WIDEPOINT

NON-FEDERAL ISSUER SHARED SERVICE PROVIDER

CERTIFICATION PRACTICE STATEMENT SUMMARY

[WP-NC-NFISSP-CPS]

Version 3.5

June 12, 2024

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: 2026.06.05 12:52:46 -04'00'

Luther Deyo, WidePoint Vice President ICAM

Godfrey.Caroline.R.ORC3020019041.ID

Digitally signed by Godfrey.Caroline.R.ORC3020019041.ID
Date: 2026.06.05 13:22:10 -04'00'

Caroline Godfrey, WidePoint Chief Security Officer

Webb.Richard.David.ORC30200000752.ID

Digitally signed by Webb.Richard.David.ORC30200000752.ID
Date: 2026.06.04 12:24:30 -04'00'

Richard Webb, WidePoint Corporate Security Auditor

DOCUMENT REVISION HISTORY

Date	Version	Description of Change
2011-03-11	0.1	Initial version established to support cross-certification with FBCA as an NFI
2011-05-02		Edits to comply with WidePoint NFI CP.
2011-05-05		Edits to comply with WidePoint NFI CP.
2011-06-10	1.0	Edits resulting from Triennial Phase 1 audit.
2011-10-17	1.1	Updates resulting from operational updates and completion of Triennial Phase 1 audit.
2013-06-12	1.2	Updates corresponding to changes to CP.
2014-03-20	1.3	Review and updates to Section 5.1.2 procedures to include access for authorized WidePoint personnel and contractors; Update to OIDs; Updates resulting from 2013 audit.
2015-07-15	1.3.1	Annual review and update
2015-08-14	1.3.2	Formatting update
2015-11-23	1.3.3	Edits to Section 3.2.3.2 removing unneeded sub-heading; adding clarifying text.
2016-02-04	1.3.4	Add corporate name change from ORC to WidePoint Cybersecurity Solutions Corporation; addition of Cert-on-device capabilities
2016-04-28	1.3.5	Add “Notice” to clarify corporate name change and its implication.
2016-07-21	1.3.7	Certificate policy description update
2018-08-29	1.3.8	Annual review and update
2019-03-15	1.3.10	Update to address FBCA CP change requests Annual review and update
2019-04-11	1.3.11	Key Recovery Practices
2024-06-12	3.5	Full rewrite to bring in line with other CPSs, the WidePoint NFI SSP CP v3.5 and the FBCA CP v3.5 dated May 8, 2024. Reset version number to track with FBCA CP.

TABLE OF CONTENTS

1 INTRODUCTION

This document, the WidePoint Non-Federal Issuer Shared Service Provider Certification Practice Statement, hereafter referred to as the WidePoint NFI SSP CPS, defines and describes the operations of the WidePoint Non-Federal Issuer Shared Service Provider, hereafter referred to as the WidePoint NFI SSP. The WidePoint NFI SSP is cross certified by the Federal Bridge Certificate Policy Certification Authority operated by the Federal PKI Management Authority, hereafter referred to as the Federal Bridge Certificate Policy CA, to support the issuance of federally approved digital certificates. This WidePoint NFI SSP CPS governs the operation of the WidePoint NFI 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 NFI SSP for the purposes of requesting, receiving, using, and revoking digital certificates issued by the WidePoint NFI SSP to end-entities.

This WidePoint NFI 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 NFI SSP. This WidePoint NFI SSP CPS also advises of the policies, practices, and procedures that the WidePoint NFI SSP follows for requesting, issuing, validating, and revoking certificates issued by the WidePoint NFI SSP.

This WidePoint NFI SSP CPS is written to conform to the requirements and format of the WidePoint NFI SSP Certificate Policy version 3.5, dated June 12, 2024, hereafter referred to as WidePoint NFI SSP CP, which in turn is based on the X.509 Certificate Policy for the Federal Bridge Certification Authority Version 3.5, dated May 8, 2024, hereafter referred to as Federal Bridge Certificate Policy. In the event of any policy discrepancies between Federal Bridge Certificate Policy, the WidePoint NFI SSP CP, or this WidePoint NFI SSP CPS, the Federal Bridge Certificate Policy takes precedence.

Digital certificates issued under this WidePoint NFI SSP CPS identify the entity named in the certificate and bind that entity to a particular public/private key pair. This WidePoint NFI SSP CPS addresses requirements defined in the Federal Bridge Certificate Policy CP for the issuance of digital certificates to Subscribers of the WidePoint NFI SSP. Subscribers of the WidePoint NFI 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 NFI 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 NFI 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 NFI SSP implements the security and privacy controls as required by the Federal Bridge Certificate Policy CP. Additionally, the WidePoint NFI SSP operates in accordance with a baseline equivalent to 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 NFI 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-I credential issuance systems.
- Privilege and authorization management; and
- System management functions (e.g., security audit, configuration management, archive, etc.).

The WidePoint NFI 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 NFI 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 Federal Bridge Certificate Policy and this WidePoint NFI SSP CPS are further described in Section 1.4.1.1 of both documents.

Certificate – This term is used in this WidePoint NFI 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 NFI 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 NFI 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 NFI 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 NFI SSP CPS.

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

1.1 OVERVIEW

The WidePoint NFI SSP issues X.509 version 3 digital certificates in accordance with assurance levels as defined in Federal Bridge Certificate Policy. The practices and procedures in this WidePoint NFI 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 NFI SSP has been established as a cross certified certification authority with the Federal Bridge Certification Authority.

This WidePoint NFI SSP CPS describes the operations and processes for the services that the WidePoint NFI 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 NFI SSP Certification Practice Statement is subordinate to the WidePoint NFI SSP Certificate Policy which is cross-certified with the X.509 Certificate Policy for the U.S. Federal PKI Federal Bridge Certificate Policy, Version 3.5 dated May 8, 2024 and is not subordinate to any other Certificate Policy.

Certificates issued by the WidePoint NFI SSP Certificate Authorities 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 NFI SSP certificates issued under this WidePoint NFI SSP CPS, which are available to all Relying Parties. Each WidePoint NFI SSP certificate issued asserts the appropriate level of assurance in the certificatePolicies extension.

1.1.2 RELATIONSHIP BETWEEN THE FEDERAL BRIDGE CERTIFICATION AUTHORITY CP , THE WIDEPOINT NFI SSP CP AND THIS WIDEPOINT NFI SSP CPS

This WidePoint NFI SSP CPS is subordinate to the WidePoint NFI SSP Certificate Policy, Version 3.5 dated June 12, 2024. The FPCPF states what assurance can be placed in a certificate issued by the WidePoint NFI SSP CAs. This WidePoint NFI SSP CPS states how the WidePoint NFI SSP CA(s) establishes that assurance. The policies and procedures in this WidePoint NFI 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

The WidePoint NFI SSP exists to facilitate trusted electronic business transactions for State and Local Governments, and non-Federal organizations, individuals and devices. This WidePoint NFI SSP Certification Practice Statement describes the following:

- Roles, responsibilities, and relationships among the CAs, Registration Authorities (RAs), Certificate Manufacturing Authorities (CMAs), Repositories, Subscribers, Relying Parties, and the Policy Authority (PA) (referred to collectively herein as “Program Participants”) authorized to participate in the PKI described by the WidePoint NFI SSP Certificate Policy and the WidePoint NFI SSP Certification Practice Statement
- The primary obligations and operational responsibilities of the Program Participants
- The rules and requirements for the issuance, acquisition, management, and use of WidePoint NFI SSP certificates to verify digital signatures

This WidePoint NFI SSP Certificate Practice Statement provides a high level description of the policies and operation of the WidePoint NFI SSP. Specific detailed requirements for the services outlined in this document may be found in each WidePoint NFI CA's Cert

1.1.4 Interoperation with the WidePoint NFI SSP and Certificate Authorities Issuing under Different Policies

The WidePoint NFI SSP is cross-certified with the Federal Bridge Certification Authority and has a policy mapping as described in Section 1.2 below. The WidePoint NFI SSP may also cross-certified and signed subordinate Certificate Authority certificates and in turn map the Subordinate certificate policies to the WidePoint NFI SSP certificate policies identified in Section 1.2.

1.2 Document Name and Identification

The WidePoint NFI SSP operates in a manner consistent with the practices established in Federal Bridge Certificate Policy. Federal Bridge Certificate 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 Federal Bridge Certificate Policy Framework and is written and maintained by the Federal PKI Policy Authority as described in Section 1.3.1 of this WidePoint NFI SSP CPS. Whenever this is the intended use, this WidePoint NFI SSP CPS shall refer to the Certificate Policy as Federal Bridge Certificate 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 NFI 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 Federal Bridge Certificate Policy certificate policy name, the certificate policy OIDs that may be asserted in digital certificates created by the WidePoint NFI SSP, and the Level of Assurance as defined in Section 1.4.1.4 of this WidePoint NFI SSP CPS that each one represents:

WP Certificate Policy Name	WP NFI SSP Certificate Policy Oid	FBCA Certificate Policy Oid	LOA
id-orc-nfissp-ca	1.3.6.1.4.1.3922.1.1.1.100		
id-orc-nfissp-medium	1.3.6.1.4.1.3922.1.1.1.3	2.16.840.1.101.3.2.1.3.3	Med
id-orc-nfissp-mediumHardware	1.3.6.1.4.1.3922.1.1.1.12	2.16.840.1.101.3.2.1.3.12	MHW
id-orc-nfissp-pivi-hardware	1.3.6.1.4.1.3922.1.1.1.18	2.16.840.1.101.3.2.1.3.18	PIVI-HW
id-orc-nfissp-pivi-cardAuth	1.3.6.1.4.1.3922.1.1.1.19	2.16.840.1.101.3.2.1.3.19	CA-PIVI
id-orc-nfissp-pivi-contentSigning	1.3.6.1.4.1.3922.1.1.1.20	2.16.840.1.101.3.2.1.3.20	CS-PIVI
id-orc-nfissp-mediumDevice	1.3.6.1.4.1.3922.1.1.1.37	2.16.840.1.101.3.2.1.3.37	Med
id-orc-nfissp-mediumDeviceHardware	1.3.6.1.4.1.3922.1.1.1.38	2.16.840.1.101.3.2.1.3.38	Med HW

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

The WidePoint NFI SSP supports all certificate policies defined in the table above. The WidePoint NFI SSP CPS supports all of the OIDs defined in Federal Bridge Certificate Policy, listed above.

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

Certificates Valid for Human Subscribers	WP Certificate Policy Name
PIV-I Authentication certificate	id-orc-nfissp-pivi-hardware
Digital Signature certificate with the private key generated on a PIV-I credential	id-orc-nfissp-mediumHardware
Key Management certificate associated with a PIV-I credential	id-orc-nfissp-medium
All other hardware-based certificates	id-orc-nfissp-pivi-hardware
All software-based certificates	id-orc-nfissp-medium

The requirements associated with id-orc-nfissp-pivi-hardware are identical to id-orc-nfissp-mediumHardware except where specifically noted in the text and further described in Appendix A.

The requirements associated with the id-orc-nfissp-mediumHardware policy are identical to those defined for the id-orc-nfissp-medium policy except for subscriber cryptographic module requirements (see Section 6.2.1).

1.3 PKI PARTICIPANTS

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

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

WidePoint NFI SSP Certificate Status Services, hereafter referred to as WidePoint NFI SSP CSA(s) that provide Online Certificate Status Protocol (OCSP) and Server-based Certificate Validation Protocol (SCVP) status responses are operated by the WidePoint NFI SSP and are also considered a part of a WidePoint NFI SSP CMA. All WidePoint NFI SSP CMA(s) are operated in compliance with this WidePoint NFI SSP CPS and Federal Bridge Certificate 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 Federal Bridge Certificate Policy,
- Approving the WidePoint NFI SSP CP that aligns with the Federal Bridge Certificate Policy,
- Approving the compliance audit report for the WidePoint NFI SSP issuing certificates cross-certified with Federal Bridge Certificate Policy, and
- Ensuring continued conformance of WidePoint NFI SSP that issues certificates cross-certified with Federal Bridge Certificate Policy with applicable requirements as a condition for allowing continued participation.

1.3.2 WIDEPOINT NFI SSP POLICY MANAGEMENT AUTHORITY (WIDEPOINT NFI SSP PMA)

The WidePoint NFI SSP Policy Management Authority, hereafter referred to as the WidePoint NFI SSP PMA, is comprised of WidePoint Executives and Trusted personnel who oversee the operations and compliance of the WidePoint NFI SSP with the policies inherited from the FPKIPA and the Federal Bridge Certificate Policy.

The WidePoint NFI SSP PMA is responsible for:

- Maintaining the WidePoint NFI SSP Certificate Policy,
- Approving this WidePoint NFI SSP CPS that issues certificates in a manner consistent with the WidePoint NFI SSP CP,
- Approving the compliance audit report for the WidePoint NFI SSP,

- Approving Organization Certification Practice Statements and Organization Registration Practices Statements that derived from the WidePoint NFI SSP CP or the WidePoint NFI SSP CPS respectively, and,
- Ensuring continued conformance of WidePoint NFI SSP that issues certificates cross-certified with Federal Bridge Certificate Policy with applicable requirements as a condition for allowing continued participation.

1.3.3 WIDEPOINT CERTIFICATION AUTHORITIES

The WidePoint NFI SSP is issued a cross-certificate by the Federal Bridge Certificate Policy CA for each WidePoint NFI SSP issue certificate authority. Each WidePoint NFI 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 NFI SSP security boundary. Each WidePoint NFI SSP CA generates certificates in accordance with this WidePoint NFI SSP CPS and in compliance with the certificate profiles described in Section 10. Each WidePoint NFI 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 NFI SSP CPS. Each WidePoint NFI 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 NFI SSP Certificate Authority signing keys
- Ensuring that all aspects of the WidePoint NFI SSP Certificate Authority services, operations, and infrastructure related to certificates issued under this WidePoint NFI SSP CPS are performed in accordance with the requirements, representations, and warranties of this WidePoint NFI SSP CPS.

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

Each WidePoint NFI 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 NFI SSP CA throughout its lifecycle.

1.3.4 WIDEPOINT NFI SSP CARD MANAGEMENT SYSTEMS

Each WidePoint NFI SSP Card Management System, hereafter referred to as a WidePoint NFI SSP CMS, is authorized by the WidePoint NFI SSP to process, issue, and revoke WidePoint NFI SSP PIV-I credentials, which contain printed card elements, certificates asserting a certificate policy of **id-orc-nfissp-pivi-hardware**, **id-orc-nfissp-pivi-cardAuth**, **id-orc-nfissp-mediumHardware, or id-orc-nfissp-medium** and their private keys including previous encryption keys, and other data objects including digitally signed biometrics in accordance with the FBCA CP, the WidePoint NFI SSP CP, and the WidePoint NFI 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 NFI SSP CMS is authorized by the WidePoint NFI SSP through the issuance of a content signing certificate that asserts a certificate policy of **id-orc-nfissp-pivi-contentsigning** by a WidePoint NFI SSP CA. Each WidePoint NFI SSP CMS's content signing certificate is used by the WidePoint NFI SSP CMS to digitally sign data elements on WidePoint NFI SSP PIV-I credentials. Each WidePoint NFI SSP CMS is also issued a connector certificate with assigned privileges on the corresponding WidePoint NFI SSP CA for requesting certificate issuance and revocation. Each WidePoint NFI SSP CMS is considered a WidePoint NFI SSP Registration Authority and adheres to all the requirements specified for WidePoint NFI SSP Registration Authorities in this WidePoint NFI SSP CPS. Additionally, privileged users of a WidePoint NFI SSP CMS who can direct the WidePoint NFI SSP CMS to perform certificate related actions are considered to be WidePoint NFI SSP Registration Authorities, as described in Section 1.3.4 of this WidePoint NFI SSP CPS.

1.3.5 WIDEPOINT REGISTRATION AUTHORITIES

WidePoint Registration Authorities are entities that enter into an agreement with the WidePoint NFI SSP for the purpose of collecting and submitting digitally signed verification of Applicant and WidePoint NFI 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 NFI SSP CPS which is approved by the WidePoint NFI SSP and the FPKIPA. WidePoint Registration Authorities register Applicants and WidePoint NFI 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 NFI 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 NFI SSP CPS;
- WidePoint Registrars perform the registration process associated with WidePoint NFI SSP PIV-I credentials and approve Applicants and WidePoint NFI SSP Subscribers credential requests for issuance of a WidePoint NFI SSP PIV-I credential to an Applicant or WidePoint NFI SSP Subscriber;
- WidePoint Issuers reaffirm the identity of the WidePoint NFI SSP Subscriber who has been approved for issuance of a WidePoint NFI SSP PIV-I credential by a WidePoint Registrar and authorize and witness the key generation of the WidePoint NFI SSP PIV-I credential to the WidePoint NFI SSP Subscriber; and
- WidePoint Key Recovery Agents recover escrowed keys in accordance with the stipulations of this WidePoint NFI 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 NFI 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 NFI 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 NFI SSP Subscribers or third-party requestors and forward those requests to WidePoint Registration Authorities.

Trusted Agents are individuals who act on behalf of WidePoint Registration Authorities in performing identity verification and authorization verification tasks on Applicants and WidePoint NFI SSP Subscribers to the WidePoint NFI SSP. A Trusted Agent is a person authorized to act as a representative of the WidePoint NFI SSP in providing Applicant or WidePoint NFI 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 NFI SSP CAs or any WidePoint NFI SSP CMA system or function. Trusted Agents are further defined by the categories below in this section.

1.3.6 WIDEPOINT CERTIFICATE STATUS SERVERS

WidePoint NFI SSP Certificate Status Services, hereafter referred to as WidePoint NFI SSP CSS(s), provide Online Certificate Status Protocol (OCSP) and Server-based Certificate Validation Protocol (SCVP) status responses. The WidePoint NFI SSP CSS(s) are operated by the WidePoint NFI SSP and are also considered a part of a WidePoint NFI SSP CMA. All WidePoint NFI SSP CMA(s) are operated in compliance with this WidePoint NFI SSP CPS, the WidePoint NFI SSP CP, and the Federal Bridge Certification Authority Certificate Policy. Every issued by the WidePoint NFI SSP is encoded with the location of the WidePoint NFI SSP CSS in the Authority Information Access (AIA) extension in accordance with RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

1.3.7 KEY RECOVERY AUTHORITIES

The WidePoint NFI 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 NFI SSP Certificate Authority requirements are applied to all WidePoint Key Escrow Databases and to all WidePoint NFI 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
- WidePoint Registration Authority requirements are applied to the KRO and WidePoint Key Recovery Official automated systems, when the WidePoint Key Recovery Official has privileged access to all WidePoint Key Escrow Databases.

1.3.7.1 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.

1.3.7.2 Data Decryption Server

A WidePoint NFI SSP Data Decryption Server is an automated system that has the capability to obtain subscriber private keys from the WidePoint NFI SSP Key Escrow Database or another WidePoint NFI SSP Data Decryption Server for data monitoring or other purposes (e.g., email inspection). WidePoint NFI SSP Data Decryption Servers do not provide keys to WidePoint NFI SSP Subscribers or other Third-Party Requestors. A WidePoint NFI 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 NFI SSP Data Decryption Server is optional based on customer organization requirements. As of this publication of the WidePoint NFI SSP CPS, no WidePoint NFI SSP Data Decryption Server is operated by the WidePoint NFI SSP or any of WidePoint's customer organizations.

1.3.7.3 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 NFI SSP Key Escrow Database in order to extract an escrowed decryption private key. WidePoint Key Recovery Agents send the recovered key to the Requestor. WidePoint Key Recovery Agents have high-level sensitive access to the WidePoint NFI SSP Key Escrow Database and are considered Trusted Roles (see Section 5.2.1). WidePoint NFI SSP Registration Authorities as defined in this WidePoint NFI SSP CPS may fill the role of WidePoint NFI SSP Key Recovery Agent; however, because WidePoint NFI SSP Key Recovery Agents can recover large number of keys, the number and location of WidePoint NFI SSP Key Recovery Agents are tightly controlled without limiting the ability to recover or operate. The WidePoint NFI SSP may allow WidePoint NFI SSP Subscriber organizations to designate non-WidePoint employees to fulfill the role of WidePoint NFI SSP Key Recovery Agent with the stipulation that those WidePoint Key Recovery Agents may recover keys of WidePoint NFI SSP Subscribers only from the Organization/Enterprise by which that Key Recovery Agent is employed.

