skip Certs=0
Inhibit Any Policy	C=yes; SkipCerts=0
Name Constraints	Not Present
Subject Information Access	c=no; [1]Authority Info Access Access Method=Certification Repository (1.3.6.1.5.5.7.48.5) Alternative Name: URL=http://crl-server.orc.com/caCerts/caCertsIssuedBy<CA NAME>.p7c
Authority Information Access	c=no; [1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://repo.fpki.gov/fcpca/caCertsIssuedTofcpcag2.p7c
CRL Distribution Points[4]	c=no; [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://repo.fpki.gov/fcpca/fcpcag2.crl

[4] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and crlIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

10.5.2 WIDEPOINT PIV SSP CA CERTIFICATE

Note: These certificates are WidePoint PIV SSP Certificate Authorities that issue certificates to end entities.

Field	Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Value per Section 10.4
Issuer Distinguished Name	CN = Federal Common Policy CA G#, OU=FPKI, O=U.S. Government,C=US or cn=WIDEPOINT PIV SSP INTERMEDIATE [UNIQUE NAME] <#>[5], o=ORC PKI c=US
Validity Period	10 years or less from date of issue; Dates encoded per Section 10.1
Subject Distinguished Name	cn=WIDEPOINT PIV SSP [UNIQUE NAME] <#>[6], o=ORC PKI c=US or cn=[Agency specific name], o=ORC PKI c=US
Subject Public Key Information	Value per Section 10.2
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	Value per Section 10.4
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the Common Policy CA's public key information) authorityCertIssuer and authorityCertSerialNumber must not be populated.
Subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the Common Policy public key information)
key usage	c=yes; keyCertSign, cRLSign
Certificate policies	c=no; one or more of certificate policy object identifiers from Section 1.2 of this WidePoint PIV SSP CPS as appropriate and per Section 10.3;
Basic Constraints	c=yes; cA=True; path length constraint = 0
Subject Information Access	c=no; [1]Authority Info Access Access Method=Certification Repository (1.3.6.1.5.5.7.48.5) Alternative Name: URL=http://crl-server.orc.com/caCerts/<CA NAME>.p7c
Authority Information Access	c=no; [1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://crl-server.orc.com/caCerts/<CA NAME>.p7c
CRL Distribution Points[7]	c=no; [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://repo.fpki.gov/fcpca/fcpcag2.crl or URL= http://crl-server.orc.com/CRLs/<CA Name>.crl

[5] The optional "UNIQUE NAME" field can be used to provide additional descriptive information about a CA (e.g., HW, SW, etc.).

[6] The optional "UNIQUE NAME" field can be used to provide additional descriptive information about a CA (e.g., HW, SW, etc.).

[7] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and crlIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

10.5.3 PIV CONTENT SIGNING CERTIFICATE

This certificate profile is for the certificate that signs the content that is embedded on each WidePoint PIV SSP PIV credential. Each WidePoint PIV SSP CMS has its own PIV content signing certificate.

Field	Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) ecdsa-with-Sha512 (1.2.840.10045.4.3.4) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms, the parameters field is NULL.
Issuer Distinguished Name	cn=WIDEPOINT PIV SSP <UNIQUE NAME #>, o=ORC PKI c=US
Validity Period	9 years or less from date of issue; Dates encoded per Section 10.1
Subject Distinguished Name	cn=<Descriptive WidePoint PIV SSP CMS Name>, o=ORC PKI c=US
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public keys must be encoded in uncompressed form. ECParameters is one of the following curves: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Extensions	
authority key identifier[8]	c=no; octet string
subject key identifier[9]	c=no; octet string
key usage	c=yes; digitalSignature
Extended key usage	c=yes; id-fpki-piv-content-signing; {2.16.840.1.101.3.6.7}
Authority Information Access	C=no; always present, [1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://crl-server.orc.com/caCerts/<CA NAME>.p7c [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://<CA short name>.eva.orc.com/

[8] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.

[9] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.

Field	Certificate Value
CRL Distribution Points[10]	c=no; always present, [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl-server.orc.com/CRLs/<CA NAME>.crl
Certificate policies	c=no; [1]Certificate Policy: Must only assert Policy Identifier=2.16.840.1.101.3.2.1.3.39 {id-fpki-common-contentSigning};

[10] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and crlIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

10.5.4 PIV AUTHENTICATION CERTIFICATE

Field	Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) ecdsa-with-Sha512 (1.2.840.10045.4.3.4) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms, the parameters field is NULL.
Issuer Distinguished Name	cn=WIDEPOINT PIV SSP [UNIQUE NAME] <#>, o=ORC PKI c=US
Validity Period	3 years or less from date of issue; Dates encoded per Section 10.1
Subject Distinguished Name	Must use one of the name forms for human subscribers specified in Section 3.1.1 of the WidePoint PIV SSP CPS.
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public keys must be encoded in uncompressed form. ECParameters is one of the following curves: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Extensions	
key usage	c=yes; digitalSignature
Extended key usage	c=no; The following keyPurposeID values must be included: 1.3.6.1.5.5.7.3.2 TLS client authentication 1.3.6.1.4.1.311.20.2.2 Microsoft Smart Card Logon One or more additional keyPurposeIds consistent with authentication purposes may be specified. For example; 1.3.6.1.5.2.3.4 id-pkinit-KPClientAuth 1.3.6.1.5.5.7.3.21 id-kp-secureShellClient (May only be required for administrators) Must not include the anyExtendedKeyUsage value. For certificates issued prior to June 30, 2019, anyExtendedKeyUsage may be present or this extension may be absent.
authority key identifier[11]	c=no; octet string
subject key identifier[12]	c=no; octet string

[11] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.

[12] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.

Field	Certificate Value
subject Alternative Name	c=no; Must include FASC-N and UUID. FASC-N otherName has type-id 2.16.840.1.101.3.6.6 and specifies the FASC-N of the PIV Card. UUID uniformResourceIdentifier contains the GUID data element of the CHUID of the PIV Card encoded as a URN as specified in Section 3 of RFC 4122. Any additional name types may be included to support local applications. A common example is the Microsoft User Principal Name (UPN) 1.3.6.1.4.1.311.20.2.3
CRL Distribution Points[13]	c=no; always present, [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl-server.orc.com/CRLs/<CA NAME>.crl
Authority Information Access	C=no; always present, [1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://crl-server.orc.com/caCerts/<CA NAME>.p7c [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://<CA short name>.eva.orc.com/
Certificate policies	c=no; [1]Certificate Policy: Policy Identifier=2.16.840.1.101.3.2.1.3.13 {id-fpki-common-authentication};
PIV NACI (optional)	The PIV interim_indicator extension is defined in appendix B.2 of FIPS 201-3. The value of this extension is asserted as follows: TRUE if, at the time of credential issuance the subject's NACI has not been completed. FALSE if, at the time of credential issuance, the subject's NACI has been completed and successfully adjudicated.
Subject Directory Attributes (optional)	c=no; {id-pda-countryOfCitizenship AttributeType ::= {1.3.6.1.5.5.7.9.4} CountryOfCitizenship ::= PrintableString (SIZE (2)) -- ISO 3166 Country Code}[14]

[13] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and crlIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

[14] The system shall be capable of asserting multiple citizenships using the CountryOfCitizenship OID multiple times.