1.3.7.4 WidePoint Key Recovery Official

A WidePoint Key Recovery Official may optionally be used to support identity verification and authorization validation tasks. WidePoint Key Recovery Official does not have privileged access to the WidePoint NFI SSP Key Escrow Database.

1.3.8 KEY RECOVERY REQUESTORS

A Requestor is the person who requests the recovery of decryption private key(s). A Requestor is generally the WidePoint NFI SSP Subscriber, a third-party from the WidePoint NFI SSP Subscriber's organization (e.g., supervisor, corporate officer) or a law enforcement officer who is authorized to request recovery of a WidePoint NFI SSP Subscriber's escrowed key. Any individual who can demonstrate a reasonably verifiable authority in accordance with the WidePoint NFI SSP Subscriber's organization information access and release policy and need to obtain a recovered key can be considered a Requestor.

1.3.8.1 Internal Third-Party Requestor

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

1.3.8.2 External Third-Party Requestor

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

1.3.9 WIDEPOINT NFI SSP SUBSCRIBERS

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

- Non-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 the organizations.

There is a subset of Human WidePoint NFI SSP Subscribers who will be issued role-based certificates. These certificates identify a specific role on behalf of which the WidePoint NFI SSP Subscriber is authorized to act rather than the WidePoint NFI 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, it will be issued in addition to an individual WidePoint NFI SSP Subscriber certificate. A specific role may be identified in certificates issued to multiple WidePoint NFI SSP Subscribers; however, the key pair will be unique to each individual role-based certificate. For example, there may be four individuals with a certificate issued in the role of "Board of Directors." However, each of the four certificates will have unique keys and certificate serial numbers. Roles for which role-based certificates may be issued are limited to those that are held by a unique individual within an organization (e.g., Chief Information Officer is a unique individual whereas Program Analyst is not).

Practice Note: When determining whether a role-based certificate is authorized, consider whether the role carries inherent authority beyond the job title. Role-based certificates may also be used for individuals on temporary assignment, where the temporary assignment carries an authority not shared by the individuals in their usual occupation, for example: "Watch Commander, Task Force 1".

1.3.10 AFFILIATED ORGANIZATIONS

WidePoint NFI SSP Subscriber certificates may be issued on behalf of an organization, other than the organization operating the Entity PKI, that has a relationship with the Applicant or Subscriber; this is termed affiliation. The organizational affiliation is indicated in the certificate. The Affiliated Organization is responsible for verifying the affiliation at the time of certificate application and requesting revocation of the certificate if the affiliation is no longer valid.

1.3.11 RELYING PARTIES

A Relying Party is an entity who, by using another's WidePoint NFI 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 NFI 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.

1.3.12 Other Participants

1.3.12.1 WidePoint NFI SSP PKI Sponsor

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

1.3.12.2 Other Authorities

1.3.12.2.1 WidePoint Corporate Security Auditor

A WidePoint Corporate Security Auditors ensures that compliance audits as stipulated in this WidePoint NFI 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 NFI 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 NFI SSP CPS, including aperiodic audits. Audits of the WidePoint NFI SSP will follow the guidelines and specifications of currently accepted standards and practices, as approved by the FPKIPA.

1.3.12.2.2 External Auditor

The WidePoint NFI SSP retains a nationally recognized firm with expertise in IT Security Auditing and Evaluation as an external 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 NFI SSP is intended to support the following security services: *confidentiality, integrity, authentication,* and *technical non-repudiation*. The WidePoint NFI 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 NFI SSP Subscribers and Relying Parties. The WidePoint NFI 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 NFI 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 NFI 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 NFI SSP offers various digital certificate types (i.e., certificates that perform a specific function) to promote these security services. The WidePoint NFI SSP issues certificates to WidePoint NFI SSP Subscribers that assert one of the certificate policy object identifiers specified in Section 1.2 of this WidePoint NFI 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 NFI SSP CPS, which is required. The WidePoint NFI SSP issues the following certificate types:

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

Signature Certificates *– This certificate type, sometimes referred to as an identity certificate, is issued to a WidePoint NFI SSP Subscriber as a means for the WidePoint NFI SSP Subscriber to identify themselves electronically to applications and other people. The Identity Certificate type uniquely identifies the WidePoint NFI SSP Subscriber and allows for the WidePoint NFI 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 NFI SSP Subscriber.*

Encryption Certificates *– This certificate type is issued to a WidePoint NFI SSP Subscriber as a means for the WidePoint NFI 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 NFI SSP Subscriber whenever they receive a signature certificate. Encryption certificates are escrowed as part of the issuance process of the WidePoint NFI SSP to facilitate self-recovery and third-party recovery and may only assert the certificate policy object identifier of* ***id-orc-nfissp-medium****. Encryption certificates do not assert the key-usage of non-repudiation.*

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 NFI SSP CSS, as described in Section 1.3 of this WidePoint NFI 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 NFI SSP. An OCSP Signing Certificate identifies the name of the WidePoint NFI 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 NFI SSP CA that signed it.*

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

PIV-I Authentication Certificates – *This certificate type identifies the WidePoint NFI SSP or Organization Subscriber to whom a WidePoint NFI SSP or Organization PIV-I credential was issued and can only be issued to and whose private key can only exist within a WidePoint NFI SSP or Organization PIV-I Credential. This certificate ties the WidePoint NFI SSP or Organization Subscriber to the physical card that constitutes the physical aspect of the WidePoint NFI SSP or Organization 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 NFI SSP PIV-I Credential and uniquely identifies the FIPS 201-3 compliant card that holds the WidePoint NFI SSP issued card authentication certificate. This certificate type does not contain any Personally Identifiable Information (PII) data about the WidePoint NFI SSP Subscriber to whom the WidePoint NFI SSP 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 NFI SSP CMS, as described in Section 1.3.3 of this WidePoint NFI SSP CPS, to sign the data elements (i.e. the content) that is captured during the issuance process for a WidePoint NFI SSP PIV-I Credential and that will be stored on the credential. This certificate type identifies the name of the WidePoint NFI SSP CMS that controls the issuance process for WidePoint NFI SSP PIV-I credentials. This certificate has a key usage of digital signature and is only used to sign the data elements on the WidePoint NFI 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 NFI 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 NFI 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 NFI SSP Subscribers as part of the WidePoint NFI SSP program. The credential types described may or may not have a direct correlation to Federal Bridge Certificate Policy but are used to define a package that contains elements that do have a direct correlation. Additionally, an Applicant or a WidePoint NFI 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 NFI SSP credential. The credential types that the WidePoint NFI 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-orc-nfissp-mediumHardware** and an encryption certificate that asserts a certificate policy of **id-orc-nfissp-medium**. 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 NFI SSP CPS.*

***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-orc-nfissp-pivi-cardAuth**, an authentication certificate that asserts the certificate policy of **id-orc-nfissp-pivi-hardware**, an identity certificate that asserts the certificate policy of **id-orc-nfissp-mediumHardware** and an encryption certificate that asserts a certificate policy of **id-orc-nfissp-medium**. WidePoint NFI SSP PIV-I Credentials may only be issued through the WidePoint NFI 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 NFI 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 NFI SSP PIV-I Credential holder. The biometric data is signed by a WidePoint NFI 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 NFI SSP Subscriber. Additional features of the WidePoint NFI 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 NFI SSP Subscriber as part of a previous WidePoint NFI SSP PIV-I Credential issuance are also recovered to the new*

WidePoint NFI SSP PIV-I Credential for decrypting previously encrypted information by the WidePoint NFI SSP Subscriber.

Elevated Privileges Credential – *This credential is a companion credential to a WidePoint NFI SSP Subscriber who holds an existing WidePoint NFI 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-orc-nfissp-mediumHardware****. This is typically for Systems Administrators or other personnel who have privileged rights on a system or systems. When a WidePoint NFI 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 NFI 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 Federal Bridge Certificate 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 NFI SSP of the degree of confidence that a Relying Party may reasonably place in the binding of a WidePoint NFI SSP Subscriber's public key to the identity and privileges asserted in the certificate. Assurance level depends on the proper registration of WidePoint NFI SSP Subscribers and the proper generation and management of the certificate and associated private keys, in accordance with the stipulations of this WidePoint NFI SSP CPS. Personnel, physical, procedural, and technical security controls, as described in this WidePoint NFI SSP CPS, are used to maintain the assurance level of the certificates issued by the WidePoint NFI 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 NFI 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 NFI 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 Federal Bridge Certificate 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 NFI 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 NFI 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 NFI SSP can only assert the certificate policy value of **id-orc-nfissp-medium** for human WidePoint NFI SSP Subscribers and a certificate policy value of **id-orc-nfissp-mediumDevice** or **id-orc-nfissp-mediumDeviceHardware**. 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 NFI SSP Subscriber has generated their private keys in the presence of a WidePoint NFI SSP Registration Authority or WidePoint NFI 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 NFI 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 Federal Bridge Certificate Policy and the WidePoint NFI SSP. Medium Hardware Assurance certificates issued by the WidePoint NFI SSP can only assert the certificate policy value of **id-orc-nfissp-mediumHardware** and only for human WidePoint NFI 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 NFI SSP PIV-I credentials as described in Section 1.4.1.

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 NFI SSP PIV-I Credentials and their associated WidePoint NFI 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 NFI SSP PIV-I Credential. Card Authentication PIV-I Assurance certificates issued by the WidePoint NFI SSP can only assert the certificate policy value of **id-orc-nfissp-pivi-cardAuth** and may only be issued to WidePoint NFI SSP PIV-I Credentials through a WidePoint NFI 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 NFI SSP Subscriber has generated their private keys in the presence of a WidePoint NFI SSP Issue upon completion of the WidePoint NFI 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 NFI SSP can only assert the certificate policy value

of **id-orc-nfissp-pivi-hardware** and may only be issued to WidePoint NFI SSP PIV-I Credentials through a WidePoint NFI SSP CMS.

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

1.4.2 PROHIBITED CERTIFICATE USES

Certificates that assert **id-orc-nfissp-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.

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 NFI SSP CPS, in accordance with the requirements stipulated in Federal Bridge Certificate Policy.

1.5.2 CONTACT PERSON

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

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

WIDEPOINT NFI 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

WidePoint NFI SSP shall determine suitability of this WidePoint NFI SSP CPS with the WidePoint NFI SSP CP using a compliance analysis and approval process. The FPKIPA determines the suitability of the WidePoint NFI SSP CP using a compliance analysis and approval process.

FEDERAL PKI POLICY AUTHORITY

fpki@gsa.gov

1.5.4 WIDEPOINT NFI SSP CPS APPROVAL PROCEDURES

The FPKIPA will make the determination that the WidePoint NFI SSP CP complies with Federal Bridge Certificate Policy for a given level of assurance. The compliance analysis is performed by an independent party. WidePoint has met all requirements for an approved CP prior to commencing operations. This WidePoint NFI SSP CPS has been determined to be an approved CPS in compliance with the WidePoint NFI SSP CP and with Federal Bridge Certification Authority CP version 3.5 dated May 8, 2024. Registration Authority practices are documented in the WidePoint NFI SSP Registration Practices Statement, hereafter referred to as the WidePoint NFI 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 NFI SSP operates and maintains repositories in support of WidePoint NFI SSP Subscribers and Relying Parties and their use and acceptance of certificates issued by the WidePoint NFI SSP. The location of any publication is available to Subscribers and Relying Parties as stipulated in this CPS.

Information in WidePoint NFI SSP Repositories is protected in accordance with the provisions of this WidePoint NFI 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 NFI 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 NFI SSP Repository is located at https://orc.widepoint.com/certificates-and-credentials/piv-i/. The WidePoint NFI SSP maintains the repository using two separate, but identical iterations run behind a load balancer. In addition, a copy of the WidePoint NFI 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 NFI SSP CPS and described in the WidePoint System Security Plan Physical and Environmental Protection Control Family.[PE] These capabilities allow the WidePoint NFI 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 NFI SSP posts WidePoint NFI 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 NFI 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 NFI SSP at:

- http://crl-server.orc.com/caCerts/caCertsIssuedByWIDEPOINTNFIROOT<#>.p7c

All Certificate Authority certificates issued to the WidePoint NFI SSP are published to a file publicly available and encoded in the Authority Information Access (AIA) extension in all valid certificates issued by the WidePoint NFI SSP at:

- http://crl-server.orc.com/caCerts/caCertsIssuedToWIDEPOINTNFIROOT2.p7c

All WidePoint NFI SSP Certificate Authorities and Subordinate Certificate Authorities that issue certificates under this WidePoint NFI 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 NFI 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 NFI SSP posts CRLs at the following locations, accessible via HTTP:

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

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

Pre-generated OCSP responses may be created by the WidePoint NFI 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 NFI SSP CRLs.

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

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

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

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

The WidePoint NFI SSP Repository meets the following obligations:

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

The WidePoint NFI SSP maintains a copy of at least all certificates and CRLs issued by WidePoint NFI SSP CAs and provides this information for archiving. The WidePoint NFI 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 NFI SSP Repository is a publicly accessible repository that is available to subscribers and relying parties that contains:

- All WidePoint NFI SSP issued encryption certificates that assert a certificate policy listed in Section 1.2 of this WidePoint NFI SSP CPS;
- The most recently issued CRL for each WidePoint NFI SSP CA;
- All WidePoint NFI SSP CA certificates used as signing key and CRLs;
- All certificates issued to WidePoint NFI SSP CAs;
- A copy of the current Federal Bridge Certificate Policy CP, including any waivers granted to the WidePoint NFI SSP by the FPKIPA; and,
- An abridged version of this approved WidePoint NFI 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 NFI 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 Federal Bridge Certificate Policy or this WidePoint NFI SSP CPS.

The WidePoint NFI SSP Repository is located at https://orc.widepoint.com/certificates-and-credentials/piv-i/. The WidePoint NFI SSP maintains the repository using two separate, but identical iterations run behind a load balancer. In addition, a copy of the WidePoint NFI 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 NFI SSP CPS and described in the WidePoint System Security Plan Physical and Environmental Protection Control Family.[PE] These capabilities allow the WidePoint NFI SSP to maintain 99% availability of the repository overall per year and scheduled downtime not to exceed 0.5% annually.

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

- All certificates issued to WidePoint NFI SSP CAs;
- A copy of the current Federal Bridge Certificate Policy CP, including any waivers granted to the WidePoint NFI SSP by the FPKIPA;
- A copy of the WidePoint NFI SSP annual PKI Compliance Audit Letter; and,
- An abridged version of this approved WidePoint NFI 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 NFI 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 Federal Bridge Certificate Policy or this WidePoint NFI SSP CPS.

2.3 TIME OR FREQUENCY OF PUBLICATION

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

2.4 ACCESS CONTROLS ON REPOSITORIES

There are no access controls on the reading of the abridged WidePoint NFI SSP CPS summary, any supplemental policy information, or any supplemental practice information published by the WidePoint NFI 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 NFI SSP Repository is restricted only to specific trusted roles, as described in Section 5.2.1 of this WidePoint NFI SSP CPS, using certificate authenticated access control over TLS. The WidePoint NFI 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 NFI SSP systems and system components are limited to the appropriate trusted roles as described in Section 5.2.1 of this WidePoint NFI SSP CPS and protected by strong authentication methods[IA-5] as stipulated in this WidePoint NFI 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 NFI SSP personnel in trusted roles as identified in Section 5.2.1 of this WidePoint NFI 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 NFI SSP systems and system components.
- The WidePoint Corporate Security Auditor determines and periodically reviews user access rights[AC-2].
- WidePoint NFI 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 NFI SSP Repository or any public repository.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 TYPES OF NAMES

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

All WidePoint NFI SSP CA certificates cross-certified with the Federal Bridge will include a non-NULL subject DN. All certificates issued by the WidePoint NFI SSP CA(s) to end entities will include a non-NULL subject DN. WidePoint NFI SSP RAs will ensure by visual inspection on the WidePoint NFI CAs that the certificates will be issued with a non-null subject DN prior to issuance.

The table below specifies the naming requirements that apply to each level of assurance

Assurance Level	Naming Requirements
Medium (All policies)	Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical
PIV-I Card Authentication	Non-Null Subject Name, and Subject Alternative Name

3.1.1.1 Subject Names

All certificates issued by the WidePoint NFI SSP under this WidePoint NFI SSP CPS use the Distinguished Name (DN) format for subject and issuer name fields. In the case of individual certificates, the WidePoint NFI SSP assigns an X.501 distinguished name specifying a geo-political name. In the case of component/device certificates, the WidePoint NFI SSP assigns a geo-political name.

DNs consist of a combination of a Common Name (CN) and a Relative Distinguished Name (RDN). CNs are either:

- full names for individuals;
- the authenticated registered domain name of the Application server; a unique device identification naming convention (e.g., FQDN, IP address, MAC address, IMEI, etc.); or an application name depending on device type; or
- the name of the code signer's organization for code signing certificates.

The common name used represents the WidePoint NFI SSP Subscriber in a way that is easily understandable for humans. For people, this is typically a legal name. In the case of all human certificates:

- CN = Nickname Smith; or
- CN = John J Smith; or
- CN = John Jay Smith; or
- CN = Smith.John.Jay

Devices that are the subject of certificates issued by the WidePoint NFI SSP are assigned either a geo-political name or an Internet domain component name. Device names take one of the following forms:

For certificates with an Affiliated Organization:

- cn=device name, ou=Affiliated Organization Name,{Base DN}

For certificates with no Affiliated Organization where device name is a descriptive name for the device:

- cn=device name, ou=Unaffiliated, ou=Entity CA's Name, {Base DN}

Role-based and group certificates may be issued asserting **id-orc-nfissp-medium** or **id-orc-nfissp-mediumHardware** (For these certificates, the common name specifies the role, as follows:

- Role-based certificates identify a specific role on behalf of which one or more WidePoint NFI SSP Subscribers are authorized to act rather than the WidePoint NFI SSP Subscriber's name. Where the organization is implicit in the role, it may be omitted. Where the role alone is ambiguous, the organization shall be present in the DN.
- The subjectName DN in a group certificate shall not imply that the subject is a single individual, e.g., by inclusion of a human name form.

For PIV-I Card Authentication Subscriber certificates, use of the Subscriber common name is prohibited, instead a serialNumber=UUID is required. PIV-I Card Authentication certificates indicate whether or not the Subscriber is associated with an Affiliated Organization by taking one of the following forms:

For certificates with an Affiliated Organization:

- serialNumber=UUID, ou=Affiliated Organization Name, {Base DN}

For certificates with no Affiliated Organization:

- serialNumber=UUID, ou=Unaffiliated, ou=<WidePoint NFI SSP CA Name>, {Base DN}

The UUID is encoded within the serialNumber attribute using the UUID string representation defined in Section 3 of RFC 4122 (e.g., "f81d4fae-7dec-11d0-a765-00a0c91e6bf6").

Certificates asserting **id-orc-nfissp-medium, id-orc-nfissp-mediumHardware**, or **id-orc-nfissp-pivi-hardware** indicate whether or not the WidePoint NFI SSP Subscriber is associated with an Affiliated Organization by taking one of the following forms:

For certificates with an Affiliated Organization:

- cn=Subscriber's full name, ou=Affiliated Organization Name, {Base DN}

For certificates with no Affiliated Organization:

- cn=Subscriber's full name, ou=Unaffiliated, ou=<WidePoint NFI SSP CA Name>, {Base DN}

PIV-I Content Signing certificates clearly indicate the organization administering the CMS.

The {Base DN} is defined as: 'o=ORC PKI, c=US'.

The WidePoint NFI CAs may supplement any of the name forms for users specified in this section by including dnQualifier, serial number, or user id attribute. When any of these attributes are included, they may appear as part of a multi-valued relative distinguished name (RDN) with the common name or as a distinct RDN that follows the RDN containing the common name attribute.

3.1.1.2 Subject Alternative Names

WidePoint NFI SSP certificates that assert a certificate policy OID of **id-orc-nfissp-pivi-hardware** or **id-orc-nfissp-pivi-cardAuth** will include a subject alternative name extension, containing a UUID encoded as a URI as specified in Section 3 of [RFC 4122].