10.5.5 CARD AUTHENTICATION CERTIFICATE

Field	Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) ecdsa-with-Sha512 (1.2.840.10045.4.3.4) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms, the parameters field is NULL.
Issuer Distinguished Name	cn=WIDEPOINT PIV SSP [UNIQUE NAME] <#>, o=ORC PKI c=US
Validity Period	3 years or less from date of issue; Dates encoded per Section 10.1
Subject Distinguished Name	Must use one of the name forms for human subscribers specified in Section 3.1.1 of the WidePoint PIV SSP CPS.
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public keys must be encoded in uncompressed form. ECParameters is one of the following curves: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Extensions	
key usage	c=yes; digitalSignature
Extended key usage	c=yes; Must assert only id-PIV-cardAuth keyPurposeID (2.16.840.1.101.3.6.8). The id-PIV-cardAuth keyPurposeID specifies that the public key is used to authenticate the PIV Card rather than the PIV card holder.
authority key identifier[15]	c=no; octet string
subject key identifier[16]	c=no; octet string
subject Alternative Name	c=no; Must include FASC-N and UUID. No other name forms may be included. FASC-N: otherName specifies the type-id (2.16.840.1.101.3.6.6) with the FASC-N value as an OCTET STRING representing the PIV Card that contains the corresponding Card Authentication key. UUID: uniformResourceIdentifier contains the UUID from the GUID data element of the CHUID of the PIV Card encoded as a URI as specified in Section 3 of RFC 4122.

[15] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.

[16] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.

Field	Certificate Value
CRL Distribution Points[17]	c=no; always present, [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl-server.orc.com/CRLs/<CA NAME>.crl
Authority Information Access	C=no; always present, [1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://crl-server.orc.com/caCerts/<CA NAME>.p7c [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://<CA short name>.eva.orc.com/
Certificate policies	c=no; [1]Certificate Policy: Policy Identifier=2.16.840.1.101.3.2.1.3.17 {id-fpki-common-cardAuth};
PIV NACI (optional)	The PIV interim_indicator extension is defined in appendix B.2 of FIPS 201-3. The value of this extension is asserted as follows: TRUE if, at the time of credential issuance, (1) the FBI National Criminal History Fingerprint Check has completed successfully, and (2) a NACI has been initiated but has not completed. FALSE if, at the time of credential issuance, the subject's NACI has been completed and successfully adjudicated.
Subject Directory Attributes (optional)	c=no; {id-pda-countryOfCitizenship AttributeType ::= {1.3.6.1.5.5.7.9.4} CountryOfCitizenship ::= PrintableString (SIZE (2)) -- ISO 3166 Country Code}[18]

[17] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and crlIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

[18] The system shall be capable of asserting multiple citizenships using the CountryOfCitizenship OID multiple times.

10.5.6 SIGNATURE CERTIFICATE

Field	Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) ecdsa-with-Sha512 (1.2.840.10045.4.3.4) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms, the parameters field is NULL.
Issuer Distinguished Name	cn=WIDEPOINT PIV SSP [UNIQUE NAME] <#>, o=ORC PKI c=US
Validity Period	3 years or less from date of issue; Dates encoded per Section 10.1
Subject Distinguished Name	Must use one of the name forms for human subscribers specified in Section 3.1.1 of the WidePoint PIV SSP CPS.
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public keys must be encoded in uncompressed form. ECParameters is one of the following curves: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Extensions	
key usage	c=yes; digitalSignature, nonRepudiation
Extended key usage	c=no; One or more keyPurposeIDs consistent with digital signature must be specified. Recommended: 1.3.6.1.5.5.7.3.4 id-kp-emailProtection (required for PIV) 1.3.6.1.4.1.311.10.3.12 MSFT Document Signing Must not include the anyExtendedKeyUsage value. For certificates issued prior to June 30, 2019, anyExtendedKeyUsage may be present or this extension may be absent.
authority key identifier[19]	c=no; octet string
subject key identifier[20]	c=no; octet string
subject Alternative Name (Optional)	c=no; rfc822Name is required if id-kp-emailProtection (1.3.6.1.5.5.7.3.4) is asserted in Extended Key Usage. otherName values (e.g., Microsoft UPN) may be included to support local applications.

[19] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.

[20] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.

Field	Certificate Value
CRL Distribution Points[21]	c=no; always present, [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl-server.orc.com/CRLs/<CA NAME>.crl
Authority Information Access	C=no; always present, [1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://crl-server.orc.com/caCerts/<CA NAME>.p7c [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://<CA short name>.eva.orc.com/
Certificate policies	c=no; One or more of the following policies must be asserted: [1]Certificate Policy: Policy Identifier=2.16.840.1.101.3.2.1.3.6 {id-fpki-common-policy} Policy Identifier=2.16.840.1.101.3.2.1.3.7 {id-fpki-common-hardware} Additional applicable agency specific policies may be asserted.
Subject Directory Attributes (optional)	c=no; {id-pda-countryOfCitizenship AttributeType ::= {1.3.6.1.5.5.7.9.4} CountryOfCitizenship ::= PrintableString (SIZE (2)) -- ISO 3166 Country Code}[22]

[21] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and crlIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

[22] The system shall be capable of asserting multiple citizenships using the CountryOfCitizenship OID multiple times.

10.5.7 KEY MANAGEMENT CERTIFICATE

Field	Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) ecdsa-with-Sha512 (1.2.840.10045.4.3.4) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms, the parameters field is NULL.
Issuer Distinguished Name	cn=WIDEPOINT PIV SSP [UNIQUE NAME] <#>, o=ORC PKI c=US
Validity Period	3 years or less from date of issue; Dates encoded per Section 10.1
Subject Distinguished Name	Must use one of the name forms for human subscribers specified in Section 3.1.1 of the WidePoint PIV SSP CPS.
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public keys must be encoded in uncompressed form. ECParameters is one of the following curves: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Extensions	
key usage	c=yes; keyEncipherment for RSA Subject Public Key keyAgreement for ECC Subject Public Key
Extended key usage	c=no; One or more keyPurposeIds consistent with key management purposes must be included. For PIV, 1.3.6.1.5.5.7.3.4 id-kp-emailProtection must be included. Must not include the anyExtendedKeyUsage value. For certificates issued prior to June 30, 2019, anyExtendedKeyUsage may be present or this extension may be absent.
authority key identifier[23]	c=no; octet string
subject key identifier[24]	c=no; octet string
subject Alternative Name (Optional)	c=no; rfc822Name is required if id-kp-emailProtection (1.3.6.1.5.5.7.3.4) is asserted in Extended Key Usage. otherName values (e.g., Microsoft UPN) may be included to support local applications.

[23] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.

[24] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.

Field	Certificate Value
CRL Distribution Points[25]	c=no; always present, [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl-server.orc.com/CRLs/<CA NAME>.crl
Authority Information Access	C=no; always present, [1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://crl-server.orc.com/caCerts/<CA NAME>.p7c [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://<CA short name>.eva.orc.com/
Certificate policies	c=no; [1]Certificate Policy: Policy Identifier=2.16.840.1.101.3.2.1.3.6 {id-fpki-common-policy}
Subject Directory Attributes (optional)	c=no; {id-pda-countryOfCitizenship AttributeType ::= {1.3.6.1.5.5.7.9.4} CountryOfCitizenship ::= PrintableString (SIZE (2)) -- ISO 3166 Country Code}[26]

[25] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and crlIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

[26] The system shall be capable of asserting multiple citizenships using the CountryOfCitizenship OID multiple times.

10.5.8 DERIVED PIV AUTHENTICATION CERTIFICATE

Field	Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) ecdsa-with-Sha512 (1.2.840.10045.4.3.4) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms, the parameters field is NULL.
Issuer Distinguished Name	cn=WIDEPOINT PIV SSP [UNIQUE NAME] <#>, o=ORC PKI c=US
Validity Period	3 years or less from date of issue; Dates encoded per Section 10.1
Subject Distinguished Name	Must use one of the name forms for human subscribers specified in Section 3.1.1 of the WidePoint PIV SSP CPS.
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public keys must be encoded in uncompressed form. ECParameters is one of the following curves: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Extensions	
key usage	c=yes; digitalSignature
Extended key usage	c=no; The following keyPurposeID values must be included: 1.3.6.1.5.5.7.3.2 TLS client authentication One or more additional keyPurposeIds consistent with authentication purposes may be specified. For example; 1.3.6.1.4.1.311.20.2.2 Microsoft Smart Card Logon 1.3.6.1.5.2.3.4 id-pkinit-KPClientAuth 1.3.6.1.5.5.7.3.21 id-kp-secureShellClient (May only be required for administrators) Must not include the anyExtendedKeyUsage value. For certificates issued prior to June 30, 2019, anyExtendedKeyUsage may be present or this extension may be absent.
authority key identifier[27]	c=no; octet string
subject key identifier[28]	c=no; octet string

[27] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.

[28] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.

Field	Certificate Value
subject Alternative Name	c=no; Must include uniformResourceIdentifier containing the UUID encoded as a URN as specified in Section 3 of RFC 4122. Any additional name types may be included to support local applications. A common example is the Microsoft User Principal Name (UPN) 1.3.6.1.4.1.311.20.2.3
CRL Distribution Points[29]	c=no; always present, [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl-server.orc.com/CRLs/<CA NAME>.crl
Authority Information Access	C=no; always present, [1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://crl-server.orc.com/caCerts/<CA NAME>.p7c [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://<CA short name>.eva.orc.com/
Certificate policies	c=no; [1]Certificate Policy: Must assert one of the following: Policy Identifier=2.16.840.1.101.3.2.1.3.40 {id-fpki-common-derived-pivAuth}; Policy Identifier=2.16.840.1.101.3.2.1.3.41 {Id-fpki-common-derived-pivAuth-hardware};
PIV NACI (optional)	The PIV interim_indicator extension is defined in appendix B.2 of FIPS 201-3. The value of this extension is asserted as follows: TRUE if, at the time of credential issuance, (1) the FBI National Criminal History Fingerprint Check has completed successfully, and (2) a background investigation has been initiated but has not completed. FALSE if, at the time of credential issuance, the subject's NACI has been completed and successfully adjudicated.
Subject Directory Attributes (optional)	c=no; {id-pda-countryOfCitizenship AttributeType ::= {1.3.6.1.5.5.7.9.4} CountryOfCitizenship ::= PrintableString (SIZE (2)) -- ISO 3166 Country Code}[30]

[29] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and crlIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

[30] The system shall be capable of asserting multiple citizenships using the CountryOfCitizenship OID multiple times.

10.5.9 AUTHENTICATION CERTIFICATE

Field	Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) ecdsa-with-Sha512 (1.2.840.10045.4.3.4) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms, the parameters field is NULL.
Issuer Distinguished Name	cn=WIDEPOINT PIV SSP [UNIQUE NAME] <#>, o=ORC PKI c=US
Validity Period	3 years or less from date of issue; Dates encoded per Section 10.1
Subject Distinguished Name	Must use one of the name forms for human subscribers specified in Section 3.1.1 of the WidePoint PIV SSP CPS.
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public keys must be encoded in uncompressed form. ECParameters is one of the following curves: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Extensions	
key usage	c=yes; digitalSignature
Extended key usage	c=no; The following keyPurposeID values must be included: 1.3.6.1.5.5.7.3.2 TLS client authentication One or more additional keyPurposeIds consistent with authentication may be specified. For example; 1.3.6.1.4.1.311.20.2.2 Microsoft Smart Card Logon 1.3.6.1.5.2.3.4 id-pkinit-KPClientAuth 1.3.6.1.5.5.7.3.21 id-kp-secureShellClient (May only be required for administrators) Must not include the anyExtendedKeyUsage value. For certificates issued prior to June 30, 2019, anyExtendedKeyUsage may be present or this extension may be absent.
authority key identifier[31]	c=no; octet string
subject key identifier[32]	c=no; octet string

[31] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.

[32] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.

Field	Certificate Value
subject Alternative Name (Optional)	c=no; One or more of the following are permitted: rfc822Name otherName values (e.g., Microsoft UPN) to support local applications directoryName to support local applications FASC-N must not be included
CRL Distribution Points[33]	c=no; always present, [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl-server.orc.com/CRLs/<CA NAME>.crl
Authority Information Access	C=no; always present, [1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://crl-server.orc.com/caCerts/<CA NAME>.p7c [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://<CA short name>.eva.orc.com/
Certificate policies	c=no; One or more of the following policies must be asserted: [1]Certificate Policy: Policy Identifier=2.16.840.1.101.3.2.1.3.6 {id-fpki-common-policy} Policy Identifier=2.16.840.1.101.3.2.1.3.7 {id-fpki-common-hardware} Additional applicable agency specific policies may be asserted.
Subject Directory Attributes (optional)	c=no; {id-pda-countryOfCitizenship AttributeType ::= {1.3.6.1.5.5.7.9.4} CountryOfCitizenship ::= PrintableString (SIZE (2)) -- ISO 3166 Country Code}[34]

[33] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and crlIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

[34] The system shall be capable of asserting multiple citizenships using the CountryOfCitizenship OID multiple times.

10.5.10 DEVICE CERTIFICATE

Device certificates are issued to devices of all types. The primary profile below represents a TLS web server. Additional components are identified in the following subsections with changed or added fields. The list in the following subsections is not exhaustive and additional types of devices may come to market that have the capability to protect the private key in a manner proscribed by this WidePoint PIV SSP CPS.