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

WidePoint NFI 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.

WidePoint NFI 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 organization.

- Before issuing a publicly trusted serverAuth certificate containing a wildcard, the WidePoint NFI SSP ensures the sponsoring organization 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: 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 NFI 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 NFI SSP Subscriber certificates will identify the person or object to which they are assigned.

Within the DN structure of certificates issued by the WidePoint NFI SSP to WidePoint NFI SSP Subscribers, the Common Name, hereafter referred to as CN, will represent the WidePoint NFI 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 NFI SSP CPS. Additionally, the DN will accurately reflect organizational structures within the directory information tree.

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

3.1.3 Anonymity of Pseudonymity of Subscribers

WidePoint NFI SSP Certificate Authority certificates will not contain anonymous or pseudonymous identities.

The WidePoint NFI SSP does not issue anonymous or pseudonymous certificates.

Role-based certificates may be issued by the WidePoint NFI SSP to support internal operations. WidePoint NFI 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 NFI SSP CPS.

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 NFI SSP complies with uniqueness of names; including X.500 DNs. The WidePoint NFI 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 NFI 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 NFI SSP CPS.

The WidePoint NFI SSP ensures the following for subscriber names:

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

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

Additionally, the WidePoint NFI SSP may append a Unique Identification String for a Subscriber receiving certificates from the WidePoint NFI SSP CAs. The Unique Identification String consists of a 10-digit number, prefixed by an alpha-numeric string. Figure 1 provides an example below:

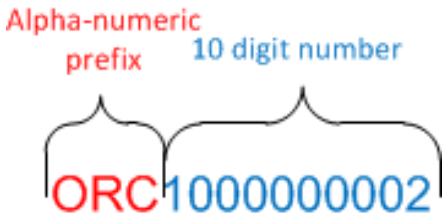

Figure 1: Example of WidePoint Unique Identifier String for Subscriber

The 10-digit number is assigned sequentially by the WidePoint NFI SSP whenever a new WidePoint NFI SSP Subscriber receives certificates from a WidePoint NFI SSP CA. WidePoint NFI SSP Subscribers with existing certificates from the WidePoint NFI SSP who have not changed name or organizational affiliation will be assigned the same 10-digit number from their previous certificates issued by the WidePoint NFI SSP, in accordance with Section 3.2.3.1 and 3.2.3.2. WidePoint NFI SSP Subscribers with existing certificates from the WidePoint NFI SSP who have changed name or organizational affiliation will be assigned the next available sequential 10-digit number. The next available sequential 10-digit number is determined by a query against the WidePoint NFI SSP certificate repository for all certificates issued to date. The alpha-numeric prefix of the Unique Identification String is assigned by the WidePoint NFI SSP.

Additionally, the WidePoint NFI SSP may append additional information to the end of the 10 digit number to identify the certificate type. This additional designation may be, but is not limited to, the following:

- .ID (for Signature Certificates)
- .encrypt (for Encryption Certificates)
- .Auth (for Authentication Certificates)

In cases where the additional information identifying certificate type is applied, the Unique Identification String will take the following form, as depicted in Figure 2:

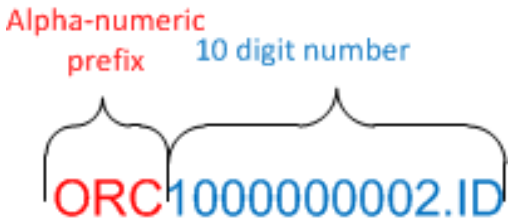

Figure 2: WidePoint Unique Identification String with Certificate Type Appended

Once the WidePoint NFI SSP Unique Identification String has been fully constructed, the Unique Identification String is appended to the CN string. The full CN string for all Subscribers will take one of the forms listed above. An example is depicted in Figure 3:

Figure 3: Full CN String for Subscribers with Appended WidePoint Unique ID String

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. Trademarks will not be used as a name form or as any part of the name form for WidePoint NFI SSP issued certificates. The WidePoint NFI SSP will not knowingly issue a certificate from the WidePoint NFI 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 NFI SSP issued certificate contains a name that has infringed the referenced ruling. The WidePoint NFI SSP will revoke the previous issued certificates in accordance with Section 4.9.1 of this WidePoint NFI SSP CPS. WidePoint NFI SSP Subscribers who have been revoked under this stipulation will have to reapply at cost and without refund for new WidePoint NFI SSP Subscribers certificates that assert a trademark name that they or their organization have not infringed upon another party. Additionally, the WidePoint NFI SSP is not required to re-issue a correctly issued WidePoint NFI 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 NFI SSP Subscribers generating keys for requesting certificates (identity, device and non-escrowed encryption) that assert **id-orc-nfissp-medium**, **id-orc-nfissp-mediumHardware**, **id-orc-nfissp-pivi-hardware**, **id-orc-nfissp-pivi-cardAuth**, **id-orc-nfissp-pivi-hardware**, **id-orc-nfissp-pivi-cardAuth**, id-orc-nfissp-pivi-contentSigning, the WidePoint NFI SSP authenticates the Applicant or WidePoint NFI 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 NFI 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-orc-nfissp-medium**, the public key generated by the browser's associated Cryptographic Service Provider (CSP) and the challenge string supplied by the WidePoint NFI 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 base 64 encoded and sent to the WidePoint NFI SSP CA as part of the certificate request; the WidePoint NFI 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-orc-nfissp-mediumDevice**, the WidePoint NFI 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 NFI SSP PKI Sponsor submits the PKCS10 object to the WidePoint NFI SSP CA for certificate processing.

For **id-orc-nfissp-mediumHardware**, **id-orc-nfissp-mediumDeviceHardware**, **id-orc-nfissp-pivi-hardware**, **id-orc-nfissp-pivi-cardAuth**, **id-orc-nfissp-pivi-hardware**, **id-orc-nfissp-pivi-cardAuth**, and **id-orc-nfissp-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 NFI 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 NFI 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 NFI SSP CA as part of the certificate request; the WidePoint NFI 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 NFI SSP only provides escrow for the encryption certificate issued through the WidePoint NFI SSP CMS for certificates asserting the **id-orc-nfissp-medium** certificate policy OID. The WidePoint NFI SSP Subscriber's private key for the PIV-I encryption certificate is generated in the HSM and stored encrypted and protected by the Key Encryption Key (KEK) in a WidePoint NFI 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 NFI 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 NFI 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 NFI 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 NFI 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 NFI SSP Subscriber's affiliation.
- Applicant or WidePoint NFI SSP Subscriber presenting a government-issued photo badge including the Applicant or WidePoint NFI SSP Subscriber's affiliation.
- Applicant or WidePoint NFI 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 NFI SSP Subscriber presenting an un-expired photo ID badge issued by the organization.

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

Requests for Third-Party recovery of WidePoint NFI 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 NFI 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 NFI SSP Subscriber certificates that will assert the certificate policy OID of **id-orc-nfissp-medium** or **id-orc-nfissp-mediumHardware**, the Applicant or WidePoint NFI SSP Subscriber's in-person or supervised remote identity verification may be performed by a WidePoint NFI SSP Registration Authority, a WidePoint NFI SSP Local Registration Authority, or a WidePoint Trusted Agent as defined in Section 1.3.4 of this WidePoint NFI SSP CPS. Authentication by a WidePoint Trusted Agent does not relieve the WidePoint NFI SSP Registration Authority of their responsibility to verify that the required procedures were followed as detailed in this section.

The WidePoint NFI SSP offers supervised remote identity proofing in accordance with NIST SP 800-63A, Digital Identity Guidelines: Enrollment and Identity Proofing, Section 5.3.3. The WidePoint NFI SPP provides supervised remote identity proofing and enrollment transactions in locations where it is not possible or that perform in-person identity proofing imposes time or cost restraints on Applicants or WidePoint NFI SSP Subscribers. The WidePoint NFI SSP provides hardened and secured kiosks throughout the Unites States that meet the following conditions:

- The WidePoint NFI SSP monitors the entire identity proofing session by high-resolution video transmission, from which the Applicant or WidePoint NFI SSP Subscriber shall not depart from the view of the video.
- A live WidePoint NFI SSP Registration Authority, a WidePoint NFI SSP Local Registration Authority, or a WidePoint Trusted Agent participates remotely with the applicant for the entirety of the identity proofing session.
- All actions taken by the Applicant or WidePoint NFI SSP Subscriber during the identity proofing session are clearly visible to the remote WidePoint NFI SSP Registration Authority, a WidePoint NFI SSP Local Registration Authority, or a WidePoint Trusted Agent.
- Digital verification of evidence presented by the Applicant or WidePoint NFI SSP Subscriber, for such things as identity documentation, biometric capture (photo, fingerprints, retinal, palm, vein, etc.), be performed by integrated scanners and sensors that are encased within the kiosk and inaccessible by the Applicant or WidePoint NFI SSP Subscriber except for the parts of the component that do the scanning or sensing.
- All WidePoint NFI SSP Registration Authority, a WidePoint NFI SSP Local Registration Authority, or a WidePoint Trusted Agent have undergone a training program to detect potential fraud and to properly perform a supervised remote proofing session.
- The WidePoint NFI SSP kiosks employ physical tamper detection and resistance features consistent with the tamper detection requirements of the other components of the WidePoint NFI SSP.
- All communications occur over a mutually authenticated protected channels using TLS encryption.

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

At a minimum, authentication procedures for WidePoint NFI SSP organization applicants must include the following steps:

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

1. Process #1:

   A. The Applicant or WidePoint NFI SSP Subscriber presents a government-issued form of identification (e.g., an Organization ID badge, a passport, or driver's license) as proof of identity, and
   B. The WidePoint NFI 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 NFI SSP Registration Authority for currency and legitimacy (e.g., the Organization 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 NFI SSP Subscriber presents a government-issued form of identification (e.g., an Organization ID badge, a passport, or driver's license) as proof of identity, and
   B. The WidePoint NFI SSP Registration Authority examines the presented credential for biometric data that can be linked to the Applicant or WidePoint NFI SSP Subscriber (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and
   C. The Applicant or WidePoint NFI SSP Subscriber presents current corroborating information (e.g., current credit card bill or recent utility bill) to the WidePoint NFI SSP Registration Authority. The identifying information (e.g., name and address) on the credential presented above is verified by the WidePoint NFI SSP Registration Authority for currency and legitimacy (e.g., the Organization 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 NFI 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 NFI SSP Subscriber was submitted by an authorized sponsoring organization employee (e.g., contracting officer or contracting officer's technical representative).
- Verify sponsoring organization employee's identity and employment through either one of the following methods:

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

- Establish Applicant or WidePoint NFI 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 NFI SSP Subscriber presents a government-issued form of identification (e.g., an Organization ID badge, a passport, or driver's license) as proof of identity, and
     B. The WidePoint NFI SSP Registration Authority examines the presented credential for biometric data that can be linked to the Applicant or WidePoint NFI SSP Subscriber (e.g., a photograph on the credential itself or a securely linked photograph of Applicant or WidePoint NFI SSP Subscriber), and
     C. The credential presented shall be verified by the WidePoint NFI SSP Registration Authority for currency and legitimacy (e.g., the Organization 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 NFI SSP Subscriber presents a government-issued form of identification (e.g., an Organization ID badge, a passport, or driver's license) as proof of identity, and
     B. The WidePoint NFI SSP Registration Authority examines the presented credential for biometric data that can be linked to the Applicant or WidePoint NFI SSP Subscriber (e.g., a photograph on the credential itself or a securely linked photograph of Applicant or WidePoint NFI SSP Subscriber), and
     C. The Applicant or WidePoint NFI SSP Subscriber presents current corroborating information (e.g., current credit card bill or recent utility bill) to the WidePoint NFI 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 NFI 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 NFI SSP Registration Authority or a WidePoint NFI 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 NFI SSP Registration Authority records the following information:

- The identity of the person performing the validation process.
- Applicant or WidePoint NFI 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 NFI SSP Subscriber's identity, including identification type and unique number or alphanumeric identifier on the ID.
- A biometric of the Applicant or WidePoint NFI SSP Subscriber (facial image, fingerprint, etc.).
- The date and time of verification.
- A handwritten signature by the Applicant or WidePoint NFI 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-I 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 NFI SSP may request additional information or verification if deemed necessary to confirm the requestor's identity.

For WidePoint NFI SSP Subscriber certificates that assert the certificate policies OID of **id-orc-nfissp-pivi-hardware**, identity-proofing is performed in accordance with Section 2.7, PIV Identity Proofing and Registration Requirements, of FIPS 201-3. Additionally, the Applicant or WidePoint NFI SSP Subscriber must appear before the WidePoint NFI SSP Registration Authority either in person or via supervised remote and the WidePoint NFI SSP Registration Authority must capture:

- An electronic facial image used for printing facial image on the card, as well as for performing visual authentication during card usage;
- Two electronic fingerprints to be stored on the card for automated authentication during card usage; and

For WidePoint NFI SSP Subscriber certificates that assert the certificate policies OID of **id-orc-nfissp-medium** or **id-orc-nfissp-mediumHardware**, WidePoint NFI SSP Registration Authorities may accept authentication of the Applicant or WidePoint NFI 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 NFI SSP Registration Authority of its responsibility to verify required procedures were followed as described above.

3.2.3.2 Authentication of Human Subscribers for Role-based Certificates

Roles for which role-based certificates may be issued are limited to those that uniquely identify a specific role within an organization (e.g., Chief Information Officer is a unique role whereas Program Analyst is not). Role-based certificates from the WidePoint NFI SSP are not shared and shall be issued to individual subscribers and protected in the same manner as individual certificates.

The WidePoint NFI SSP records the information identified in Section 3.2.3.1 for a sponsor associated with the role before issuing a role-based certificate. The sponsor must hold an individual certificate in his/her own name issued by the WidePoint NFI SSP at the same or higher assurance level as the role based certificate.

The procedures for issuing role-based tokens comply with all other stipulations of this WidePoint NFI SSP CPS (e.g., key generation, private key protection, and Subscriber obligations).

For pseudonymous certificates that identify subjects by their organizational roles, the WidePoint NFI SSP validates with the organizational Point of Contact or Sponsor that the individual either holds that role or has been delegated the authority to sign on behalf of the role.

Practice Note: When determining whether a role-based certificate is warranted, consider whether the role carries inherent authority beyond the job title. Role-based certificates may also be used for individuals on temporary assignment, where the temporary assignment carries an authority not shared by the individuals in their usual occupation, for example: “Shift Lead, Security Operations Center”

3.2.3.3 Authentication of Human Subscribers for Group Certificates

Normally, a certificate is issued to a single WidePoint NFI SSP Subscriber. For cases where there are several entities acting in one capacity, and where non-repudiation for transactions is not required, a certificate may be issued that corresponds to a private key that is shared by multiple WidePoint NFI SSP Subscribers. The WidePoint NFI SSP through the WidePoint Registration Authorities shall record the information identified in Section 3.2.3.1 for a sponsor from the organization’s Information Systems Security Office or equivalent before issuing a group certificate.

In addition to the authentication of the sponsor, the following applies:

- The Information Systems Security Office or equivalent is responsible for ensuring control of the private key, including maintaining a list of WidePoint NFI SSP Subscribers who have access to use of the private key, and accounting for which WidePoint NFI SSP Subscriber had control of the key at what time.
- The subjectName DN shall not imply that the subject is a single individual, e.g., by inclusion of a human name form;
- The list of those with access to the shared private key shall be provided to, and retained by, the WidePoint NFI SSP; and
- The procedures for issuing tokens for use in shared key applications shall comply with all other stipulations of this WidePoint NFI CPS (e.g., key generation, private key protection, and Subscriber obligations).

3.2.3.4 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 NFI SSP CAA, or approved WidePoint NFI 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 NFI SSP Subscriber responsibilities.

For each WidePoint Card Management System and each Organization Card Management System, a digitally-signed e-mail from an authorized person is sent requesting authorization to the WidePoint NFI SSP.

For each Fully-Qualified Domain Name listed in certificate that asserts a certificate policy OID of **id-orc-nfissp-mediumDevice** or **id-orc-nfissp-mediumDeviceHardware**, the WidePoint NFI 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 organization must have a naming policy for devices that receive a certificate that asserts a certificate policy OID of **id-orc-nfissp-mediumDevice** or **id-orc-nfissp-mediumDeviceHardware** that specifies unique meaningful FQDN names and the WidePoint NFI SSP CPS documents how the WidePoint NFI SSP ensures compliance with the sponsoring organization's policy.

Note: FQDNs shall be listed in the certificate that asserts a certificate policy OID of **id-orc-nfissp-mediumDevice** or **id-orc-nfissp-mediumDeviceHardware** 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 NFI 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.

3.2.4 Non-Verified Subscriber Information

WidePoint NFI 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 NFI 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 NFI SSP Registration Authority or a WidePoint NFI SSP Local Registration Authority. The WidePoint NFI SSP accomplishes this validation for WidePoint NFI SSP Registration Authority and WidePoint NFI SSP Local Registration Authority via an Organizational Affiliation letter which is available on the WidePoint NFI SSP website. The Organizational Affiliation letter must be completed on organization letterhead and submitted with the certificate request documentation.

3.2.6 CRITERIA FOR INTEROPERATION

The WidePoint NFI SSP PMA determines the interoperability criteria for Certificate Authorities operating under the WidePoint NFI SSP CP. Memoranda Of Agreement(s) with the FPKIPA and other entities ensure interaction and interoperability with WidePoint NFI SSP or Organization Certificate Authorities, authorized State and Local Government agencies, and non-government Certificate Authorities. At no point will certificate authority or end-entity certificates issued under this WidePoint NFI SSP CP have more than one path back to the FBCA.

Note: Multiple trust paths created as a result of certificate renewal or CA rekey do not violate the single trust path requirement above.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

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

WidePoint NFI SSP Subscriber 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 NFI SSP Subscriber 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-orc-nfissp-medium**, **id-orc-nfissp-mediumHardware**, **id-orc-nfissp-pivi-hardware**, or **id-orc-nfissp-pivi-hardware**, a human WidePoint NFI 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 WidePoint NFI SSP Subscriber certificates that assert a certificate profile object identifier of **id-orc-nfissp-mediumDevice** or **id-orc-nfissp-mediumDeviceHardware**, 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 NFI 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 NFI SSP Subscriber who has had their certificate revoked will revert to being an Applicant and will be unknown to the WidePoint NFI SSP in terms of applying for certificate requests from the WidePoint NFI SSP in the future.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

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

A WidePoint Registration Authority may revoke a WidePoint NFI SSP Subscriber's certificate for cause as specified in Section 4.9.1 of this WidePoint NFI 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 NFI SSP Subscriber violated the terms of the Subscriber Agreement they acknowledged and signed. The WidePoint NFI SSP will maintain a list of authorized parties that includes persons appointed by the FPKIPA who may request revocation of any WidePoint NFI SSP Subscriber or WidePoint NFI SSP CA certificate. Revocation requests made by the FPKIPA are final and not subject to appeal or arbitration requests by the WidePoint NFI SSP Subscriber to whom the revocation requests apply.

Additionally, a WidePoint NFI SSP Local Registration Authority may perform a revocation request on behalf of a WidePoint NFI SSP Subscriber or for the organization to whom the WidePoint NFI SSP Subscriber is or was

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

3.5 IDENTIFICATION AND AUTHENTICATION FOR KEY RECOVERY REQUEST

3.5.1 KEY RECOVERY AGENT AUTHENTICATION

WidePoint NFI SSP Key Recovery Agents authenticate to a WidePoint NFI SSP Key Encryption Database or a WidePoint NFI SSP Data Decryption Server using a public key certificate issued by a WidePoint NFI SSP. 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 and must meet the requirements of a WidePoint NFI SSP Registration Authority PIV-I credential.

3.5.2 KEY RECOVERY OFFICIAL AUTHENTICATION

A WidePoint NFI SSP Key Recovery Official does not have access privileges to any WidePoint NFI SSP Key Encryption Database or a WidePoint NFI SSP Data Decryption Server. A WidePoint NFI SSP Key Recovery Official may request key recovery for any WidePoint NFI 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 NFI SSP Subscriber certificate that is at an assurance level equivalent to or greater than the WidePoint NFI SSP Subscriber certificate for which they are requesting recovery.

3.5.3 WIDEPOINT NFI SSP SUBSCRIBER KEY RECOVERY REQUEST AUTHENTICATION

The WidePoint NFI SSP securely stores all encryption private keys issued by WidePoint NFI SSP CAs to all WidePoint NFI 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 NFI SSP. Escrow of the private key occurs at the time of issuance of the certificate bound to that private key.

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

WidePoint NFI SSP Subscribers may authenticate to the WidePoint NFI SSP CA with their valid WidePoint NFI SSP certificate to request the recovery of their escrowed keys. The WidePoint NFI 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 NFI SSP Subscribers may request recovery through a WidePoint NFI SSP Registration Authority or a WidePoint NFI SSP Local Registration Authority by establishing their identity either through use of their WidePoint NFI SSP certificate in the form of a digitally signed message that is signed by a valid WidePoint NFI 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 NFI SSP CPS. If the recovery request is submitted by a WidePoint NFI SSP LRA on behalf of the WidePoint NFI SSP Subscriber, the WidePoint NFI SSP LRA will submit the recovery request to a WidePoint NFI SSP Registration Authority by digitally signed message that is signed by a valid WidePoint NFI SSP certificate issued to the WidePoint NFI SSP Local Registration Authority and that asserts a certificate policy equal to or greater than the certificate policy in the associated certificate of the escrowed key for which recovery has been requested.

3.5.4 Third-Party Key Recovery Request Authentication

Third Parties, described as any entity other than the WidePoint NFI SSP Subscriber to whom the associated certificate of an escrowed key has been issued, may request recovery of escrowed keys from the WidePoint NFI SSP. All third-party requests will be coordinated through a WidePoint NFI SSP Registration Authority. The WidePoint NFI 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 NFI SSP and the FPKIMA as appropriate.

The third-party requestor will establish their identity to the WidePoint NFI SSP RA either through use of their own WidePoint NFI SSP certificate or federal certificate that is cross-certified with Federal Bridge Certificate 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 NFI 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 NFI SSP Registration Authority of the intended key recovery through the same methods stipulated in this paragraph.

Third-party requestors may be a WidePoint NFI SSP PKI Point of Contact for organizations wishing to recover the escrowed keys of WidePoint NFI 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 NFI SSP and the FPKIPA prior to any recovery being permitted.

3.5.5 WidePoint NFI SSP Data Decryption Server Authentication

A WidePoint NFI SSP Data Decryption Server or organization Data Decryption Server authenticates to a WidePoint NFI SSP KED directly using a public key certificate issued by the WidePoint NFI SSP. The assurance level of the certificate issued to a WidePoint NFI SSP Data Decryption Server or organization Data Decryption Server shall be issued with the certificate policy OID of **id-orc-nfissp-mediumDeviceHardware** 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 NFI SSP Key Encryption Database or a WidePoint NFI SSP Data Decryption Server or organization Data Decryption Server.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

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

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

The WidePoint NFI SSP may certify other certificate authorities. The WidePoint NFI SSP may issue certificates to either a WidePoint NFI SSP subordinate certificate authority or a WidePoint NFI SSP subordinate certificate authority to an external entity or organization.

4.1.1 WHO CAN SUBMIT A CERTIFICATE APPLICATION

The WidePoint NFI SSP only accepts certificate applications from Applicants or WidePoint NFI SSP Subscribers for WidePoint NFI 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 NFI SSP CPS except **id-orc-nfissp-pivi-contentSigning**.

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

A WidePoint NFI SSP PKI Sponsor for a device certificate asserting a certificate policy **id-orc-nfissp-mediumDevice** or **id-orc-nfissp-mediumDeviceHardware** must accept and abide by the responsibilities of a WidePoint NFI SSP Subscriber for the certificate of the device.

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

4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES

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

4.1.2.1 Browser and Token Based Enrollment Process and Responsibilities

Applicants and WidePoint NFI SSP Subscribers requesting certificates that assert a certificate policy OID of **id-orc-nfissp-medium,** and **id-orc-nfissp-mediumHardware,** 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, for initial identity validation, in accordance with Section 3.2 for identity proofing as described in this WidePoint NFI SSP CPS. Applicants and WidePoint NFI SSP Subscribers requesting certificates that assert a certificate policy OID of **id-orc-nfissp-medium**, may generate their certificate requests prior to appearing before a WidePoint Registration

Authority, a WidePoint Local Registration Authority, or a Trusted Agent to have their identity verified. Applicants and WidePoint NFI SSP Subscribers requesting certificates that assert a certificate policy OID of **id-orc-nfissp-mediumHardware** are required to appear in-person and must have the generation of their certificate requests and the key generation on the FIPS 140-3 Level 2 token witnessed by a WidePoint Registration Authority or a WidePoint Local Registration Authority who possess a WidePoint NFI SSP Medium Hardware or WidePoint NFI SSP PIV-I credential.

Upon acceptance by the Applicant or WidePoint NFI SSP Subscriber of the Subscriber Obligations detailed in Section 9.6.4 of this WidePoint NFI SSP CPS, the Applicant or WidePoint NFI SSP Subscriber will submit the certificate request with their user specific information in accordance with Section 3.1.1 of this WidePoint NFI SSP CPS. This information will include:

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

Once the Applicant or WidePoint NFI SSP Subscriber has verified the accuracy of the data they are providing in the certificate request, the Applicant or WidePoint NFI SSP Subscriber submits the certificate request to the WidePoint NFI SSP for processing. At this time, a dual-key generation process is initiated. The specific dual-key generation process for each assurance level is detailed below:

For certificates that assert a certificate policy OID of **id-orc-nfissp-medium**, this process is initiated in the Applicant or WidePoint NFI SSP Subscriber's FIPS 140-3 Level 1 compliant browser where the public key generated during the key generation process is bundled with the Applicant or WidePoint NFI SSP Subscriber's data into a CRMF and sent to the WidePoint NFI SSP. The WidePoint NFI SSP, upon receiving the Applicant or WidePoint NFI SSP Subscriber's 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 Applicant or WidePoint NFI SSP Subscriber, completed and taken either to a WidePoint Registration Authority or a Trusted Agent for identity verification as described in Section 3.2.3.1 of this WidePoint NFI SSP CPS.

For certificates assert a certificate policy OID of **id-orc-nfissp-mediumHardware**, this process is initiated in the Applicant or WidePoint NFI SSP Subscriber's FIPS 140-3 Level 2 compliant token where the public key generated during the generation process is bundled with the Applicant or WidePoint NFI SSP Subscriber's data into a CRMF and sent to the WidePoint NFI SSP. The certificate generation process must occur in-person with a WidePoint Registration Authority or a WidePoint Local Registration Authority. The WidePoint NFI SSP, upon receiving the Applicant or WidePoint NFI SSP Subscriber's request data, will verify and process the request and return a request confirmation form populated with the request information that is to be printed, completed and signed by the Applicant or WidePoint NFI SSP Subscriber in the presence of the WidePoint Registration Authority or the WidePoint Local Registration Authority that witnessed the key generation process at time of request submittal. The WidePoint Registration Authority or a WidePoint Local Registration Authority that witnessed the key generation process at time of request submittal will sign the printed key form attesting that they performed the identity verification as described in Section 3.2.3.1 of this WidePoint NFI SSP CPS and witnessed the key generation process for the Applicant or WidePoint NFI SSP Subscriber.

When applicable, as in the case of all identity and encryption assert a certificate policy OID of **id-orc-nfissp-medium,** and **id-orc-nfissp-mediumHardware**, that are issued to a WidePoint Registration Authority or a WidePoint Local Registration Authority, the organization to which the WidePoint Registration Authority or a WidePoint Local Registration will name a WidePoint NFI SSP PKI Point of Contact for verification of any roles or authorizations to be included in their certificates via signed letterhead or digitally signed email. WidePoint Certificate Authority Administrators or a lead WidePoint Registration Authority who is a direct employee of the WidePoint NFI SSP will record all such appointments in a log available to all WidePoint Registration Authorities and

WidePoint Local Registration Authorities. The WidePoint Registration Authority or the WidePoint Local Registration Authority can then reference the log to verify a requested role or authorization via a point of contact.

At the time of certificate request for certificates that assert a certificate policy OID of **id-orc-nfissp-mediumHardware**, the WidePoint Registration Authority or the WidePoint Local Registration Authority will record the serial number of the credential (cryptographic token) for the Applicant or the WidePoint NFI SSP Subscriber and include that information in the email sent to the WidePoint Registration Authority.

4.1.2.2 WidePoint NFI SSP PIV-I Credential Enrollment Process and Responsibilities

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

Applicants or WidePoint NFI SSP Subscribers asserting an organizational affiliation must be authorized by a WidePoint NFI SSP PKI Point of Contact for that organization. Applicants or WidePoint NFI 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 NFI SSP Subscribers requesting WidePoint NFI 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 NFI SSP CPS to complete the enrollment process.

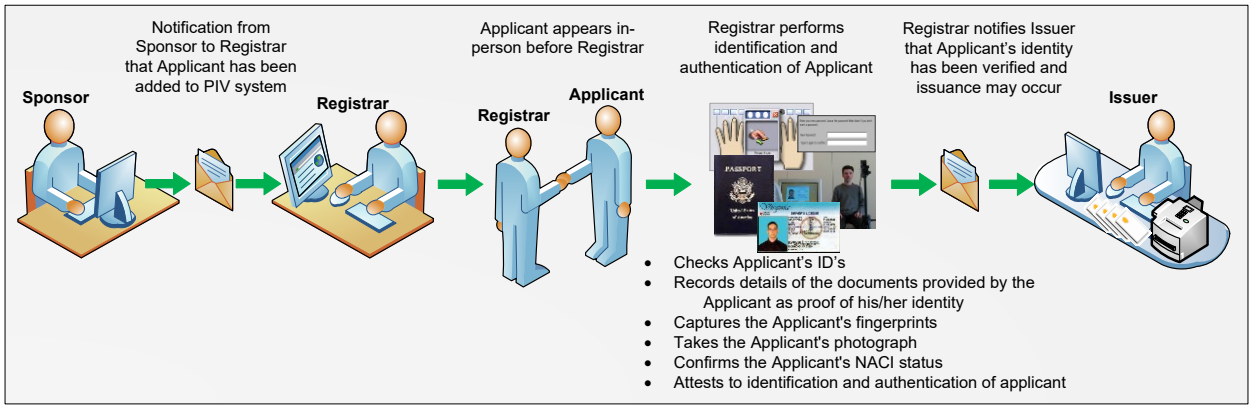

Figure 5 – WidePoint NFI SSP PIV-I Workflow

The WidePoint Registrar, upon identity verification, will capture the following from the Applicant or WidePoint NFI SSP Subscriber if it has not already been preloaded by the WidePoint NFI SSP PKI Point of Contact into the WidePoint NFI SSP or organization 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 NFI SSP Subscriber. These biometrics include:

- Fingerprints of both index fingers (substitution of fingers are allowed); and,
- Digital photo of the Applicant or WidePoint NFI SSP Subscriber

- Hair color - optional
- Eye color - optional.

Upon confirmation of the information provided and capture of the Applicant or WidePoint NFI SSP Subscriber's biometrics, the WidePoint Registrar will approve the Applicant or WidePoint NFI SSP Subscriber's request for a WidePoint NFI SSP PIV-I credential. This action asserts that the WidePoint Registrar has vetted and gathered the necessary information for the Applicant or WidePoint NFI SSP Subscriber and that the WidePoint Registrar has certified that the Applicant or WidePoint NFI SSP Subscriber may move to the issuance process controlled by the WidePoint Issuer.

4.1.2.3 WidePoint NFI SSP CA signing certificate request process and Responsibilities

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

WidePoint NFI SSP CAs only issue certificates asserting the certificate policies defined in Section 1.2 of this WidePoint NFI 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 NFI SSP Sponsor requesting certificates that assert a certificate policy OID of **id-orc-nfissp-mediumDevice** or **id-orc-nfissp-mediumDeviceHardware** 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 NFI 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 NFI SSP Sponsor acts as the WidePoint NFI SSP Subscriber for the device for which they are requesting a certificate.

Upon acceptance by the WidePoint NFI SSP Sponsor of the Component Obligations, the WidePoint NFI 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 NFI 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 NFI SSP Sponsor specific information:
    - First name
    - Middle name or initial
    - Last name
    - Organization name
    - Email address
    - Location (either United States or Non-United States)
    - Contact phone information

Once the WidePoint NFI SSP Sponsor has verified the accuracy of the data they are providing in the certificate request, the WidePoint NFI SSP Sponsor submits the PKCS#10 formatted request and the data entered for Component and WidePoint NFI SSP Subscriber information to the WidePoint NFI SSP for processing. The WidePoint NFI SSP, upon receiving the WidePoint NFI 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 NFI 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 NFI 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 NFI SSP CPS. The Applicant or WidePoint NFI 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-orc-nfissp-medium**, **id-orc-nfissp-mediumHardware**, **id-orc-nfissp-mediumDevice**, or **id-orc-nfissp-mediumDeviceHardware** or a WidePoint Registrar in the case of WidePoint NFI SSP PIV-I credentials.

In the case of persons legally empowered by the WidePoint NFI SSP to witness and certify the validity of documents and to take affidavits and depositions, it is the responsibility of the Applicant or WidePoint NFI SSP Subscriber to ensure that the notarized certificate request and validation package is mailed to the WidePoint NFI SSP via United States Postal Service mail or other appropriate delivery method such as Federal Express, United Parcel Service, or another provider that requires a signed receipt.

Upon receipt of a complete certificate request and identity validation package from the Applicant or WidePoint NFI 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 NFI SSP CPS. The verifying WidePoint NFI SSP Local Registration Authority will send a digitally signed message to a WidePoint Registration Authority approving the Applicant or WidePoint NFI 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 NFI SSP Subscriber identity was authenticated. In no case will WidePoint NFI 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 NFI SSP Registration Authority or a WidePoint NFI SSP Local Registration Authority will deny issuance if:

- the WidePoint NFI SSP Registration Authority or WidePoint NFI 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 NFI SSP CPS; or,
- the Applicant or WidePoint NFI SSP Subscriber fails to provide documentation verifying their name or organizational affiliation.

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

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

4.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS

The entire process from Applicant or WidePoint NFI SSP Subscriber appearing before a WidePoint Registration Authority, a WidePoint NFI 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 NFI SSP PIV-I credential issuance, the WidePoint NFI SSP Issuer accesses a WidePoint NFI SSP CMS workstation by authenticating with their WidePoint NFI SSP PIV-I credential to the WidePoint NFI SSP CMS. The WidePoint NFI SSP CMS workstation is comprised of a desktop or laptop and various peripherals, as shown below in Figure 8.

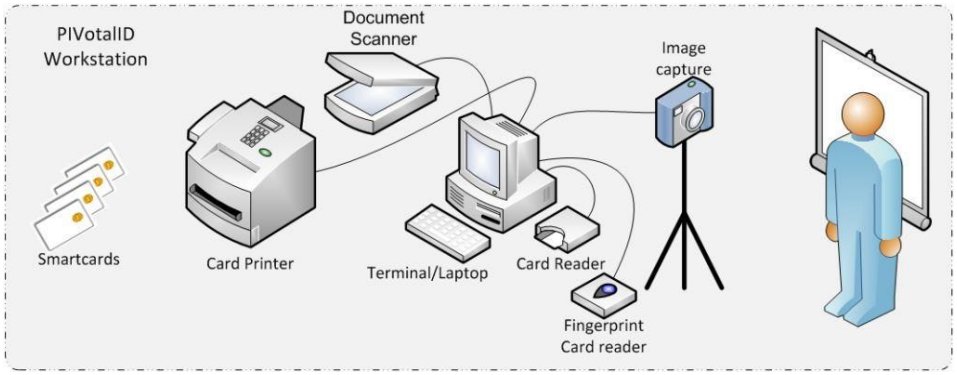

Figure 8 – WidePoint NFI SSP CMS Workstation Components

The Applicant or WidePoint NFI SSP Subscriber must appear in person before a WidePoint NFI SSP Issuer at a WidePoint NFI SSP CMS workstation. A WidePoint NFI SSP Issuer will compare the identity documentation provided by the Applicant or the WidePoint NFI 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 NFI SSP Issuer will print the WidePoint NFI SSP Subscriber's PIV-I credential. After the card has been successfully printed, the Applicant or WidePoint NFI 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 NFI SSP Subscriber's card begins the activation process. Upon successful completion of the WidePoint NFI SSP PIV-I Credential Activation, the Applicant or WidePoint NFI SSP Subscriber must attest to the WidePoint NFI SSP Subscriber Obligations as detailed in Section 9.6.4 of this WidePoint NFI SSP CPS.

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

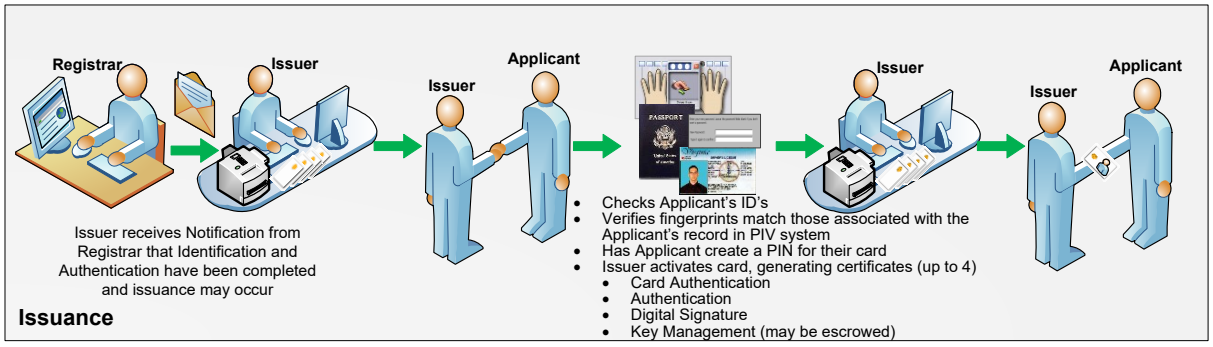

Figure 9 – WidePoint NFI SSP Issuer Workflow

For **id-orc-nfissp-mediumDevice** and **id-orc-nfissp -pivi-contentSigning** upon successful completion of the subscriber identification and authentication process in accordance with Section 3.2.3, Authentication of Individual Identity, of this WidePoint NFI SSP CPS, a WidePoint Registration Authority creates the requested certificate, notifies the applicant thereof, and, after ensuring that the WidePoint NFI SSP 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.

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

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

The WidePoint NFI SSP Subscriber will import their certificate(s) from the WidePoint NFI SSP CA. The WidePoint NFI 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 NFI SSP Subscriber constitutes acceptance. Additionally, the WidePoint NFI SSP logs the acceptance of the certificate by the WidePoint NFI SSP Subscriber.

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

For WidePoint NFI SSP PIV-I credentials, the WidePoint NFI SSP Issuer authorizes the WidePoint NFI SSP CMS to authenticate to the WidePoint NFI SSP CA with its internal connector certificate that is a trusted user on the WidePoint NFI SSP CA. The WidePoint NFI SSP CA creates all certificates for the WidePoint NFI SSP PIV-I credentials, generates, and escrows the encryption private key and recovers any previous encryption keys escrowed for the WidePoint NFI SSP Subscriber. This process is conducted in the presence of the WidePoint NFI SSP Subscriber and the WidePoint NFI SSP Subscriber is notified as part of the Certificate Acceptance process as defined in Section 4.4 Certificate Acceptance below.

4.4 Certificate Acceptance

Prior to the issuance of any WidePoint NFI SSP Subscriber certificate and before any effective use of the WidePoint NFI SSP Subscriber's private key, the WidePoint NFI SSP:

- Explains to the WidePoint NFI SSP Subscriber their responsibilities and obligations as defined in Section 9.6.3.
- Informs the WidePoint NFI SSP Subscriber of the creation of their certificate and the contents of the certificate.
- Requires the WidePoint NFI SSP Subscriber to accept their obligations and their certificate, with a handwritten signature in the case of manual enrollment process or through a digital signature in the case of enrollment through the WidePoint NFI SSP CMS.