Field	Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) ecdsa-with-Sha512 (1.2.840.10045.4.3.4) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms, the parameters field is NULL.
Issuer Distinguished Name	cn=WIDEPOINT PIV SSP <UNIQUE NAME #>,o=ORC PKI c=US
Validity Period	3 years or less from date of issue; Dates encoded per Section 10.1
Subject Distinguished Name	Must use one of the name forms for human subscribers specified in Section 3.1.1 of the WidePoint PIV SSP CPS.
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public keys must be encoded in uncompressed form. ECParameters is one of the following curves: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Extensions	
authority key identifier[35]	c=no; octet string
subject key identifier[36]	c=no; octet string
key usage	c=yes; nonRepudiation must not be asserted in a device certificate. If a certificate is used for digital signature or authentication of ephemeral keys (e.g., TLS), digitalSignature must be asserted. If a certificate is used for key management: keyEncipherment must be asserted when public key is RSA keyAgreement must be asserted when public key is elliptic curve Note: Use of a single certificate for both digital signatures and key management is deprecated but may be used to support legacy applications that require the use of such certificates.

[35] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.

[36] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.

Field	Certificate Value
Extended key usage	c=yes or no; May be critical or non-critical. One or more key purposes consistent with the keyUsage must be specified. Must not include the anyExtendedKeyUsage value. For certificates issued prior to June 30, 2019, anyExtendedKeyUsage may be present or this extension may be absent.
subject Alternative Name (Optional)	c=no; One or more of the following are permitted: rfc822Name otherName values (e.g., Microsoft UPN) to support local applications directoryName to support local applications FASC-N must not be included
CRL Distribution Points[37]	c=no; always present, [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl-server.orc.com/CRLs/<CA NAME>.crl
Authority Information Access	C=no; always present, [1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://crl-server.orc.com/caCerts/<CA NAME>.p7c [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://<CA short name>.eva.orc.com/
Certificate policies	c=no; One of the following policies must be asserted: [1]Certificate Policy: Policy Identifier=2.16.840.1.101.3.2.1.3.8 {id-fpki-common-devices} Policy Identifier=2.16.840.1.101.3.2.1.3.36 {id-fpki-common-devicesHardware} Additional applicable agency specific policies may be asserted.

10.5.10.1 Domain Controller Certificate

This certificate type is used for Microsoft Domain Controllers and is required to enable smart card logon through a WidePoint PIV SSP signature or WidePoint PIV SSP PIV-I credential with a smart card logon extension. Each domain controller in the forest requires their own domain controller certificate.

Extensions	
key usage	c=yes; keyEncipherment and digitalSignature for RSA or digitalSignature for EC

[37] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and crlIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

Extended key usage	c=yes or no; May be critical or non-critical. One or more key purposes consistent with the keyUsage must be specified. Must not include the anyExtendedKeyUsage value. For certificates issued prior to June 30, 2019, anyExtendedKeyUsage may be present or this extension may be absent.
subject Alternative Name	c=no; DNS Name=<fully qualified computer name>; Other Name=DC GUID {1.3.6.1.4.1.311.25.1}=<GUID of Device receiving certificate>
Certificate Template {1.3.6.1.4.1.311.20.2.3}[38]	c=no; BMPString: DomainController; The actual extension value in HEX: 1E200044006F006D00610069006E0043006F006E00740072006F006C006C0065 0072

10.5.10.2 Machine Identity Certificate

This certificate type is used for identifying devices for VPN IPSec authentication primarily but can also be used to identify the device to applications and services.

Extensions	
key usage	c=yes; digitalSignature
Extended key usage	c=yes or no; May be critical or non-critical. One or more key purposes consistent with the keyUsage must be specified. Must not include the anyExtendedKeyUsage value. For certificates issued prior to June 30, 2019, anyExtendedKeyUsage may be present or this extension may be absent.
subject Alternative Name	c=no; DNS Name=<fully qualified computer name>; Other Name=DC GUID {1.3.6.1.4.1.311.25.1}=<GUID of Device receiving certificate>

10.5.10.3 Multi SAN Certificate

This certificate type is used for identifying multiple webservers with a single certificate through placing multiple domain names in the subject Alterative Name field. Up to twenty-five (25) domain names can be represented with one Multi SAN Certificate.

Extensions	
key usage	c=yes; digitalSignature
Extended key usage	c=yes or no; May be critical or non-critical. One or more key purposes consistent with the keyUsage must be specified. Must not include the anyExtendedKeyUsage value. For certificates issued prior to June 30, 2019, anyExtendedKeyUsage may be present or this extension may be absent.
subject Alternative Name	c=no; DNS Name=<fully qualified computer name>; DNS Name=<fully qualified computer name 2>; … DNS Name=<fully qualified computer name n>

[38] Field is specific to Domain controller certificates, may not appear in other device certificates

10.5.11 DELEGATED OCSP RESPONDER CERTIFICATE

Note: This profile is used only for WidePoint PIV SSP CSSs responder certificates. The WidePoint PIV SSP does not delegate OCSP Responder capabilities to organizations external to WidePoint.

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) ecdsa-with-Sha512 (1.2.840.10045.4.3.4) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms, the parameters field is NULL.
Issuer Distinguished Name	cn=WIDEPOINT PIV SSP <UNIQUE NAME #>,o=ORC PKI c=US
Validity Period	120 days or less from date of issue; Dates encoded per Section 10.1
Subject Distinguished Name	Must use one of the name forms for human subscribers specified in Section 3.1.1 of the WidePoint PIV SSP CPS.
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public keys must be encoded in uncompressed form. ECParameters is one of the following curves: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the WidePoint PIV SSP CA's public key information)
Subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the WidePoint PIV SSP CSS Responder public key information)
Key usage	c=yes; digitalSignature
Extended key usage	c=yes; Must assert only 1.3.6.1.5.5.7.3.9 id-kp-OCSPSigning
Subject Alternative Name (Optional)	c=no; The following name types may be present: dNSName is an IA5String that contains the DNS name of the subject URI is an IA5String that contains the URI of the subject rfc822Name that contains the email address of the sponsor, administrator, or help desk otherName values may also be included to support local applications
OCSP No Check	NULL

Field	Value
Authority Information Access (Optional)	C=no; always present, [1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://crl-server.orc.com/caCerts/<CA NAME>.p7c Must include the id-ad-caIssuers access method containing an HTTP URI pointing to either: a certs-only Cryptographic Message Syntax file (RFC 8551) with an extension of .p7c, or (discouraged) a single DER encoded certificate that has an extension of .cer (RFC 2585). The OCSP access method must not be included. See Section 5.2.
Certificate policies	c=no; Must assert all policy OIDs for which the OCSP server is authoritative. One or more of the following policies must be asserted: 2.16.840.1.101.3.2.1.3.6 id-fpki-common-policy 2.16.840.1.101.3.2.1.3.7 id-fpki-common-hardware 2.16.840.1.101.3.2.1.3.8 id-fpki-common-devices 2.16.840.1.101.3.2.1.3.13 id-fpki-common-authentication 2.16.840.1.101.3.2.1.3.17 id-fpki-common-cardAuth 2.16.840.1.101.3.2.1.3.36 id-fpki-common-devices-hardware 2.16.840.1.101.3.2.1.3.39 id-fpki-common-piv-contentSigning 2.16.840.1.101.3.2.1.3.40 id-fpki-common-derived-pivAuth 2.16.840.1.101.3.2.1.3.41 id-fpki-common-derived-pivAuth-hardware 2.16.840.1.101.3.2.1.3.45 id-fpki-common-pivi-authentication 2.16.840.1.101.3.2.1.3.46 id-fpki-common-pivi-cardAuth 2.16.840.1.101.3.2.1.3.47 id-fpki-common-pivi-contentSigning Additional applicable agency specific policy OIDs may be asserted.