- Notifies the WidePoint NFI SSP Subscriber that their Encryption certificate decryption key has been escrowed in accordance with the procedures of this WidePoint NFI SSP CPS; and,
- Documents the WidePoint NFI SSP Subscriber's acceptance of their responsibilities and their certificate.

For acceptance of the responsibilities and obligations of WidePoint NFI SSP device certificates that assert the certificate policy of **id-orc-nfissp-mediumDevice** or **id-orc-nfissp-mediumDeviceHardware**, the WidePoint NFI SSP Sponsor of the referenced device performs the functions of the WidePoint NFI SSP Subscriber.

4.4.1 Conduct Constituting Certificate Acceptance

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

4.4.2 Publication of the Certificate by the WidePoint NFI SSP

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

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

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

4.5 Key Pair and Certificate Usage

4.5.1 WidePoint NFI SSP Subscriber Private Key and Certificate Usage

The WidePoint NFI SSP Subscriber and the WidePoint NFI SSP Sponsor in the case of device certificates attest to their obligations as specified in Section 9.6.3 of this WidePoint NFI 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 NFI SSP will publicly post a summary of this WidePoint NFI SSP CPS on the WidePoint NFI SSP Repositories as specified in Section 2.1 to provide Relying Parties information regarding the expectation of the WidePoint NFI SSP and use of certificates issued to WidePoint NFI 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 NFI SSP issued certificate. Additional Relying Party obligations are stipulated in Section 9.6.4 of this WidePoint NFI SSP CPS.

4.6 CERTIFICATE RENEWAL

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

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

- The certificate presented was issued by the WidePoint NFI 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 NFI SSP CA that issued the certificate.

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

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

The WidePoint NFI SSP Renewal Portal captures the certificate policy from the certificate presented by the WidePoint NFI 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 NFI SSP Subscriber certificate presented. The WidePoint NFI SSP Renewal Portal accomplishes this by checking flag fields in the WidePoint NFI SSP Subscriber's entry in the WidePoint NFI SSP Repository that are set during the WidePoint NFI 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 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 NFI 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-orc-nfissp-mediumHardware**, the WidePoint NFI 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 NFI 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-orc-nfissp-mediumHardware** to be renewed has a current validity of 1 or 2 years, the WidePoint NFI SSP Renewal Portal will only allow the WidePoint

NFI 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 NFI SSP Subscriber renewal requests are then pre-populated with the information from the previous requests and issued certificates and are unalterable by the WidePoint NFI 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 NFI SSP. This retrieved record contains the profile information on the WidePoint NFI SSP that created the certificate presented during electronic authentication and the renewal request is submitted against that same profile. The WidePoint NFI 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 NFI 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 NFI SSP Subscriber of the renewal request cannot exceed the maximum key life determined by this WidePoint NFI SSP CPS and Federal Bridge Certificate Policy for the certificate policy requested. The maximum validity period that the WidePoint NFI SSP Subscriber can request is 3 years; and,
- A unique request ID number assigned by the WidePoint NFI SSP.

When a successful renewal request is made, the WidePoint NFI SSP Renewal Portal presents a request form to the WidePoint NFI SSP Subscriber. The WidePoint NFI 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 NFI SSP Subscriber then transmits the renewal request form to a WidePoint NFI SSP Registration Authority or WidePoint NFI SSP Local Registration Authority. If the renewal request form is transmitted to a WidePoint NFI SSP Local Registration Authority, the WidePoint NFI SSP Local Registration Authority will send a digitally signed email requesting that the renewal certificates be issued. The WidePoint NFI SSP Local Registration Authority then sends a digitally signed email that includes the request ID numbers to the WidePoint NFI SSP Registration Authority requesting issuance of the renewal certificate(s) based on the WidePoint NFI 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 NFI SSP Subscriber Certificate renewal request forms from the WidePoint NFI SSP Subscriber, or a digitally-signed email containing certificate renewal request information (including the request ID number) from an approved WidePoint NFI SSP Local Registration Authority for the organization for which the certificate has been issued and is requested, a WidePoint NFI SSP Local Registration Authority performs a manual search of the WidePoint NFI 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 NFI SSP Local Registration Authority examines all prior certificate issuances to the named WidePoint NFI SSP Subscriber. Since the renewed public portion of the WidePoint NFI 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 NFI SSP Subscriber's expiring or renewed certificate. When the WidePoint NFI SSP Subscriber's renewed certificate is imported into the secure container, the WidePoint NFI SSP Subscriber's expiring public certificate is overwritten. Only one version of the WidePoint NFI SSP Subscriber's certificate can be present on the secure container. When the WidePoint NFI SSP Subscriber's renewed certificate is imported, the WidePoint NFI SSP Subscriber's expiring certificate is destroyed. Therefore, a WidePoint NFI 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 NFI SSP Local Registration Authority will not forward the request for issuance, the WidePoint NFI SSP LRA will contact the WidePoint NFI SSP Subscriber to ensure the proper importation of the previously renewed WidePoint NFI SSP Subscriber certificate. This procedure ensures that a WidePoint NFI SSP Subscriber certificate is not further renewed or rekeyed.

WidePoint NFI SSP does not accept renewal requests from certificates that assert a policy oid of **id-orc-nfissp-pivi-hardware** or **id-orc-nfissp-pivi-cardAuth** except during recovery from a CA key compromise (see Section 5.7.3), In such cases, the renewed certificate must expire as specified in the original WidePoint NFI SSP Subscriber certificate.

In all cases, the WidePoint NFI 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 NFI SSP accepts requests for certificate renewal pursuant to the following circumstances:

- The public key of the WidePoint NFI SSP Subscriber certificate presented has not reached the end of its validity.
- The WidePoint NFI SSP Subscriber certificate presented has not been revoked.
- The total lifetimes of certificate issued to the WidePoint NFI 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 NFI SSP Subscriber certificate presented has not been compromised; and,
- The WidePoint NFI SSP Subscriber name and attributes in the current valid certificate have not changed.

WidePoint NFI 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 NFI SSP Subscriber provides a link to the WidePoint NFI SSP Renewal Portal where WidePoint NFI SSP Subscribers may submit certificate renewal requests.

4.6.2 Who May Request Renewal

All WidePoint NFI SSP Subscribers who have certificates that assert a certificate policy of **id-orc-nfissp-mediumHardware** may submit requests themselves, to PKI Sponsors or WidePoint Registration Authorities to have their certificates renewed.

4.6.3 Processing Certificate Renewal Requests

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

4.6.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2 of this WidePoint NFI SSP CPS.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

See Section 4.4.1 of this WidePoint NFI SSP CPS.

4.6.6 Publication of the Renewal Certificate by the CA

See Section 4.4.2 of this WidePoint NFI SSP CPS.

4.6.7 Notification of Certificate Issuance by the CA to other Entities

See Section 4.4.3 of this WidePoint NFI SSP CPS.

4.7 Certificate Re-Key

The WidePoint NFI SSP only accepts electronic authentication for certificate re-key for currently valid digital WidePoint NFI SSP Subscriber certificates issued by the WidePoint NFI SSP that assert a certificate policy of **id-orc-nfissp-medium**. The WidePoint NFI SSP does not offer certificate re-key for WidePoint NFI SSP Subscribers certificates that assert any other certificate policy as described in Section 1.2 of this WidePoint NFI SSP CPS but

may renew those certificates if they meet the requirements as specified in Section 4.6 of this WidePoint NFI SSP CPS. WidePoint NFI 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 NFI 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 NFI SSP accepts requests for certificate re-key pursuant to the following circumstances:

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

WidePoint NFI 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 NFI SSP Subscriber provide a link to the WidePoint NFI SSP Renewal Portal where WidePoint NFI SSP Subscribers may submit certificate re-key requests.

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

4.7.2 Who May Request Certification of a New Public Key

All WidePoint NFI SSP Subscribers who have certificates that assert a certificate policy of **id-orc-nfissp-medium** may submit requests to have their certificates re-keyed.

4.7.3 Processing Certificate Re-Keying Requests

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

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

[1] 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.

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

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 NFI 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 NFI SSP may choose to update a certificate of a WidePoint NFI SSP Subscriber who mistyped their email address. The old certificate is revoked, and therefore cannot be further re-keyed, renewed, or updated.

The WidePoint NFI 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 NFI SSP RA or LRA searches the WidePoint NFI 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 NFI SSP does not accept modification for certificates that assert a certificate policy of **id-orc-nfissp-mediumHardware**, **id-orc-nfissp-pivi-hardware**, **id-orc-nfissp-pivi-cardAuth** or **id-orc-nfissp-pivi-contentSigning**. If a certificate that asserts a certificate policy of **id-orc-nfissp-pivi-hardware**, or **id-orc-nfissp-pivi-cardAuth**, requires modification a new WidePoint NFI SSP PIV-I Credential is created, and new certificates are issued.

4.8.1 Circumstances for Certificate Modification

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

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

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

4.8.2 Who May Request Certificate Modification

A WidePoint NFI SSP Subscriber may request certificate modification to a WidePoint NFI SSP LRA. The WidePoint NFI SSP LRA confirms the desired modification and forwards the modification request to a WidePoint NFI SSP RA. The WidePoint NFI SSP LRA will validate any changes in the WidePoint NFI SSP Subscriber's authorizations reflected in the certificate such as email address, or length of validity period 1, 2, or 3 years.

The method by which the WidePoint NFI SSP LRA confirms the desired modification will depend on the nature of the certificate being modified (assurance level, etc.) and the desired modification(s). Where possible, the modification will be confirmed via electronic mail digitally signed by a Partner LRA or by the Subscriber. However, since the most common modification is for the email address, digitally signed electronic mail is not always possible. In this case the WidePoint NFI SSP RA or LRA will confirm that the WidePoint NFI SSP Subscriber is in possession of

the private key through a successful authentication as described in Section 3.2.3.2 of this WidePoint NFI SSP CPS and will verify other information to include the certificate's serial number, validity dates, common name and WidePoint NFI SSP UID against the WidePoint NFI SSP Repository.

4.8.3 Processing Certificate Modification Requests

WidePoint NFI SSP Subscribers may submit requests for certificate modification in writing, via email, or via help-desk requests. WidePoint NFI 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 NFI SSP RA or LRA. WidePoint NFI 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 NFI SSP personnel is sent by email or recorded in a help desk application. The request for certificate modification is assigned to a WidePoint NFI SSP LRA for processing. The WidePoint NFI SSP LRA reviews the requested modification and all records related to the certificate issuance. Upon successful review, the WidePoint NFI SSP LRA will forward the certificate modification request to the WidePoint NFI SSP RA for issuance. The WidePoint NFI SSP LRA may contact the WidePoint NFI SSP Subscriber to gather amplifying information and evidence or reject the request if sufficient information and evidence cannot be obtained. A modified certificate may use the same or a different subject public key as the original certificate, depending on issuance constraints. However, if the same key is used, certificate operational periods and key lifetimes as defined in Section 6.3.2 continue to apply.

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 NFI SSP Subscriber, or the Sponsoring Organization (where applicable), is responsible for promptly requesting revocation of any WidePoint NFI SSP Subscriber certificate for any of the reasons listed below. WidePoint NFI 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 NFI 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 NFI 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.

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

Whenever any of the above circumstances occur, the associated certificate will be revoked and placed on the CRL for the WidePoint NFI 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 NFI SSP certificates will remain on the CRL of the WidePoint NFI SSP CA that issued the certificates until they expire. Revoked WidePoint NFI SSP certificates are removed from the respective CRL upon their expiration but must at least appear in one CRL.

WidePoint NFI SSP Subscribers leaving the organization that sponsored their participation are required to surrender to their organization's WidePoint NFI 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 NFI 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 NFI SSP LRA to revoke the certificate, providing the WidePoint NFI SSP Subscriber's:

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

The WidePoint NFI SSP LRA searches the WidePoint NFI SSP Repository for certificates issued to the WidePoint NFI SSP Subscriber and identifies certificates by verifying the submitted information. The WidePoint NFI SSP LRA then notes the serial number(s) and date of issuance of every current certificate issued to that WidePoint NFI SSP Subscriber and sends a request to the WidePoint NFI 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 NFI SSP Subscriber that express an organizational affiliation, the organization's WidePoint PKI Point of Contact must inform the WidePoint NFI SSP of any changes in a WidePoint NFI SSP Subscriber's affiliation through a digitally signed email or through a digitally signed transaction through the WidePoint NFI SSP CMS. If the Affiliated Organization no longer authorizes the affiliation of a WidePoint NFI SSP Subscriber, the WidePoint NFI SSP will revoke any certificates issued to that WidePoint NFI SSP Subscriber containing the organization affiliation. If an Affiliated Organization terminates its relationship with the WidePoint NFI SSP such that it no longer provides updates to organizational affiliation information, the WidePoint NFI 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 NFI SSP certificate:

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

If any individual has reason to believe that a WidePoint NFI SSP issued certificate private key has been compromised, that individual is required to notify the WidePoint NFI SSP of the compromise suspicion. It is the responsibility of the WidePoint NFI SSP, in particular a WidePoint NFI SSP RA, to investigate the information and

determine if certificate revocation is warranted, based on communications with either the WidePoint NFI SSP Subscriber that is identified by the suspected compromised certificate or an organization representative such as the WidePoint NFI SSP PKI Point of Contact for that organization or an employee of the organization who has been duly appointed as a WidePoint NFI SSP LRA for the WidePoint NFI SSP Subscriber's organization. The WidePoint NFI SSP RA will verify the WidePoint NFI SSP Subscriber Name, Organization and email address associated with the certificate to be revoked. If there is ambiguity, the WidePoint NFI SSP will investigate for additional information to ensure accuracy.

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

4.9.3 PROCEDURE FOR REVOCATION REQUEST

Revocation requests of human or device WidePoint NFI SSP Subscriber certificates can be made through the WidePoint NFI SSP Help Desk or directly to a WidePoint NFI 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 NFI SSP Help Desk call, the revocation request will be forwarded to a WidePoint NFI SSP RA for verification and processing. WidePoint NFI SSP Help Desk personnel will send a digitally signed email with the information identified above to the WidePoint NFI SSP RA or LRA. A revocation request may also be submitted in letter form through a signed letter delivered to the WidePoint NFI SSP to the address identified in Section 1.5.2 of this WidePoint NFI SSP CPS. A WidePoint NFI SSP Form Letter Revocation Request is available at the WidePoint NFI SSP website or can be provided via a help desk request.

Upon receipt of a revocation request, a WidePoint NFI 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 NFI 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 NFI SSP PKI Point of Contact or an organization executive with approval authority if the WidePoint NFI SSP PKI Point of Contact is unavailable for any reason including a revocation request submitted against their own WidePoint NFI SSP Subscriber certificate. If the named WidePoint NFI SSP Subscriber is requesting revocation of their own certificate, the WidePoint NFI SSP, typically a WidePoint NFI 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 NFI SSP CPS. If a WidePoint NFI SSP RA chooses to revoke a certificate because of sufficient evidence of noncompliance with this WidePoint NFI SSP CPS, the WidePoint NFI SSP RA will document the reason for certificate revocation and will notify the WidePoint NFI SSP Subscriber unless directed otherwise by the FPKIPA or a court of competent jurisdiction.

If the WidePoint NFI SSP RA or WidePoint NFI SSP Issuer determines there is a need to revoke the certificate once an authorized request is received, the WidePoint NFI SSP RA or WidePoint NFI 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 NFI SSP RA or WidePoint NFI 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 NFI SSP Subscriber and the WidePoint indicates that reason in their respective revocation request email.

For WidePoint NFI SSP Subscribers, who have received cryptographic tokens such as needed for a WidePoint NFI SSP PIV-I credential and are leaving the organization that sponsored their participation in the WidePoint NFI SSP, must surrender to their organization's WidePoint NFI 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 NFI 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. WidePoint NFI SSP Subscriber

credentials (cryptographic tokens) are the responsibility of the sponsoring organization, including procurement and final disposition. If a WidePoint NFI SSP Subscriber leaves an affiliated organization and the WidePoint NFI SSP Subscriber credentials (cryptographic tokens) cannot be obtained from the WidePoint NFI SSP Subscriber, then all WidePoint NFI 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 NFI SSP Subscriber certificates will be revoked upon request as soon as the need can be verified. There is no grace period. A WidePoint NFI SSP Subscriber, or their sponsoring organization's WidePoint NFI SSP PKI Point of Contact or an organization executive with approval authority if the WidePoint NFI SSP PKI Point of Contact is unavailable for any reason, FPKIPA personnel, and WidePoint NFI SSP personnel must request revocation from the WidePoint NFI 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 NFI SSP CAs process revocation requests as quickly as practical upon receipt of an authenticated revocation request as will be but as an operating practice within two hours or receipt. The WidePoint NFI SSP Subscriber, or their sponsoring organization, must request revocation from WidePoint NFI SSP as soon as the need for revocation has been determined. Revocation requests for WidePoint NFI SSP PIV-I credentials are processed immediately upon receipt by the WidePoint NFI SSP or approved organization Card Management System which then authenticates to the appropriate WidePoint NFI SSP Certificate Authority and revokes the certificates associated with the WidePoint NFI SSP PIV-I credential. All revocations requests received within two hours of the next CRL issuance will be processed before the next CRL is published. The CRL issuance frequency for each WidePoint NFI SSP CA is addressed in Section 4.9.7 of this WidePoint NFI SSP CPS.

The WidePoint NFI 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 NFI 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 NFI 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 NFI 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 NFI 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 NFI SSP Subscriber certificate against the Certificate Revocation List, hereafter referred to as CRL, of the WidePoint NFI SSP CA that issued the WidePoint NFI 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 NFI SSP Subscriber certificate or make an informed decision to accept the risk, responsibility, and consequences for using a WidePoint NFI SSP Subscriber certificate whose authenticity cannot be guaranteed to the standards of the this WidePoint NFI SSP CPS and Federal Bridge Certificate Policy.

The following text is included in the WidePoint NFI SSP Subscriber Agreement and posted on the WidePoint NFI 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 NFI SSP CA is required to issue CRLs daily. As a general rule, WidePoint NFI SSP CAs issue a new CRL every 6 hours but in all cases WidePoint NFI SSP CAs will issue a new CRL within 24 hours of the last issued CRL. WidePoint NFI SSP CA CRLs are issued with a maximum validity period of 48 hours. New CRLs for WidePoint NFI 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 NFI SSP CA is published to the pointer location designated in the CRL Distribution Point Field of each certificate issued by that WidePoint NFI SSP CA and as described in Section 2 of the WidePoint NFI SSP CPS. Each superseded CRL for each WidePoint NFI SSP CA is archived to a folder by year and month on the WidePoint NFI SSP Repository to ensure a complete CRL history for each WidePoint NFI SSP CA.

WidePoint NFI SSP Certificate Authorities that are operated off-line are required to issue CRLs once every 35 days. New CRLs for off-line WidePoint NFI 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 35 days from "thisUpdate" field of the CRL.

CRLs are posted to webservers that use the HTTP protocol. CRL locations for each WidePoint NFI SSP CA is embedded in each certificate issued by that WidePoint NFI 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 NFI SSP website.

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

4.9.8 MAXIMUM LATENCY FOR CRLS

WidePoint NFI SSPs are configured to auto-issue a CRL every 6 hours, and each WidePoint NFI SSP CRL will be posted to the location for that corresponds to the value embedded in the CRLDP for each certificate issued by that WidePoint NFI SSP CA upon generation, but within no more than four hours after generation. Each WidePoint NFI 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 NFI SSP CA versus the publicly available CRL found at the CRLDP. If the CRL on the WidePoint NFI 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 NFI SSP Certificate Status Services (WidePoint NFI SSP CSSs), which are delegated trust OCSP responders, ensure that:

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

- Each WidePoint NFI SSP Certification Authority issues an OCSP Responder certificate according to the profile stipulated in Section 10.13.

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

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

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 NFI SSP supports CRLs. Client software using on-line revocation checking need not obtain CRLs.