10.5.12 SUBORDINATE CA CRL

Field	Subordinate CA CRL Value
Version	V2 (1)
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) ecdsa-with-Sha512 (1.2.840.10045.4.3.4) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms, the parameters field is NULL.
Issuer Distinguished Name	cn=WIDEPOINT PIV SSP <UNIQUE NAME #>,o=ORC PKI c=US
thisUpdate	Date encoded per Section 10.1
nextUpdate	thisUpdate + 2 days ≥ nextUpdate ≥ thisUpdate + CRL Issuance Frequency + 4 hours; Date encoded per Section 10.1

Field	Subordinate CA CRL Value
Revoked certificates list	userCertificate is the serial number of the certificate being revoked. revocationDate is the date and time of revocation. reasonCode CRL entry extension must be included for certificateHold. If the revocation reason is unspecified, this extension should be omitted. Use of this extension is optional for other reason codes. removeFromCRL must be used only in delta CRLs. Note: certificateHold must be used only for suspension of subscriber certificates. invalidityDate CRL entry extension may be included if the invalidity date precedes the revocation date.
CRL Extensions	
CRL Number	cRLNumber is a sequentially increasing number
Authority Key Identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the Common Policy public key information)

10.5.13 OCSP REQUEST FORMAT

OCSP requests are not expected to be signed. WidePoint PIV SSP CSS Responder will not check the signature on the request. See [RFC 6960] for detailed syntax. The following table lists which fields are required by the WidePoint CSS Responder.

Field	Expected Value
Version	V1 (0)
Requester Name	Not Required
Request List	List of certificates – generally this should be the list of two certificates: a WidePoint PIV SSP CA certificate and the end entity certificate issued by that WidePoint PIV SSP CA.
Signature	Not Required
Extensions	Not Required

10.5.14 OCSP RESPONSE FORMAT

See RFC2560 for detailed syntax. The following table lists which fields are populated by a WidePoint PIV SSP CSS Responder:

Field	Expected Value
Response Status	Successful | Malformed Request | Internal Error | Try Later
Response Type	id-pkix-ocsp-basic {1 3 6 1 5 5 7 48 1 1}
Version	V1 (0)
Responder ID	Hash of Responder public key
Produced At	Generalized Time
List of Responses	Each response will contain certificate id; certificate status[39], thisUpdate, nextUpdate[40],
Signature Algorithm	Value per Section 10.4
Signature	Present
Certificates	Applicable certificates issued to the OCSP Responder
Extensions	
Nonce	Will be present if nonce extension is present in the request

[39] If the certificate is revoked, the OCSP Responder will provide revocation time and revocation reason from CRL entry and CRL entry extension.

[40] The OCSP Responder will use thisUpdate and nextUpdate from CA CRL.

10.5.15 COMMON PIV-I CONTENT SIGNING CERTIFICATE

This certificate profile is for the certificate that signs the content that is embedded on each WidePoint PIV SSP PIV credential. Each WidePoint PIV SSP CMS has its own PIV content signing certificate.

Field	Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms, the parameters field is NULL.
Issuer Distinguished Name	cn=WIDEPOINT PIV SSP <UNIQUE NAME #>, o=ORC PKI c=US
Validity Period	9 years or less from date of issue; Dates encoded per Section 10.1
Subject Distinguished Name	Must use one of the name forms specified in Section 3.1.1 of the Common Certificate Policy and must indicate the organization administering the PIV-I card issuance system.
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public keys must be encoded in uncompressed form. ECParameters is one of the following curves: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Extensions	
authority key identifier[41]	c=no; octet string
subject key identifier[42]	c=no; octet string
key usage	c=yes; digitalSignature
Extended key usage	c=yes; id-fpki-pivi-content-signing; {2.16.840.1.101.3.8.7}
Authority Information Access	C=no; always present, [1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://crl-server.orc.com/caCerts/<CA NAME>.p7c [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://<CA short name>.eva.orc.com/
CRL Distribution Points[43]	c=no; always present, [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl-server.orc.com/CRLs/<CA NAME>.crl

[41] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.

[42] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.

[43] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and crlIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

Field	Certificate Value
Certificate policies	c=no; [1]Certificate Policy: Must only assert Policy Identifier=2.16.840.1.101.3.2.1.3.47 {id-fpki-common-pivi-contentSigning};

10.5.16 COMMON PIV-I AUTHENTICATION CERTIFICATE

Field	Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms, the parameters field is NULL.
Issuer Distinguished Name	cn=WIDEPOINT PIV SSP [UNIQUE NAME] <#>, o=ORC PKI c=US
Validity Period	3 years or less from date of issue; Dates encoded per Section 10.1
Subject Distinguished Name	Must use one of the name forms for human subscribers specified in Section 3.1.1 of the WidePoint PIV SSP CPS.
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public keys must be encoded in uncompressed form. ECParameters is one of the following curves: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Extensions	
key usage	c=yes; digitalSignature
Extended key usage	c=no; The following keyPurposeID values must be included: 1.3.6.1.5.5.7.3.2 TLS client authentication 1.3.6.1.4.1.311.20.2.2 Microsoft Smart Card Logon One or more additional keyPurposeIds consistent with authentication purposes may be specified. For example; 1.3.6.1.5.2.3.4 id-pkinit-KPClientAuth 1.3.6.1.5.5.7.3.21 id-kp-secureShellClient (May only be required for administrators) Must not include the anyExtendedKeyUsage value.
authority key identifier[44]	c=no; octet string
subject key identifier[45]	c=no; octet string
subject Alternative Name	c=no; Must include UUID. UUID uniformResourceIdentifier contains the GUID data element of the CHUID of the PIV-I Card encoded as a URN as specified in Section 3 of RFC 4122. Any additional name types may be included to support local applications. A common example is the Microsoft User Principal Name (UPN) 1.3.6.1.4.1.311.20.2.3

[44] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.

[45] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.

Field	Certificate Value
CRL Distribution Points[46]	c=no; always present, [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl-server.orc.com/CRLs/<CA NAME>.crl
Authority Information Access	C=no; always present, [1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://crl-server.orc.com/caCerts/<CA NAME>.p7c [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://<CA short name>.eva.orc.com/
Certificate policies	c=no; [1]Certificate Policy: Policy Identifier=2.16.840.1.101.3.2.1.3.45 {id-fpki-common-pivi-authentication};
Subject Directory Attributes (optional)	c=no; {id-pda-countryOfCitizenship AttributeType ::= {1.3.6.1.5.5.7.9.4} CountryOfCitizenship ::= PrintableString (SIZE (2)) -- ISO 3166 Country Code}[47]

[46] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and crlIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

[47] The system shall be capable of asserting multiple citizenships using the CountryOfCitizenship OID multiple times.

10.5.17 COMMON PIV-I CARD AUTHENTICATION CERTIFICATE

Field	Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Signature Algorithm	Choice of the following algorithms: id-RSASSA-PSS (1.2.840.113549.1.1.10) sha256WithRSAEncryption (1.2.840.113549.1.1.11) ecdsa-with-Sha256 (1.2.840.10045.4.3.2) ecdsa-with-Sha384 (1.2.840.10045.4.3.3) For id-RSASSA-PSS, specify the SHA-256 hash algorithm (2.16.840.1.101.3.4.2.1) as a parameter. For all other RSA algorithms, the parameters field is NULL.
Issuer Distinguished Name	cn=WIDEPOINT PIV SSP [UNIQUE NAME] <#>, o=ORC PKI c=US
Validity Period	3 years or less from date of issue; Dates encoded per Section 10.1
Subject Distinguished Name	Must use one of the name forms for human subscribers specified in Section 3.1.1 of the WidePoint PIV SSP CPS.
Subject Public Key	Must be either RSA or elliptic curve: RSA Encryption (1.2.840.113549.1.1.1) Elliptic Curve (1.2.840.10045.2.1) For RSA, modulus must be 2048, 3072, or 4096 bits and the parameters field is NULL. For EC, public keys must be encoded in uncompressed form. ECParameters is one of the following curves: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)
Extensions	
key usage	c=yes; digitalSignature
Extended key usage	c=yes; Must assert only id-PIV-cardAuth keyPurposeID (2.16.840.1.101.3.6.8). The id-PIV-cardAuth keyPurposeID specifies that the public key is used to authenticate the PIV-I Card rather than the PIV-I card holder.
authority key identifier[48]	c=no; octet string
subject key identifier[49]	c=no; octet string
subject Alternative Name	c=no; Must include UUID. No other name forms may be included. UUID: uniformResourceIdentifier contains the UUID from the GUID data element of the CHUID of the PIV Card encoded as a URI as specified in Section 3 of RFC 4122.
CRL Distribution Points[50]	c=no; always present, [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl-server.orc.com/CRLs/<CA NAME>.crl

[48] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.

[49] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.

[50] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and crlIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

Field	Certificate Value
Authority Information Access	C=no; always present, [1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://crl-server.orc.com/caCerts/<CA NAME>.p7c [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://<CA short name>.eva.orc.com/
Certificate policies	c=no; [1]Certificate Policy: Policy Identifier=2.16.840.1.101.3.2.1.3.46 {id-fpki-common-pivi-cardAuth};
Subject Directory Attributes (optional)	c=no; {id-pda-countryOfCitizenship AttributeType ::= {1.3.6.1.5.5.7.9.4} CountryOfCitizenship ::= PrintableString (SIZE (2)) -- ISO 3166 Country Code}[51]

[51] The system shall be capable of asserting multiple citizenships using the CountryOfCitizenship OID multiple times.

11 PIV-INTEROPERABLE SMART CARD DEFINITION

To support technical interoperability of PIV-I cards with Federal Agency PIV implementations, certificates asserting any of the PIV-I policies must comply with the technical specifications used for Federal Agency issued PIV cards. Hardware tokens used for Medium Hardware PIV-I and Card Authentication PIV-I certificates and the systems used to create them shall meet all of the following requirements.

- To ensure interoperability with Federal systems, PIV-I Cards shall use a smart card platform that is on GSA's Personal Identity Verification (PIV) of Federal Employees and Contractors [FIPS201-3] Evaluation Program Approved Product List (APL) and uses the PIV application identifier (AID).
- When Card Management System is used for PIV-I issuance, the Card Management Master Key shall conform to NIST SP 800-78.
- PIV-I Cards shall conform to NIST Special Publication 800-73, Interfaces for Personal Identity Verification [SP800-73], ensuring that PIV-I UUID requirements are met.
- PIV-I Cards shall contain an authentication certificate that conforms to the Medium Hardware PIV-I policy and the profile specified in Section 10.
- PIV-I Cards shall contain a card authentication certificate that conforms to the Card Authentication PIV-I policy, [SP800-73], and the profile specified in Section 10.
- PIV-I Cards shall contain an electronic representation (as specified in [SP800-73] and NIST Special Publication 800-76, Biometric Data Specification for Personal Identity Verification [SP800-76] of the Cardholder Facial Image printed on the card.
- PIV-I Cards shall contain an electronic representation (as specified in [SP800-76] of the fingerprint images collected during card registration.
- PIV-I Cards shall contain signature and encryption certificates that conform to the Medium Hardware PIV-I policy and the profile specified in Section 10.
- PIV-I Cards shall be visually distinguishable from Federal PIV Cards to ensure no suggestion of attempting to create a fraudulent Federal PIV Card. At a minimum, images or logos on a PIV-I Card shall not be placed entirely within Zone 11, Agency Seal, as defined by [FIPS201-3].
- The PIV-I Card physical topography shall include, at a minimum, the following items on the front of the card:
    - Cardholder facial image;
    - Cardholder full name;
    - Organizational Affiliation, if exists; otherwise, the issuer of the card; and
    - Card expiration date.
- PIV-I Cards shall have an expiration date not to exceed 3 years after issuance date.
- Expiration of the PIV-I Card shall not be later than expiration of Content Signing PIV-I certificate used to sign the content on the card.
- The digital signature certificate that is used to sign objects on the PIV-I Card (e.g., CHUID, Security Object) shall contain the Content Signing PIV-I policy OID and shall conform to the profile in Section 10.
- The Content Signing PIV-I certificate, and corresponding private key shall be managed within a trusted CMS.
- At issuance, the RA shall activate and release the PIV-I Card to the subscriber only after a successful 1:1 biometric match of the applicant against the biometrics collected in Section 3.2.3.1.
- To activate the card for personalization or update, the card management system shall perform a challenge response protocol using cryptographic keys stored on the card in accordance with [SP800-73]. When cards are personalized, card diversified keys shall be set to be specific to each PIV-I Card. That is, each PIV-I Card shall contain a unique card diversified key. Card diversified keys shall meet the algorithm and key size requirements stated in NIST Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification [SP800-78]. At a minimum, the Secure Channel specification version 02 with three key 3DES along with a plan to transition to AES shall be implemented