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

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

4.9.11 Other Forms of Revocation Advertisements Available

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

4.9.12 Special Requirements Related to key Compromise

The WidePoint NFI SSP uses reason codes that specify the reason that a certificate has been revoked as part of the CRL created by each WidePoint NFI 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 NFI SSP CA.

For WidePoint NFI SSP Certificate Authorities, when a certificate is revoked because of compromise, or suspected compromise, of a private key, or that a previous revoked certificate reason code has been transitioned to compromise, an emergency CRL must be published within 18 hours after notification.

4.9.13 Circumstances for Suspension and Restoration

The WidePoint NFI SSP does not support certificate suspension for Certificate Authorities covered by this WidePoint NFI SSP CPS. WidePoint NFI 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 NFI 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 NFI 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 NFI SSP Card Management Systems or authorized agency Card Management Systems for certificates that have been issued as part of the PIV-Icredential issuance process and include the certificate policy of **id-orc-nfissp-pivi-hardware**, **id-orc-nfissp-pivi-cardAuth**, **id-orc-nfissp-mediumHardware,** or **id-orc-nfissp-medium** in the case of a PIV-I credential or **id-orc-nfissp-pivi-hardware**, **id-orc-nfissp-pivi-cardAuth**, **id-orc-nfissp-mediumHardware,** or **id-orc-nfissp-medium** policy in the case of a PIV-I credential or authorize the suspension directly through the WidePoint NFI SSP Certificate Authority that issued the certificate for WidePoint NFI SSP Subscriber certificates that were not issued through the WidePoint NFI SSP Card Management System or approved agency Card Management Systems and that assert a certificate policy of **id-orc-nfissp-medium, id-orc-nfissp-mediumHardware, id-orc-nfissp-mediumDevice,** or **id-orc-nfissp-mediumDeviceHardware.** WidePoint NFI SSP issued certificates asserting a certificate policy of **id-orc-nfissp-pivi-contentSigning** shall never be placed on suspension for any reason or any amount of time. All WidePoint NFI 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 NFI SSP Subscriber certificate serial numbers that have been restored from suspension will not be present on the next full CRL published by the WidePoint NFI SSP Certificate Authority that issued the WidePoint NFI 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 the case of WidePoint NFI SSP Subscriber certificates that have been issued as part of the PIV-Icredential issuance process and include the certificate policy of **id-orc-nfissp-pivi-hardware**, **id-orc-nfissp-pivi-cardAuth**, **id-orc-nfissp-mediumHardware,** or **id-orc-nfissp-medium** in the case of a PIV-I credential or **id-orc-nfissp-pivi-hardware**, **id-orc-nfissp-pivi-cardAuth**, **id-orc-nfissp-mediumHardware,** or **id-orc-nfissp-medium** in the case of a PIV-I credential documentation of request shall be recorded by the WidePoint NFI SSP CMS or approved organization CMS that is process the request. In the case of WidePoint NFI SSP Subscriber certificates that assert a certificate policy of **id-orc-nfissp-medium, id-orc-nfissp-mediumHardware, id-orc-nfissp-mediumDevice,** or **id-orc-nfissp-mediumDeviceHardware** 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 NFI SSP as proof of request and retained in accordance with the archive requirements as identified in Section 5.5.2 of this WidePoint NFI SSP CPS.

If a WidePoint NFI SSP Subscriber is requesting restoration of their suspended certificate, the identity of the WidePoint NFI SSP Subscriber shall be re-established before restoring the certificate. The WidePoint NFI SSP Subscriber's identity shall be re-established using processes defined in Section 3.2.3.1 of this WidePoint NFI 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 NFI SSP Subscriber.

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

4.9.16 Limits on Suspension Period

The maximum time period a WidePoint NFI SSP Subscriber certificate may be suspended is 100 calendar days. In the case of WidePoint NFI SSP Subscriber certificates that have been issued as part of the PIV-Icredential issuance process and include the certificate policy of **id-orc-nfissp-pivi-hardware**, **id-orc-nfissp-pivi-cardAuth**, **id-orc-nfissp-mediumHardware,** or **id-orc-nfissp-medium** in the case of a PIV-I credential or **id-orc-nfissp-pivi-hardware**, **id-orc-nfissp-pivi-cardAuth**, **id-orc-nfissp-mediumHardware,** or **id-orc-nfissp-medium** in the case of a PIV-I credential, the WidePoint NFI SSP Card Management Systems or authorized organization Card Management Systems will revoke any certificate that has not been restored from suspension within 100 calendar days of having been suspended. In the case of WidePoint NFI SSP Subscriber certificates that assert a certificate policy of **id-orc-nfissp-medium, id-orc-nfissp-mediumHardware, id-orc-nfissp-mediumDevice,** or **id-orc-nfissp-mediumDeviceHardware**, WidePoint Registration Authorities are responsible for revoking any certificates that were placed in suspension 100 days prior.

No WidePoint NFI SSP Subscriber certificates shall be published on a CRL with a reason code of “certificateHold” beyond the expiration date of the certificate.

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 NFI SSP operates Certificate Status Services (CSSs) using OCSP responders that provides revocation status. WidePoint NFI SSP CSSs practices (see below) conform to the stipulations of Federal Bridge Certificate Policy, applicable internet standards and this WidePoint NFI SSP CPS. All WidePoint NFI SSP CSSs updates, as well as any subsequent changes will be updated in this WidePoint NFI SSP CPS and submitted to the FPKIPA for conformance assessment. WidePoint NFI SSP CSSs practices include:

- Conformance to the stipulations of Federal Bridge Certificate Policy, applicable Internet Standards, and this WidePoint NFI SSP CPS.
- Ensuring that certificate and revocation information is accepted only from valid WidePoint NFI SSP Certificate Authorities.
- Only valid and appropriate responses.
- Maintaining evidence that due diligence is exercised in validating certificate status.
- WidePoint NFI SSP CSS certificates that conform to the OCSP Responder Certificate profile as specified in Section 10.13.
- WidePoint NFI 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 NFI SSP does not currently support SCVP.

4.10.1 Operational Characteristics

WidePoint NFI SSP CSSs will comply with the requirements of this WidePoint NFI SSP CPS and Federal Bridge Certificate Policy, as detailed in Section 4.10.

4.10.2 Service Availability

WidePoint NFI SSP CSSs maintain service availability through redundancy of equipment and redundancy of network services by striving to operate at 99% up-time annually.

4.10.3 Optional Features

WidePoint NFI 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 NFI SSP is synonymous with the validity period of the WidePoint NFI SSP Subscriber's certificate issued by a WidePoint NFI SSP CA. The subscription ends when the WidePoint NFI 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

The WidePoint NFI SSP supports key escrow and recovery for private keys associated with encryption certificates. The WidePoint NFI SSP does not support key recovery using key encapsulation techniques.

4.12.1 Key Escrow and Recovery Policy and Procedures

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

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

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

As part of the key escrow process, all Applicants and WidePoint NFI SSP Subscribers for whom the WidePoint NFI 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 NFI SSP Subscribers must use electronic means to request their own escrowed keys from the WidePoint NFI SSP. The WidePoint NFI SSP Subscriber may submit the request to a designated WidePoint Key Recovery Agent or a WidePoint Key Recovery Official. The WidePoint NFI SSP Subscriber will digitally sign the request using an WidePoint NFI SSP issued signature certificate of assurance level equal to or greater than that of the escrowed key.

WidePoint NFI SSP Subscribers may use the self-recovery process available as part of the WidePoint NFI SSP by presenting a current and valid WidePoint NFI SSP issued certificate to the WidePoint NFI SSP self-recovery portal. The WidePoint NFI SSP self-recovery portal delivers the recovered key to the WidePoint NFI SSP Subscriber in p12 format through the authenticated session after performing all of the following:

- Verifying that the authenticated identity of the requestor is the same as the WidePoint NFI SSP Subscriber associated with the escrowed keys being requested.

- Ensuring that the escrowed keys are being sent only to the authenticated WidePoint NFI SSP Subscriber associated with the escrowed keys; and,
- Ensuring that the recovered keys are encrypted by a strong password provided by the WidePoint NFI SSP Subscriber in accordance with Section 6.4.1 of this WidePoint NFI SSP CPS during the self-recovery process and that the self-recovery session is conducted through a TLS session established between the WidePoint NFI SSP self-recovery portal and the appropriate WidePoint NFI SSP CA in accordance with Section 6.2.6 of this WidePoint NFI SSP CPS.

WidePoint NFI SSP Subscribers may submit a request signed by hand to a WidePoint Registration Authority or a WidePoint NFI SSP Key Recovery Official. The WidePoint Registration Authority or WidePoint NFI SSP Key Recovery Official must validate the identity of the requestor. WidePoint NFI 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 NFI SSP PIV-I credential to the WidePoint NFI 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 NFI SSP Subscriber via hand delivery or through certified mail. The password, which is generated in accordance with Section 6.4.1 of this WidePoint NFI 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 NFI 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 NFI 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 NFI SSP CPS.

WidePoint NFI SSP Subscribers who have WidePoint NFI SSP 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 NFI SSP PIV-I credential issuances recovered to their new WidePoint NFI SSP PIV-I credential. The previously escrowed encryption keys will be recovered and each placed into a separate container of the newly issued WidePoint NFI SSP 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 NFI SSP PIV-I credentials will hold up to five previously escrowed encryption keys from WidePoint NFI SSP PIV-I credentials. PIV-I Card stock may be acquired that could recover up to 20 previously escrowed keys from WidePoint NFI SSP PIV-I credentials. Note: the issuance process for WidePoint NFI SSP PIV-I credentials is controlled and secured by a WidePoint NFI SSP CMS and only permits recovery of encryption keys issued through a WidePoint NFI SSP CMS issuance process.

Third party requestors must use electronic means to request the WidePoint NFI 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 Federal Bridge Certificate 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 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 NFI SSP PIV-I credential to the WidePoint NFI 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 requestor via hand delivery or through certified mail. The password, which is generated in accordance with Section 6.4.1 of this WidePoint NFI 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 NFI 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, requestor and their affiliation, the WidePoint NFI SSP Subscriber that is subject to the request, the document authorizing the request and the authorizing entity, 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 NFI SSP CPS. If possible, a copy of the document authorizing the request (i.e., a court order or other legally binding document) is scanned in with the WidePoint Key Recovery Witness Statement and placed in archive as specified in Section 5.5 of this WidePoint NFI SSP CPS.

Third party requestors shall be bound, by legal means and the stipulations of this WidePoint NFI SSP CPS and Federal Bridge Certificate 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 NFI SSP encryption key associated with the WidePoint NFI 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 NFI SSP Registration Authority or WidePoint NFI 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.”

4.12.1.2.1 Key Recovery Through WidePoint NFI SSP Key Recovery Agent

WidePoint NFI SSP Subscribers may submit a request signed by hand to a WidePoint Registration Authority or a WidePoint NFI SSP Key Recovery Official. The WidePoint Registration Authority or WidePoint NFI SSP Key Recovery Official must validate the identity of the requestor. WidePoint NFI 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 NFI SSP PIV-I credential to the WidePoint NFI 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 NFI SSP Subscriber via hand delivery or through certified mail. The password, which is generated in accordance with Section 6.4.1 of this WidePoint NFI 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 NFI 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 NFI 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 NFI SSP CPS.

4.12.1.2.2 Automated Self-Recovery

WidePoint NFI SSP Subscribers may use the self-recovery process available as part of the WidePoint NFI SSP by presenting a current and valid WidePoint NFI SSP issued certificate to the WidePoint NFI SSP self-recovery portal. The WidePoint NFI SSP self-recovery portal delivers the recovered key to the WidePoint NFI SSP Subscriber in p12 format through the authenticated session after performing all of the following:

- Verifying that the authenticated identity of the requestor is the same as the WidePoint NFI SSP Subscriber associated with the escrowed keys being requested.
- Ensuring that the escrowed keys are being sent only to the authenticated WidePoint NFI SSP Subscriber associated with the escrowed keys; and,
- Ensuring that the recovered keys are encrypted by a strong password provided by the WidePoint NFI SSP Subscriber in accordance with Section 6.4.1 of this WidePoint NFI SSP CPS during the self-recovery process and that the self-recovery session is conducted through a TLS session established between the WidePoint NFI SSP self-recovery portal and the appropriate WidePoint NFI SSP CA in accordance with Section 6.2.6 of this WidePoint NFI SSP CPS.

4.12.1.2.3 Key Recovery During Token Issuance

When a WidePoint NFI SSP Subscriber is issued a new certificate on a hardware token, private key management keys for the WidePoint NFI SSP Subscriber can be recovered as part of the issuance process by authenticating to the appropriate WidePoint NFI SSP Key Encryption Database that holds the past encryption keys for the WidePoint NFI SSP Subscriber. This is done using the Global Platform Secure Channel Protocol as part of the WidePoint NFI SSP Subscriber PIV-I issuance process to inject the key history onto the hardware token directly. Up to twenty past key encryptions may be injected to the new WidePoint NFI SSP Subscriber's new PIV-I credential.

4.12.1.2.4 Key Recovery by Data Decryption Server

A WidePoint NFI SSP Data Decryption Server or organization Data Decryption Server is maintained under two-person control, as is required for any WidePoint NFI SSP Certificate Authority or WidePoint NFI SSP Key Encryption Database. A WidePoint NFI SSP Data Decryption Server or organization Data Decryption Server has permission to automatically recover keys from a WidePoint NFI SSP Key Encryption Database. The WidePoint NFI SSP Key Encryption Database performs the following activities prior to releasing the key:

- Authenticating the Requestor as a legitimate WidePoint NFI SSP Data Decryption Server or organization Data Decryption Server.
- Verifying that the WidePoint NFI SSP Data Decryption Server or organization Data Decryption Server is authorized to recover the escrowed key for the Issuing Organization to which the key belongs.
- Ensuring that the escrowed keys are protected during transmission using cryptography or other means of equal or greater strength than provided by the escrowed keys.

In order to prevent any individual WidePoint NFI SSP Key Recovery Agent, Key Recovery Official or another trusted role from accessing WidePoint NFI SSP Subscriber encryption keys, a combination of physical, procedural, and technical security controls are used to enforce continuous two-person control on the WidePoint NFI SSP Data Decryption Servers or organization Data Decryption Servers. The WidePoint NFI SSP Data Decryption Servers or organization Data Decryption Servers are designed to maximize the ability to enforce two-person control

technically and comply with the specifications set forth in Section 5.1.2.5 of this WidePoint NFI SSP CPS whether they reside within WidePoint's physical secure location or the owner organization.

4.12.1.3 Who can Submit a Key Recovery Application

WidePoint NFI SSP Subscribers may request recovery of their own escrowed keys either through contact a WidePoint Registration Authority or via an automated process directly from the WidePoint NFI SSP CA that escrowed the encryption private key.

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

An Internal requestor is the WidePoint NFI SSP PKI Point of Contact for the organization or a requestor who is in the supervisory chain of the organization to which the WidePoint NFI SSP Subscriber is or was affiliated.

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

4.12.1.4 Requestor Authorization Validation

A WidePoint NFI SSP Key Recovery Agent or a WidePoint NFI SSP Key Recovery Official, as an intermediary for the WidePoint NFI SSP Key Recovery Agent, validates the authorization of the Requestor in consultation with the WidePoint NFI SSP management and/or legal counsel, as appropriate.

An external requestor must work with an internal requestor unless the law requires the WidePoint NFI SSP to release the WidePoint NFI SSP Subscriber's private key without approval of the WidePoint NFI SSP Subscriber and their organization. Nothing in this document is intended to change the current procedures for obtaining information about individuals in connection with such requests.

4.12.1.5 WidePoint NFI SSP Subscriber Authorization Validation

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

4.12.1.6 WidePoint NFI SSP Key Recovery Agent Authorization Validation

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

4.12.1.7 WidePoint NFI SSP Key Recovery Official Authorization Validation

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

4.12.1.8 Data Decryption Server Authorization Validation

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

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

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

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

The WidePoint NFI SSP consists of equipment dedicated to the operations of all WidePoint NFI SSP CAs, WidePoint NFI SSP CMSs, WidePoint NFI SSP RA workstations, WidePoint NFI SSP CSSs, WidePoint NFI SSP Hardware Security Modules, hereafter referred to as WidePoint NFI SSP HSMs, and WidePoint NFI SSP Firewall and Networking Equipment. WidePoint NFI 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 NFI SSP in accordance with this WidePoint NFI SSP CPS and Federal Bridge Certificate Policy. Databases and directories located on WidePoint NFI SSP equipment will not be accessible to Applicants, WidePoint NFI SSP Subscribers or Relying Parties.

WidePoint NFI SSP CMS equipment is dedicated for the sole purpose of issuance of WidePoint NFI SSP 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 CA Equipment

<REDACTED>

5.1.2.2 Physical Access for WidePoint NFI SSP Registration Authority Equipment

<REDACTED>

5.1.2.3 Physical Access for WidePoint NFI SSP Certificate Status Services Equipment

<REDACTED>

5.1.2.4 Physical Access for WidePoint NFI SSP CMS Equipment

<REDACTED>.

5.1.2.5 Physical Access for WidePoint Key Encryption Database Equipment

<REDACTED>.

5.1.2.6 Physical Access for WidePoint NFI SSP or organization Data Decryption Server Equipment

<REDACTED>.

5.1.2.7 Physical Access for WidePoint NFI SSP Key Recovery Agent or Key Recovery Official Equipment

<REDACTED>.

5.1.3 POWER AND AIR CONDITIONING

<REDACTED>

5.1.4 WATER EXPOSURE

<REDACTED>

5.1.5 MEDIA STORAGE

<REDACTED>.

5.1.6 WASTE DISPOSAL

<REDACTED>.

5.1.7 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 principals 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 NFI SSP systems, “Moderate” for roles that can act as gateways that enable “High” risk roles to interact with the WidePoint NFI SSP systems, or “Low” for roles that do not interact with any of the WidePoint NFI 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 WidePoint Key Recovery Agent (KRA)

<REDACTED>.

5.2.1.6 Other Trusted Roles

5.2.1.6.1 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.
- Social Security trace must show that the person has a valid social security number,
- Verification of authorization to work in the United States.
- Place of residence.

The results of these checks will not be released except as required by Section 9.4.4 of this WidePoint NFI SSP CPS and Federal Bridge Certificate Policy.

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

5.3.7 <REDACTED>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>

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

This WidePoint NFI SSP CPS does not preclude any source of key that has been generated in accordance with the stipulations of this WidePoint NFI SSP CPS, the WidePoint NFI SSP CP, the Federal Bridge Certificate 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 NFI SSP.

A private key is considered to be generated by the entity that first comes into possession of it: a WidePoint NFI SSP Subscriber, a WidePoint Registration Authority, or a WidePoint NFI SSP Certificate Authority.

A private key associated with a WidePoint NFI SSP Subscriber certificate may not appear outside of the module in which it was generated unless it is encrypted for local transmission or for processing and storage by a key recovery mechanism.

6.1.1.1 WidePoint NFI SSP Certificate Authority Key Pair Generation

<REDACTED>.

6.1.1.2 WidePoint NFI SSP Subscriber Key Pair Generation

<REDACTED>.

6.1.1.3 WidePoint NFI SSP Certificate Status Services Key Pair Generation

<REDACTED>

6.1.1.4 WidePoint PIV-I Content Signing Key Pair Generation

<REDACTED>.

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER

In accordance with this WidePoint NFI SSP CPS, in all cases except encryption, the key is generated directly on the WidePoint NFI SSP Subscriber's token. The WidePoint NFI 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 NFI SSP generates the private key in the hardware security module of the WidePoint NFI SSP CA and stores and encrypts the key in the WidePoint NFI SSP CA's internal database.

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

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

<REDACTED>.

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

The WidePoint NFI SSP will deliver the Federal Bridge Certificate Policy CA and WidePoint NFI SSP CA public keys via a web interface to a protected server using SSL. The WidePoint NFI 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 Federal Bridge Certificate Policy CA and WidePoint NFI 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 Federal Bridge Certificate Policy CA and WidePoint NFI 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 NFI SSP CPS, the WidePoint NFI SSP will provide the Federal Bridge Certificate Policy CA to WidePoint NFI SSP Subscribers.