12 APPENDIX A: PIV AND COMMON PIV INTEROPERABLE COMPARISON

	Technical Requirements	PIV	PIV-I
Trust	Suitability Assurance: Favorably adjudicated National Agency Check with Inquiries (minimum) or other Tier 1 investigation	X	
	PIV policy object identifier on PIV Authentication Certificates	X	
	PIV-I equivalent policy object identifier on PIV-I Authentication Certificates		X
	PIV Content Signing object signing certificate	X	
	PIV-I Content Signing equivalent object signing certificate		X
	PIV Card Authentication Certificate	X	
	PIV-I Card Authentication Certificate		X
	Card must not be valid for more than 6 years and card expiration must not exceed the expiration date of object signing certificate	X	X
Credential Edge	Card stock certified by FIPS 201 Evaluation Program	X	X
	Command edge and NIST SP 800-85 conformant	X	X
	NIST SP 800-73 conformant data model and PIV Application Identifier (AID)	X	X
	NIST SP 800-73 conformant to include GUID present in the CHUID	X	X
	RFC 4122 conformant UUID required in the GUID data element of the CHUID	X	X
	RFC 4122 conformant UUID present in the Authentication Certificates	X	X
Topography	FIPS 201 compliant topography	X	
	Minimally contains facial image, cardholder name, issuing organization, and expiration, but does not replicate FIPS 201 topography requirements		X
Card Management System	Card Management Master Key maintained in a FIPS 140-3 Level 2 Cryptographic Module and conforms to [NIST SP 800-78] requirements; activation of the Card Management Master Key requires commensurate authentication of Trusted Roles	X	X

13 REFERENCES

The following documents contain information that provides background, examples, or details about the contents of this policy.

Number	Title
ABADSG	Digital Signature Guidelines, 1996-08-01. http://itlaw.wikia.com/wiki/American_Bar_Association_(ABA)_Digital_Signature_Guidelines
APL	Approved Products List (APL) https://www.idmanagement.gov/buy/#products/
AUDIT	FPKI Annual Review Requirements https://www.idmanagement.gov/docs/fpki-annual-review-requirements.pdf
CCP-PROF	Common Policy X.509 Certificate and Certificate Revocation List (CRL) Profiles https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-x509-cert-profile-ssp.pdf
Executive Order 12968	Executive Order 12968 - Access to Classified Information https://www.govinfo.gov/content/pkg/FR-1995-08-07/pdf/95-19654.pdf
FIPS 140-3	Security Requirements for Cryptographic Modules, FIPS 140-3, March 22, 2019. https://csrc.nist.gov/pubs/fips/140-3/final
FIPS 201-3	Personal Identity Verification (PIV) of Federal Employees and Contractors, FIPS 201-3, January 2022. https://csrc.nist.gov/pubs/fips/201-3/final
ITMRA	40 U.S.C. 1452, Information Technology Management Reform Act of 1996. https://govinfo.library.unt.edu/npr/library/misc/itref.html
NARA GRS	National Archives and Records Administration, General Records Schedules https://www.archives.gov/records-mgmt/grs.html
NS4009	NSTISSI 4009, National Information Systems Security Glossary, January 1999.
PACS	*Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems*, Version 2.3, The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group, December 20, 2005. https://www.idmanagement.gov/docs/pacs-tig-scepacs.pdf
PIV-I Issuers	Personal Identity Verification Interoperability for Issuers https://www.idmanagement.gov/docs/fpki-pivi-for-issuers.pdf
PIV-I Profile	X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards https://www.idmanagement.gov/docs/fpki-x509-cert-profiles-pivi.pdf
PKCS#1	Jakob Jonsson and Burt Kaliski, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, RFC 3447, February 2003. http://www.ietf.org/rfc/rfc3447.txt
PKCS#12	PKCS #12: Personal Information Exchange Syntax v1.1 July 2014. https://tools.ietf.org/html/rfc7292
RFC 2585	Internet X.509 Public Key Infrastructure: Operational Protocols: FTP and HTTP, Russel Housley and Paul Hoffman, May 1999. https://www.ietf.org/rfc/rfc2585.txt
RFC 3647	Certificate Policy and Certification Practices Framework, Chokhani and Ford, Sabett, Merrill, and Wu, November 2003. http://www.ietf.org/rfc/rfc3647.txt
RFC 4122	A Universally Unique IDentifier (UUID) URN Namespace, Paul J. Leach, Michael Mealling, and Rich Salz, July 2005. http://www.ietf.org/rfc/rfc4122.txt
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. https://www.ietf.org/rfc/rfc5280.txt
RFC 5322	Internet Message Format http://www.ietf.org/rfc/rfc5322.txt
RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP. https://tools.ietf.org/html/rfc6960
RFC 8551	Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification, J. Schaad, B. Ramsdell, S. Turner, April 2019. https://tools.ietf.org/rfc/rfc8551.txt

Number	Title
SP 800-37	Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, NIST Special Publication 800-37, Revision 2, December2018. https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
SP 800-56A	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, NIST Special Publication 800-56A https://csrc.nist.gov/publications/detail/sp/800-56a/rev-3/final
SP 800-57	Recommendation for Key Management: Part 1- General, NIST Special Publication 800-57 Part 1 Revision 5, May 2020 https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final
SP 800-63-3	Digital Identity Guidelines https://csrc.nist.gov/publications/detail/sp/800-63/3/final
SP 800-76-2	Biometric Specifications for Personal Identity Verification, NIST Special Publication 800-76-2, July 2013. https://csrc.nist.gov/publications/detail/sp/800-76/2/final
SP 800-78-5	Cryptographic Algorithms and Key Sizes for Personal Identity Verification, NIST Special Publication 800-78-5, July 2024. https://csrc.nist.gov/pubs/sp/800/78/5/final
SP 800-79-2	Guidelines for the Accreditation of Personal Identity Verification Card Issuers, NIST Special Publication 800-79 https://csrc.nist.gov/publications/detail/sp/800-79/2/final
SP 800-89	Recommendation for Obtaining Assurances for Digital Signature Applications, NIST Special Publication 800-89 https://csrc.nist.gov/publications/detail/sp/800-89/final
SP 800-157	Guidelines for Derived Personal Identity Verification (PIV) Credentials, NIST Special Publication 800-157. https://csrc.nist.gov/publications/detail/sp/800-157/final
X.509	ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

14 ACRONYMS AND ABBREVIATIONS

AES	Advanced Encryption Standard
AID	Application Identifier
APL	Approved Products List
ARA	Automated Registration Authority
BSM	Basic Security Module
CA	Certification Authority
CAA	Certificate Authority Administrator
CDR	Recordable CDROM
CDROM	Compact Disk, Read Only Memory
CM	Configuration Management
CMA	Certificate Management Authority
CMS	Card Management System
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CPU	Central Processing Unit
CRL	Certificate Revocation List
CRLDP	Certificate Revocation List Distribution Point
CSS	Certificate Status Services (OCSP Responder)
CSAA	Code Signing Attribute Authority
CSOR	Computer Security Objects Registry
CSP	Cryptographic Service Provider
DES	Data Encryption Standard
DN	Distinguished Name
DoD	Department of Defense
DRP	Disaster Recovery Plan
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
EAL	Evaluation Assurance Level
ECA	External Certification Authority
EE	End Entity
FPKIPA	Federal Public Key Infrastructure Policy Authority
FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standard
FPKI	(US) Federal Public Key Infrastructure
FTP	File Transfer Protocol
FQDN	Fully Qualified Domain Name
GSA	General Services Administration
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer
I&A	Identification and Authentication
ID	Identity (also, a credential asserting an identity)
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standards
IT	Information Technology
JAG	Judge Advocate General