6.1.5 KEY SIZES

This WidePoint NFI SSP CPS requires use of RSA PKCS #1, RSASSA-PSS, or ECDSA signatures; additional restrictions on key sizes and hash algorithms are detailed below. Certificates must contain 2048-, 3072-, or 4096-bit RSA keys, or 256- or 384-bit elliptic curve keys.

	WidePoint NFI SSP Certificate Authority certificates that expire on or before December 31, 2030	**WidePoint NFI SSP Certificate Authority certificates that expire on or before December 31, 2030**
Minimum Key Size	RSA: 2048 Elliptic Curve: 256	RSA: 3072 Elliptic Curve: 256
Hash Algorithm	SHA-256, SHA-384, or SHA-512	SHA-256, SHA-384, or SHA-512

	WidePoint NFI SSP Subscriber certificates that expire on or before December 31, 2030	**WidePoint NFI SSP Subscriber certificates that expire on or before December 31, 2030**
Minimum Key Size	RSA: 2048 Elliptic Curve: 256	RSA: 3072 Elliptic Curve: 256
Hash Algorithm	SHA-256, SHA-384, or SHA-512	SHA-256, SHA-384, or SHA-512

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

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

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

WidePoint NFI SSP KED and WidePoint NFI 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 NFI SSP CPS and Federal Bridge Certificate 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 NFI SSP key pairs whose public components are to be certified by the WidePoint NFI 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 NFI SSP Certificate Authorities perform partial key validation as specified in NIST SP 800-89 (section 5.3.3).

For WidePoint NFI SSP Certificate Authorities that use ECC, public keys will fall within curves defined in Section 7.1.3 of this WidePoint NFI SSP CPS. Additionally, the WidePoint NFI 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 NFI 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 NFI SSP CPS.

WidePoint NFI SSP certificates to be used for authentication only set the digitalSignature bit of the Key Usage Extension.

WidePoint NFI 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 NFI SSP certificates that have the nonRepudiation bit set, must not have keyEncipherment bit or keyAgreement bit set of the Key Usage Extension.

WidePoint NFI SSP certificates to be used for encryption (RSA) set the keyEncipherment bit of the Key Usage Extension.

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

Keys associated with WidePoint NFI 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-orc-nfissp-pivi-hardware**,or **id-orc-nfissp-pivi-cardAuth** are used solely for authentication.

Medium Assurance Level certificates may include a single key for use with encryption and signature in support of legacy applications. Such dual-use certificates must be generated and managed in accordance with their respective signature certificate requirements, except where otherwise noted in this WidePoint NFI SSP CP. Such dual-use certificates must never assert the nonrepudiation key usage bit and must not be used for authenticating data that will be verified on the basis of the dual-use certificate at a future time. Entities are encouraged at all levels of assurance to issue WidePoint NFI SSP Subscribers two key pairs, one for key management and one for digital signature and authentication.

For all WidePoint NFI 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 NFI SSP certificates that assert **id-orc-nfissp-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]).

WidePoint NFI SSP or Organization PIV-I Card Authentication certificates must include a critical Extended Key Usage extension that asserts id-piv-cardAuth {2.16.840.1.101.3.6.8}.

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 NFI SSP is FIPS140-3 Security Requirements for Cryptographic Modules. All WidePoint NFI 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 NFI 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 NFI SSP issued certificates at the Medium Assurance level as defined in Section 1.4.1.4 and throughout this WidePoint NFI SSP CPS. The browser-based process for requesting Medium Assurance certificates from the WidePoint NFI SSP website performs a check of the Applicant or WidePoint NFI SSP Subscriber's browser to ensure a compliant browser is being used. If an Applicant or a WidePoint NFI SSP Subscriber is using a non-compliant browser, a message notifies the Applicant or WidePoint NFI 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 NFI SSP certificates that are issued for this level may only assert a certificate policy object identifier of **id-orc-nfissp-medium** or **id-orc-nfissp-mediumDevice**.

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

WidePoint NFI SSP 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 201-3) 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 NFI SSP PIV-I Credentials for up to one year after GSA approved replacement card stock is available. WidePoint NFI SSP PIV-I Credentials issued using a card stock that has been deprecated may continue to be used until the current WidePoint NFI SSP Subscriber certificates expire unless otherwise notified by the Federal PKI Policy Authority or the DoD FPKIPA. On an annual basis, each WidePoint NFI SSP CMS will submit one sample WidePoint NFI SSP PIV-I Credential that has been issued through its configuration and shall submit the sample WidePoint NFI 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 NFI SSP and incorporated into the necessary documentation.

WidePoint NFI 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 NFI SSP CMS. The hardware security modules and hardware tokens used by WidePoint have attained FIPS 140-3 Level 2 validation.

All WidePoint NFI SSP issued certificates will be signed by a WidePoint NFI 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 NFI SSP CSS private keys are protected by a hardware security module validated at FIPS 140-3 Level 2.

WidePoint NFI SSP Certificate Authority Administrators, WidePoint Registration Authorities, and WidePoint NFI SSP Local Registration Authorities are issued WidePoint NFI 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 NFI SSP PIV-I Credentials whose card stock that has been tested and approved by the Personal Identity Verification (PIV) of Federal Employees and Contractors, (FIPS 201-3) Evaluation Program and listed on the GSA Approved Products List (APL). WidePoint NFI SSP PIV-I credentials issued using deprecated card stock may continue to be used until the current WidePoint NFI 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 NFI SSP CA, WidePoint NFI SSP CMS or a WidePoint NFI SSP CSS equipment.

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

Note that Section 6.1.1 of this WidePoint NFI 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 NFI SSP Certificate Authorities WidePoint Key Encryption Database WidePoint Data Decryption Service	3
WidePoint Certificate Status Services	2
WidePoint NFI SSP PIV-I Content Signing ➢ id-orc-nfissp-pivi-contentSigning	2
WidePoint NFI SSP Subscriber Hardware Signature and Authentication ➢ id-orc-nfissp-pivi-hardware ➢ id-orc-nfissp-pivi-cardAuth ➢ id-orc-nfissp-mediumHardware	2
WidePoint NFI SSP Subscriber Hardware Key Management ➢ id-orc-nfissp-mediumHardware	2
WidePoint NFI SSP Subscriber Hardware Device ➢ id-orc-nfissp-mediumDeviceHardware	2
WidePoint NFI SSP Subscriber Software Signature and Authentication ➢ id-orc-nfissp-medium	1
WidePoint NFI SSP Subscriber Software Key Management ➢ id-orc-nfissp-medium	1
WidePoint NFI SSP Subscriber Software Key Management ➢ id-orc-nfissp-mediumDevice	1

6.2.1.1 *Custodial Subscriber Key Stores*

The WidePoint NFI SSP does use or support Custodial Subscriber Key Stores.

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

Activation of WidePoint NFI SSP CA signature keys, WidePoint NFI 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 NFI SSP CA or WidePoint NFI 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 NFI SSP system Access Control Family Control AC-2 Account Management for logical access. Access to WidePoint NFI SSP Certification Authorities signature keys and the WidePoint NFI SSP CSS signature keys backed up for disaster recovery requires the same two-person control as the operational WidePoint NFI SSP CA signature keys and the WidePoint NFI SSP CSS signature keys.

WidePoint NFI SSP Subscriber private encryption keys requested by anyone other than the WidePoint NFI SSP Subscriber or the WidePoint NFI SSP PKI Point of Contact may only be extracted from the WidePoint NFI SSP CA key recovery databases under two-person control as specified in in Section 4.12.2.3 of this WidePoint NFI SSP CPS, namely one WidePoint Key Recovery Agent and one WidePoint Key Recovery Official. WidePoint NFI 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 NFI SSP, and this WidePoint NFI 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 NFI SSP CPS.

6.2.3 PRIVATE KEY ESCROW

Under no circumstances will a non-repudiation signature key be escrowed or held in trust by a third party other than the WidePoint NFI SSP Subscriber.

For some purposes (such as data recovery) some WidePoint NFI SSP Subscriber organizations may desire key escrow and key retrieval for the private component of the encryption certificate key pair. To facilitate this, the WidePoint NFI SSP offers a key escrow and recovery capability which is described in Section 4.12 of this WidePoint NFI SSP CPS.

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 NFI SSP CPS.

6.2.4 PRIVATE KEY BACKUP

For WidePoint NFI SSP Subscriber certificates that assert a certificate policy OID of **id-orc-nfissp-pivi-hardware**, **id-orc-nfissp-pivi-cardAuth**, or **id-orc-nfissp-mediumHardware** WidePoint NFI SSP Subscribers are notified that private signature keys may not be backed up or copied.

For WidePoint NFI SSP Subscriber certificates that assert a certificate policy OID of **id-orc-nfissp-medium** the WidePoint NFI SSP recommends to WidePoint NFI 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 NFI SSP Subscribers are also advised that backup of private signature keys for the sole purpose of key recovery may not be made.

WidePoint NFI SSP Subscribers are permitted to make operational copies of private keys residing in software cryptographic modules for each of the WidePoint NFI 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 NFI 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 NFI SSP Subscriber or WidePoint NFI 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 NFI SSP CA and WidePoint NFI SSP CSS private signature keys and WidePoint NFI 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 NFI 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 NFI SSP CAs, WidePoint NFI SSP CSSs and WidePoint NFI SSP CMSs.

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

Private Key	Backup
WidePoint NFI SSP Certificate Authorities WidePoint Key Encryption Database WidePoint Data Decryption Service	Required
WidePoint Certificate Status Authorities	Optional
WidePoint NFI SSP PIV-I Content Signing ➢ id-orc-nfissp-pivi-contentSigning	Optional
WidePoint NFI SSP Subscriber Hardware Signature and Authentication ➢ id-orc-nfissp-pivi-hardware ➢ id-orc-nfissp-pivi-cardAuth ➢ id-orc-nfissp-mediumHardware	Not Permitted
WidePoint NFI SSP Subscriber Hardware Key Management ➢ id-orc-nfissp-mediumHardware	Required
WidePoint NFI SSP Subscriber Hardware Device ➢ id-orc-nfissp-mediumDeviceHardware	Optional
WidePoint NFI SSP Subscriber Software Signature and Authentication ➢ id-orc-nfissp-medium	Optional *
WidePoint NFI SSP Subscriber Software Key Management ➢ id-orc-nfissp-medium	Required
WidePoint NFI SSP Subscriber Software Device ➢ id-orc-nfissp-mediumDevice	Optional

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

6.2.5 Private Key Archival

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

WidePoint NFI SSP Certificate Authorities that retain WidePoint NFI SSP Subscriber private encryption keys for business continuity purposes archive the escrowed WidePoint NFI 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 NFI 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 NFI SSP CAs, the cryptographic module must be a FIPS 140-3 Level 3 module (or higher). For WidePoint NFI SSP CSSs and WidePoint NFI SSP CMSs, the cryptographic module must be a FIPS 140-3 Level 2 module (or higher). For WidePoint NFI SSP Subscriber certificates that assert a certificate policy OID of **id-orc-nfissp-pivi-hardware**, **id-orc-nfissp-pivi-cardAuth,** or **id-orc-nfissp-mediumHardware,** the cryptographic module must be a FIPS 140-3 Level 2 module (or higher). For WidePoint NFI SSP Subscriber certificates that assert a certificate policy OID of **id-orc-nfissp-medium**, the cryptographic module must be a FIPS 140-3 Level 1 module (or higher).

At no time are WidePoint NFI SSP CMS Master Keys and Diversified Keys exposed in plaintext outside of the hardware security module or the WidePoint NFI SSP PIV-I Credential associated with the key. WidePoint NFI 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 NFI SSP CA.

Backup of WidePoint NFI SSP hardware security modules is handled through the WidePoint NFI 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 NFI 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-orc-nfissp-pivi-hardware ➢ id-orc-nfissp-medium ➢ id-orc-nfissp-mediumHardware ➢ id-orc-nfissp-pivi-hardware	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-orc-nfissp-mediumDevice ➢ id-orc-nfissp-mediumDeviceHardware	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-orc-nfissp-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-I issuance requirements (see [FIPS 201]). The strength of the security controls must be commensurate with the level of threat in the PIV-I credential issuance system's environment, and must protect the hardware, software, and the cryptographic token and its activation data from compromise.
➢ id-orc-nfissp-pivi-cardAuth	None

6.2.9 Method of Deactivating Private key

<REDACTED>.

6.2.10 Method of Destroying Private Key

Private keys associated with the certificates of the WidePoint NFI SSP are destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, this can be accomplished by removing the private keys from the browser through the cryptographic service provider's method of deletion. For hardware cryptographic modules, this will be executing a "zeroize" command (when the PIN or unlock code are known). Physical destruction of hardware is not required unless the PIN or unlock code are not known.

6.2.11 Cryptographic Module Rating

Requirements for cryptographic modules are as stated above in Section 6.2.1 of this WidePoint NFI 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

The key usage periods for keying material are described in Section 4.7 and Section 5.6 of this WidePoint NFI SSP CPS.

6.3.3 Subscriber Private Key Usage Environment

WidePoint NFI 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

All WidePoint NFI SSP Subscriber certificates or credentials are protected by either a password or a PIN that is in compliance with FIPS 140-3.

The password will be in compliance with Section 6.2.8 of this WidePoint NFI SSP CPS. In addition, WidePoint NFI 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 NFI SSP Subscriber, as stipulated in the subscriber's agreement.

WidePoint NFI SSP Subscribers who receive WidePoint NFI SSP PIV-I credentials are directed to protect their credential with a PIN that must be 6-8 digits at a minimum. WidePoint NFI SSP Subscribers who receive WidePoint NFI SSP 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.

WidePoint NFI SSP Subscribers who receive end entity certificates other than WidePoint NFI SSP PIV-I credentials use passwords to protect the private keys of the WidePoint NFI 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 NFI SSP does not permit password or PIN generation by anyone other than the WidePoint NFI 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 NFI SSP Subscriber. The password or PIN is known only to the WidePoint NFI SSP Subscriber.

6.4.2 ACTIVATION DATA PROTECTION

Only WidePoint Certificate Authority Administrators are authorized to know and employ the signing key password for WidePoint NFI SSP CAs and WidePoint NFI 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 NFI SSP CAs, WidePoint NFI SSP CMSs, and WidePoint NFI 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 NFI SSP system being activated.

Activation data protection for WidePoint NFI 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 NFI 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 NFI SSP 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 NFI SSP Subscribers who have a PIV-I credential that is locked due to failed login attempts must appear before WidePoint Registration Authorities to perform a PIN reset.

6.4.3 Other Aspects of Activation Data

The activation data for WidePoint NFI SSP CAs, WidePoint NFI SSP CMSs, and WidePoint NFI 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 NFI 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 NFI SSP Subscriber against the biometrics collected in Section 3.2.3.1 of this WidePoint NFI 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 NFI SSP will issue X.509 Version 3 certificates.

7.1.2 CERTIFICATE EXTENSIONS

WidePoint NFI SSP certificate profiles are in accordance with the requirements of the certificate profiles described in Federal Bridge Certificate Policy.

WidePoint NFI 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 NFI 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 NFI 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 NFI SSP CSS OCSP responses.

For WidePoint NFI 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 NFI 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 NFI 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 NFI SSP encodes all WidePoint NFI SSP CA Distinguished Names (in various fields, e.g., Issuer, Subject, Subject Alternative Name, Name constraints) as printable strings. The WidePoint NFI SSP encodes all subscriber DN portions that name constraints apply to as printable strings. For other portions of the subscriber DN, the WidePoint NFI 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 NFI SSP encodes all domain component attribute values as an IA5 string.

7.1.5 NAME CONSTRAINTS

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

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER

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

Certificates that express the **id-orc-nfissp-pivi-cardAuth** or **id-orc-nfissp-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 NFI 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 NFI SSP may contain the following policy qualifiers: WidePoint NFI SSP CPS pointer.

7.1.9 PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES EXTENSION

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

WidePoint NFI SSP Certificate Authorities operating under this WidePoint NFI SSP CPS and the Federal Bridge Certificate Policy CP must have a compliance audit mechanism in place to ensure that the requirements of this WidePoint NFI SSP CPS are being implemented and enforced. The WidePoint NFI 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-I 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 NFI 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 NFI SSP CPS. The WidePoint NFI 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 NFI SSP acknowledges the FPKIPA's right to require periodic and aperiodic inspections and compliance audits of the WidePoint NFI SSP CMA facility to validate that the WidePoint NFI SSP CMAs are operating in accordance with the security practices and procedures set forth in this WidePoint NFI SSP CPS.

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

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

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

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The compliance auditor is an independent entity who has a contractual relationship with WidePoint NFI SSP to perform the compliance audit. The WidePoint NFI SSP also performs internal audits of all WidePoint NFI SSP systems to verify compliance with this WidePoint NFI 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 NFI SSP has in place a system to assure the quality of the WidePoint NFI SSP services that it provides, and that it complies with all of the requirements of Comon Policy and this WidePoint CPS. All aspects of the WidePoint NFI SSP operation as specified in thisWidePoint CPS are subject to audit compliance inspection.

Any discrepancies between a WidePoint NFI 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 NFI SSP will determine a time for completion.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

When a compliance auditor finds a discrepancy between a WidePoint CMA's operation and the stipulations of this CPS, 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 NFI SSP will propose a remedy, including expected time for completion, to the FPKIPA.

Any remedy may include permanent or temporary WidePoint NFI SSP cessation or termination of the WidePoint NFI 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 NFI SSP as soon as possible to limit the risks created. The FPKIPA and the WidePoint NFI SSP will determine a time for completion. The implementation of remedies will be coordinated between the FPKIPA and the WidePoint NFI SSP and subsequently communicated to the appropriate authority. A special audit 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 NFI SSP and to the FPKIPA by the WidePoint NFI SSP. The WidePoint NFI 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 NFI SSP entity is found not to be in compliance with this WidePoint CPS, or the policy identified in Federal Bridge Certificate Policy, the WidePoint NFI SSP will notify the FPKIPA immediately upon completion of the audit.

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 NFI SSP to issue WidePoint NFI SSP certificates to WidePoint NFI SSP Subscribers for all credential and certificate types and profiles as described throughout this WidePoint NFI SSP CPS. Fees are published in WidePoint's GSA Schedule #47QTCA19D009F.