KEA	Key Exchange Algorithm
KED	Key Escrow Database
KRA	Key Recovery Authority
KRP	Key Recovery Policy
KRPS	Key Recovery Practices Statement
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol over Secure Sockets Layer
LRA	Local Registration Authority
MCS	Mobile Code Signing
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OCSP	Online Certificate Status Protocol
OID	Object Identifier
ORC	Operational Research Consultants, Inc.
OU	Organizational Unit
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification Interoperable
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
POC	Point of Contact
POP	Proof of Possession
QUIC	Quantum Information and Computation
RA	Registration Authority
RAID	Redundant Array of Inexpensive Disks
RD	Road
RDN	Relative Distinguished Name
RFC	Request For Comment
RSA	Rivest, Shamir, Adleman (encryption and digital signature algorithm)
SA	Systems Administrator
SBU	Sensitive But Unclassified
S/MIME	Secure Multipurpose Internet Mail Extensions
SNOC	Secure Network Operations Center
SCVP	Simple Certificate Validation Protocol
SDN	Secure Data Network
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer
TA	Trusted Agent
TCSEC	Trusted Computer System Evaluation Criteria
TLS	Transport Layer Security
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
US	United States
USC	United States Code
USD	United States Dollar
UUID	Universally Unique Identifier
WWW	World Wide Web

15 GLOSSARY

The primary source is NSTISSI 4009, National Information Systems Security Glossary; other sources were used if NSTISSI 4009 had no entry for the term, or if another source gave a definition more appropriate to PKI. If no reference is given, the definition is ad hoc.

access	Ability to make use of any information system (IS) resource. [NS4009]
access control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]
accreditation	Formal declaration by a Designated Approving Authority that an IS is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
affiliated organization	An organization that has a relationship with a subscriber and sponsors that subscriber for obtaining a certificate. Affiliated Organizations are responsible for verifying the affiliation at the time of certificate application and requesting revocation of the certificate if the affiliation is no longer valid
archive	Long-term, physically separate storage.
Attribute Authority	An entity, recognized by a CMA, as having the authority to verify the association of attributes to an identity.
audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]
audit data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
binding	Process of associating two related elements of information. [NS4009]
biometric	A physical or behavioral characteristic of a person.
CA facility	The collection of equipment, personnel, procedures, and structures that are used by a Certification Authority to perform certificate issuance and revocation.
certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.
Certificate Status Services	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness and may also provide additional attribute information for the subject certificate.
certificate-related information	Information, such as a Subscriber's postal address, which is not included in a certificate, but that may be used by a CA in certificate management.
Certification Authority (CA)	An authority trusted by one or more users to create and assign certificates. [ISO9594-8]
client (application)	A system entity, usually a computer process acting on behalf of a human user, which makes use of a service provided by a server.
compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]

confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
cryptographic module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]
cryptoperiod	Time span during which each key setting remains in effect. [NS4009]
diversified key	A unique key for each card that is generated using the Master Key and the card identifying elements
dual use certificate	A certificate that is intended for use with both digital signature and data encryption services.
e-commerce	The use of network technology (especially the Internet) to buy or sell goods and services
encryption certificate	A certificate containing a public key that is used to encrypt or decrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes. The process of storing protecting and escrowing the private component of the key pair associated with the encryption certificate is sometimes referred to as key management.
External Policy Management Authority (FPKIPA)	Authority that oversees the creation and update of Certificate Policies, reviews Certification Practice Statements, reviews the results of CA audits for policy compliance, evaluates non-domain policies for acceptance within the domain, and generally oversees and manages the PKI certificate policies.
firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
Group/Role Manager	A person who is responsible for managing the Group/Role, including assigning individuals to the Group/Role membership, and maintaining the list of Group/Role members and public key certificates issued to them.
identity certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
inside threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
integrity	Protection against unauthorized modification or destruction of information. [NS4009]
intellectual property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
intermediate CA	A CA that is subordinate to another CA and has a CA subordinate to itself.
key escrow	The retention of the private component of the key pair associated with a Subscriber's encryption certificate to support key recovery.
key exchange	The process of exchanging public keys (and other information) in order to establish secure communication.
key generation material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
master key	The key required to unlock the Open Platform Key and allow changes to the contents of the card. Each card is shipped with a Manufacturer Master Key, which may optionally be changed for a Client Master Key as part of the card initialization step.
naming authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
non-repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009]
OCSP Responder	A trusted entity that provides on-line revocation status of certificates to Relying Parties. The OCSP Responder is either explicitly trusted by the Relying Party, or through the CA that issued the certificate whose revocation status is being sought.
outside threat	An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.

PKI Sponsor	An individual who represents a device or group in all certificate life-cycle activities. A PKI Sponsor asserts that the certificate and associated private key are being used in accordance with the subscriber and certificate specific obligations in this CP.
privacy	State in which data and system access is restricted to the intended user community and target recipient(s).
Public Key Infrastructure (PKI)	Framework established to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	Entity responsible for identification and authentication of certificate subjects that has automated equipment for the communication of Subscriber data to Certification Authorities and does not sign or directly revoke certificates.
re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application.
Relying Party	A person who has received a certificate and a digital signature verifiable with reference to a public key listed in the certificate and is in a position to rely on them. [ABADSG]
Remote Workstation	In the context of FPKI, “remote workstation” refers to a system used to access either the system hosting the CA or the CA itself through a network or networks that are not dedicated to the maintenance and administration of the CA.. Note: Reference Sections 5.1, 6.5, 6.6.1, and 6.7 for additional technical controls required of remote workstations. This term does not refer to consoles within the CA’s security perimeter or to Registration Authority workstations.
renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
repository	A trustworthy system for storing and retrieving certificates or other information relevant to certificates. [ABADSG]
risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
risk tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
server	A system entity that provides a service in response to requests from clients.
subordinate CA	In a hierarchical PKI, a CA whose certificate signing key is certified by another CA, and whose activities are constrained by that other CA. (see superior CA)
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to such an entity, and (2) holds a private key that corresponds to a public key listed in that certificate. [ABADSG]. Current Subscribers possess valid ECA-issued certificates.
superior CA	In a hierarchical PKI, a CA who has certified the certificate signing key of another CA, and who constrains the activities of that CA. (see subordinate CA)
system equipment configuration	A comprehensive accounting of all system hardware and software types and settings.
technical non-repudiation	The contribution public key mechanisms make to the provision of technical evidence supporting a non-repudiation security service.
threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
trust list	Collection of Trusted Certificates used by Relying Parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of a Certificate Management Authority in providing Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.

Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure, authenticated delivery. The public keys included in Trusted Certificates are used to start certification paths. Also known as a "trust anchor".
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
two person control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements. [NS4009]
update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS140]