9.1.2 CERTIFICATE ACCESS FEES

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

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEES

WidePoint NFI 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 NFI 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

All sales are final upon acceptance of the issued certificate by the WidePoint NFI SSP Subscriber. No refund shall be given unless the WidePoint NFI SSP Subscriber certificate in question has been shown to be out of compliance with this WidePoint NFI SSP CP or the Federal Bridge Certification Authority CP. WidePoint NFI SSP certificates are issued in accordance with this WidePoint NFI CPS and the WidePoint NFI SSP CP at the time of the certificate issuance. The Applicant or WidePoint NFI SSP Subscriber is responsible for verifying from the Relying Party Application that the particular type of WidePoint NFI SSP certificate and the Assurance Level of that certificate to be purchased is the correct certificate and Assurance Level that the Applicant or WidePoint NFI SSP Subscriber needs to authenticate to that Relying Party. The WidePoint NFI SSP may, from time to time, provide guidance as to the type of certificate and Assurance Level that a Relying Party Application may need, but the WidePoint NFI SSP makes no claim that the information is current and or accurate at the time the Applicant or WidePoint NFI SSP Subscriber views that information. The WidePoint NFI SSP makes no claim that the Relying Party Application will accept a WidePoint NFI SSP Subscriber certificate that is issued at a higher Assurance Level than what the Relying Party Application currently accepts nor does the WidePoint NFI SSP claim that any WidePoint NFI SSP certificate type or Assurance Level will grant the WidePoint NFI SSP Subscriber access to the Relying Party. Access to the Relying Party Application and the information contained within and the validation that the WidePoint NFI SSP Subscriber accessing that Relying Party Application is current and not revoked is at the sole discretion of the Relying Party Application and that any legitimate, benign, or malevolent access to that information by a WidePoint NFI SSP Subscriber certificate is the responsibility of the Relying Party Application and the Relying Party Application shall have no claim against the WidePoint NFI SSP unless the issuance of that certificate has been shown to be out of compliance with this WidePoint NFI SSP CPS, the WidePoint NFI SSP CP or the Federal Bridge Certification Authority CP. No refund shall be given for any unused portion of the validity period of a WidePoint NFI SSP Subscriber certificate nor shall any unused portion of the validity period be transferred to a different WidePoint NFI SSP Subscriber certificate or provide a discount on a replacement WidePoint NFI SSP Subscriber certificate. Additionally, the WidePoint NFI SSP makes no claim that the Relying Party accepts, shall continue to accept, or will accept, a WidePoint NFI SSP certificate type and/or Assurance Level in perpetuity or that the WidePoint NFI SSP knows the full extent as to which Relying Party Applications accept, did accept or no longer accept, WidePoint NFI SSP Subscriber certificates. No refund shall be granted in the event that this WidePoint NFI SSP CPS, the WidePoint NFI SSP CP or the Federal Bridge Certification Authority CP is revised post-issuance of the WidePoint NFI SSP Subscriber certificate. No refund shall be granted in the event that regulatory bodies change or update their

requirements regarding digital certificates or any aspect of digital certificate use. This includes, but is not limited to, entities such as the CAB-FORUM for browser and webserver requirements, application vendors to include but not limited browsers and webservers, operating system vendors, and physical access vendors using card based authentication for WidePoint NFI SSP Subscribers. No refund shall be granted to either the WidePoint NFI SSP Subscriber or the Subscriber's organization if the WidePoint NFI SSP Subscriber changes their organization affiliation or their role within the organization. No refund shall be granted in the event the private keys related to WidePoint NFI SSP Subscriber certificates are destroyed by malfunctioning Subscriber-owned hardware or software to include but not limited to all workstations, servers, card readers, appliances and applications. No refund shall be granted in the event that the FPKIPA decides to terminate the operation of the Federal Bridge Certification Authorities. In the event that the FPKIPA decides to terminate the operation of the Federal Bridge Certification Authorities, WidePoint shall work with the WidePoint NFI SSP Subscriber to transition the Subscriber to another suitable WidePoint program that meets their requirements for interoperability with the DoD and their applications but that no transfer of remaining value of the WidePoint NFI SSP credential shall be applied to the new credential. Conditions not described above shall be brought to the attention of the WidePoint NFI SSP PMA for resolution and determination of the refund requested. The WidePoint NFI SSP Refund Policy shall be continuously updated and revised to address any new stipulations required as a result of further adoption by the Relying Party Application and the WidePoint NFI SSP community.

This section, 9.1.5 Refund Policy, of this WidePoint NFI SSP CPS and the WidePoint NFI SSP CP shall be referenced in all WidePoint NFI SSP Subscriber agreements.

9.2 FINANCIAL RESPONSIBILITY

This WidePoint NFI SSP CPS contains no limits on the use of any certificates issued by the WidePoint NFI SSP or Organization. Rather, entities acting as Relying Parties must determine what financial limits, if any, they wish to impose for certificates used to complete a transaction.

9.2.1 INSURANCE COVERAGE

Each of WidePoint Corporation and subsidiaries, Relying Party Applications, and the Subscriber Organization or Subscriber themselves if unaffiliated shall maintain, at its sole cost and expense, commercial insurance in types and amounts that are believed by it to be commercially reasonable for its business and operations. Each party shall provide the other party written evidence of such insurance upon reasonable request.

9.2.2 OTHER ASSETS

Each party shall be responsible for its own assets and ensuring that any certificates issued under this CPS are compatible with its own systems and operations.

9.2.3 INSURANCE OR WARRANTY COVERAGE FOR END-ENTITIES

WidePoint provides no insurance or warranty coverage for end-entities. Each party is required to maintain the insurance set forth in Section 9.2.1.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 SCOPE OF BUSINESS CONFIDENTIAL INFORMATION

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

9.3.2 INFORMATION NOT WITHIN THE SCOPE OF BUSINESS CONFIDENTIAL INFORMATION

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

9.3.3 RESPONSIBILITY TO PROTECT BUSINESS CONFIDENTIAL INFORMATION

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

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 PRIVACY PLAN

The WidePoint NFI 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 NFI SSP Subscriber information is collected and maintained within the secure WidePoint NFI SSP environment as described in this WidePoint NFI SSP CPS and the WidePoint System Security Plan. Hard-copy Applicant and WidePoint NFI SSP Subscriber information is collected and maintained at the WidePoint NFI SSP facility in Fairfax, VA in secure containers. Archived hard-copy subscriber information is either maintained within the WidePoint NFI SSP facility Fairfax, VA facility or in an off-site storage facility as described in Section 5.5.2 of this WidePoint NFI SSP CPS.

9.4.2 INFORMATION TREATED AS PRIVATE

Information requested from Applicants or WidePoint NFI 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 NFI SSP CPS and is subject to the Privacy Act of 1974 {P.L. 093-579}. All information in the WidePoint NFI 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 NFI 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 NFI SSP CPS . Private keys held by the WidePoint NFI SSP will be held in strictest confidence. Under no circumstances will any private key appear unencrypted outside the WidePoint NFI SSP hardware. Private keys held by the WidePoint NFI SSP will be released only to a trusted authority defined in Section 4.12.2.2 of this WidePoint NFI 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 NFI 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 NFI 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 NFI SSP CPS.

9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

The WidePoint NFI SSP will not disclose certificate-related information to any third party unless authorized by Federal Bridge Certificate Policy, required by law, government rule or regulation, or order of a court of competent jurisdiction. The WidePoint NFI SSP will authenticate any request for release of information. This does not prevent the WidePoint NFI 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 NFI SSP will not disclose certificate or certificate-related information to any third party unless expressly authorized by Federal Bridge Certificate Policy, required by criminal law, government rule or regulation, or order of a criminal

court with jurisdiction. The WidePoint NFI 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 NFI SSP. Permission is granted to reproduce and distribute certificates issued by the WidePoint NFI 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 NFI 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 NFI SSP certificates issued to WidePoint personnel or WidePoint components/devices, including WidePoint NFI 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 NFI SSP CA Representations and Warranties

The WidePoint NFI SSP warrants that its procedures are implemented in accordance with this WidePoint NFI 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 NFI SSP CPS. The WidePoint NFI SSP warrants that CRLs issued, and keys generated by the WidePoint NFI SSP are in conformance with this WidePoint NFI SSP CPS.

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

- Will provide to the FPKIPA this WidePoint NFI SSP CPS, as well as any subsequent changes, for conformance assessment.
- Will conform to the stipulations of Federal Bridge Certificate Policy and this WidePoint NFI 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 NFI SSP CPS and Federal Bridge Certificate 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 NFI SSP Subscribers in accordance with Section 9.6.3 of this WidePoint NFI SSP CPS and that WidePoint NFI SSP Subscribers are informed of the consequences of not complying with those obligations.
- Revokes the certificates of WidePoint NFI SSP Subscribers found to have acted in a manner counter to WidePoint NFI SSP Subscriber obligations.
- Notifies WidePoint NFI SSP Subscribers and makes public for the benefit of WidePoint NFI SSP Subscribers and Relying Parties any changes to the WidePoint NFI SSP operations that may impact interoperability or security. The WidePoint NFI 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 NFI SSP CPS; and,

- Posts certificates and CRLs to the repository.

The WidePoint NFI 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 NFI SSP CPS/KRPS prior to key escrow.
- The WidePoint NFI SSP KED operates in accordance with the stipulations of this WidePoint NFI SSP CPS/KRPS and the X.509 Certificate Policy for the U.S. Federal PKI Federal Bridge Certificate Policy Framework .
- The WidePoint NFI 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 NFI SSP KED monitors WidePoint NFI SSP Key Recovery Agent and WidePoint NFI 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 NFI SSP Subscriber (applicant) organizations that authorize their employees to perform roles as stipulated in this WidePoint NFI SSP CPS, warrant that:

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

With respect to WidePoint NFI SSP Subscriber or Relying Party Agreements or obligations made by a U.S. Government entity by purchasing the services associated with this WidePoint NFI 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 NFI SSP Registration Authorities and Key Recovery Agent/Key Recovery Official Representations and Warranties

9.6.2.1 WidePoint NFI SSP Registration Authorities Obligations

A WidePoint NFI SSP Registration Authority that performs registration functions as described in this WidePoint NFI SSP CPS must comply with the stipulations of this this WidePoint NFI SSP CPS that is approved by the FPKIPA for use with the FPKIPA Federal Bridge Certificate Policy CP. A WidePoint NFI SSP Registration Authority who is found to have acted in a manner inconsistent with these obligations is subject to revocation of WidePoint NFI SSP Registration Authority responsibilities. A WidePoint NFI 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 NFI 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 NFI SSP Registration Authorities are obligated to accurately represent the information prepared for the WidePoint NFI SSP and to process requests and responses in a timely and secure manner. WidePoint NFI 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 NFI SSP CPS. WidePoint Registration Authorities under this WidePoint NFI SSP CPS are not authorized to assume any other WidePoint NFI SSP administration functions.

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

- Approve the issuance of certificates only when both the Applicant or WidePoint NFI 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 NFI SSP Subscriber's certificate request.
- To validate that the named Applicant or WidePoint NFI SSP Subscriber actually requested the certificate.
- Revoke certificates with properly validated revocation requests.
- Notify the Applicant or WidePoint NFI 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 NFI SSP CPS.
- Notify a WidePoint NFI SSP Subscriber of certificate revocation in accordance with Section 4.9.2 of this WidePoint NFI 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 NFI SSP CA if private key compromise is suspected.
- To immediately revoke a WidePoint Registration Authority , a WidePoint Local Registration Authority or a WidePoint NFI SSP Subscriber certificate and inform the WidePoint NFI SSP Subscriber if private key compromise is suspected.
- To revoke and approve reissue of WidePoint NFI SSP Subscriber certificates, if necessary, that were validated by a WidePoint Registration Authority or aWidePoint Local Registration Authority whose private key is suspected to be compromised.
- To inform trusted agents and the WidePoint NFI 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 NFI SSP Key Recovery Agents Obligations

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

- WidePoint NFI SSP Key Recovery Agents shall keep a copy of the Federal Bridge Certificate Policy CP and this WidePoint NFI SSP CPS.
- WidePoint NFI SSP Key Recovery Agents shall protect subscribers' escrowed keys from unauthorized disclosure, including the encrypted files and associated decryption keys.
- WidePoint NFI SSP Key Recovery Agents shall protect all information associated with key recovery, including the WidePoint NFI SSP Key Recovery Agent's own key(s), that could be used to recover subscribers' escrowed keys.
- WidePoint NFI SSP Key Recovery Agents shall release WidePoint NFI SSP Subscribers' escrowed keys only for properly authenticated and authorized requests from Requestor.
- WidePoint NFI SSP Key Recovery Agents may rely upon the WidePoint NFI SSP Key Recovery Officials for authentication and verification of the identity and authority of the Requestor. However, WidePoint NFI SSP

Key Recovery Agents shall also authenticate the identity of the Requestor when the Requestor digital signature is available.

- WidePoint NFI SSP Key Recovery Agents shall authenticate the WidePoint NFI SSP Key Recovery Officials as described in Section 3.5.4.
- WidePoint NFI SSP Key Recovery Agents shall validate the authorization of the WidePoint NFI SSP Key Recovery Official by ensuring that the WidePoint NFI SSP Key Recovery Official is an authorized WidePoint NFI SSP Key Recovery Official for the Subscriber for whom key recovery has been requested.
- WidePoint NFI SSP Key Recovery Agents shall protect all information regarding all occurrences of key recovery.
- WidePoint NFI SSP Key Recovery Agents shall communicate knowledge of a recovery process only to the WidePoint NFI SSP Key Recovery Official and Requestor involved in the key recovery.
- WidePoint NFI SSP Key Recovery Agents shall not communicate any information concerning a key recovery to the Subscriber except when the WidePoint NFI SSP Subscriber is the Requestor.
- WidePoint NFI SSP Key Recovery Agents shall monitor WidePoint NFI 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 NFI SSP Key Recovery Official Obligations

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

- The WidePoint NFI SSP Key Recovery Official shall protect the WidePoint NFI SSP Subscribers' recovered keys from compromise.
- After providing the Requestor with the encrypted key, the WidePoint NFI SSP Key Recovery Official shall destroy the copy of the key in his/her system.
- The WidePoint NFI SSP Key Recovery Official shall request the Subscriber's keys only upon receipt of a request from an authorized Requestor.
- The WidePoint NFI SSP Key Recovery Official, as an intermediary for the WidePoint NFI 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 NFI SSP Key Recovery Official shall forward the Requestor's digitally signed object to the WidePoint NFI SSP Key Recovery Agent in a form verifiable by the WidePoint NFI SSP Key Recovery Agent.
- In the case of persons other than the WidePoint NFI SSP Subscriber seeking a key recovery, the WidePoint NFI SSP Key Recovery Official shall ensure that the Requestor has the authority to request the WidePoint NFI SSP Subscriber's private decryption key.
- The WidePoint NFI SSP Key Recovery Official, as an intermediary for the WidePoint NFI SSP Key Recovery Agent, shall validate the authorization for the request, to include consultation with legal counsel when appropriate.
- The WidePoint NFI SSP Key Recovery Official shall protect all information associated with key recovery, including the WidePoint NFI 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 NFI SSP Key Recovery Official shall protect all information regarding all occurrences of key recovery.
- The WidePoint NFI SSP Key Recovery Official shall communicate knowledge of any recovery process only to the Requestor
- The WidePoint NFI SSP Key Recovery Official shall not communicate any information concerning a key recovery to the Subscriber except when the WidePoint NFI SSP Subscriber is the Requestor.
- The WidePoint NFI SSP Key Recovery Official shall accurately represent himself when requesting key recovery services.
- The WidePoint NFI 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 NFI SSP LRAs are obligated to accurately represent the information prepared for the WidePoint NFI 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 NFI SSP administration functions.

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

- To operate in accordance with the stipulations of this WidePoint NFI SSP CPS.
- To validate the accuracy of all information contained in the Applicant or WidePoint NFI SSP Subscriber's certificate request.
- To validate that the named Applicant or WidePoint NFI SSP Subscriber actually requested the certificate.
- To verify to the WidePoint Registration Authority that the certificate request originated from the named Applicant or WidePoint NFI 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 NFI SSP Subscriber's certificate upon notification of changes to information contained in the certificate.
- To request revocation of the certificates of WidePoint NFI SSP Subscribers found to have acted in a manner counter to subscriber obligations.
- To inform WidePoint NFI 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 NFI SSP Subscribers in accordance with the subscriber obligations; and,
- To inform Applicants and WidePoint NFI 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 Representations and Warranties

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

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

- To operate in accordance with the stipulations of this WidePoint NFI SSP CPS.
- To accurately represent themselves in all communications with the WidePoint NFI SSP.
- To protect the WidePoint NFI SSP issued certificate private key from unauthorized access in accordance with Section 6.2 of this WidePoint NFI 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 NFI SSP issued certificate or credential is suspected.
- To use the WidePoint NFI SSP issued certificate only for authorized applications which have met the requirements of Federal Bridge Certificate Policy and this WidePoint NFI SSP CPS.
- To use the WidePoint NFI SSP issued certificate only for the purpose for which it was issued, as indicated in the key usage extension of the certificate.
- 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 NFI 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 NFI 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 NFI SSP Sponsors (as described in Section 1.3.7.2) assume the obligations of WidePoint NFI SSP Subscribers for the certificates associated with their components and attest to the following Subscriber obligations:

WidePoint NFI 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 NFI SSP CPS.
- To accurately represent themselves in all communications with the WidePoint NFI SSP.
- To protect the WidePoint NFI SSP issued certificate private key from unauthorized access in accordance with Section 6.2 of this WidePoint NFI 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 NFI SSP issued certificate or credential is suspected.
- In the event of a WidePoint NFI SSP Sponsor change due to the verified individual having left the employ of the affiliated company or is no longer assigned as the WidePoint NFI SSP Sponsor for the WidePoint NFI SSP issued certificate(s), the affiliated organization must designate a new WidePoint NFI SSP Sponsor for the certificate(s). The new WidePoint NFI SSP Sponsor must complete a new identity verification.
- When renewing the certificate, the WidePoint NFI SSP Sponsor must complete a new identity verification.
- Confirm that the WidePoint NFI 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 NFI 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 the certificate only for authorized applications which have met the requirements of this WidePoint NFI 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 NFI 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 NFI SSP Subscribers shall hold WidePoint and the WidePoint NFI 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 NFI SSP does not represent that the individual has authority to act for that organization.

9.6.4 Relying Party Representations and Warranties

The WidePoint NFI SSP will publicly post a summary of this WidePoint NFI SSP CPS to the repositories as identified in Section 2 of this WidePoint NFI SSP CPS to provide the relying party information regarding the expectation of the WidePoint NFI SSP. When accepting a certificate issued under this WidePoint NFI 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.

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 NFI SSP practice statement.

9.6.5 Representations and Warranties of Other Participants

9.6.5.1 Representations and Warranties

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

The WidePoint NFI SSP warrants that WidePoint Registration Authorities or Trusted Agents operate in accordance with the applicable sections of this WidePoint NFI SSP CPS and Federal Bridge Certificate Policy.

9.6.5.2 Repository Representations and Warranties

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

- Contain an accurate and current CRL for each WidePoint NFI 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 NFI SSP CPS; and,
- Meet or exceed the requirement of 99% availability for all repository components within the control of the WidePoint NFI SSP. Communication failures as a result of Internet problems external to the operating organization will not count against this availability requirement.

The WidePoint NFI SSP maintains a copy of all certificates and CRLs for archiving. The WidePoint NFI 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 NFI SSP Subscriber identity verification in accordance with this WidePoint NFI SSP CPS and in accordance with Federal Bridge Certificate Policy.

9.6.5.4 CSS Representations and Warranties

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

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

9.6.5.5 PKI Point of Contact Representations and Warranties

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

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

9.7 Disclaimers of Warranties

Other than the warranties included in Section 9.6.6.1 of this WidePoint NFI SSP CPS, WidePoint disclaims all warranties and obligations of any type other than those listed.

Without limiting other WidePoint NFI SSP Subscriber obligations stated in this WidePoint NFI SSP CPS, all WidePoint NFI 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 NFI SSP provided that the certificate was issued in accordance with Federal Bridge Certificate Policy and this WidePoint NFI SSP CPS and that the relying party has used validation information that complies with Federal Bridge Certificate Policy and this WidePoint NFI SSP CPS. WidePoint acknowledges professional liability with respect to the WidePoint NFI SSP or WidePoint Registration Authorities and its trusted agents. The limit for losses per transaction due to improper actions by the WidePoint NFI 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 NFI SSP or WidePoint Registration Authorities and its trusted agents is $1 million (U.S. Dollars).

9.8.2 Other Exclusions

WidePoint NFI 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 NFI SSP Subscribers will hold the WidePoint NFI 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 NFI 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 Federal Bridge Certificate Policy, WidePoint NFI SSP Subscribers and Relying Parties will have no claim against the US Federal Government arising from use of the WidePoint NFI SSP Subscriber's certificate or a

WidePoint NFI 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 NFI SSP under this WidePoint NFI SSP CPS.

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

WidePoint NFI 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 NFI SSP and by the US Federal Government.

9.9 INDEMNITIES

Agents of the WidePoint NFI 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 NFI SSP.

9.10 TERM AND TERMINATION

9.10.1 TERM

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

9.10.2 TERMINATION

This WidePoint NFI SSP CPS will survive any termination of the WidePoint NFI 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 NFI SSP CPS.

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

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

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

9.12 AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENT

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

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

9.12.2 NOTIFICATION MECHANISM AND PERIOD

The WidePoint NFI SSP will publish information (including this WidePoint NFI SSP CPS with sensitive data redacted) on the WidePoint NFI 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 Federal Bridge Certificate Policy results in a material change to the trust by the relying parties.

9.13 Dispute Resolution Provisions

Any dispute arising with respect to this WidePoint NFI SSP CPS or certificates issued under this policy shall be resolved by the Parties.

With respect to Subscriber or Relying Party Agreements or Obligations made by an entity by purchasing the services associated with this WidePoint NFI 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 NFI SSP CPS with respect to the Federal Bridge Certificate Policy and the Memorandum of Understanding between the FPKIPA and WidePoint, the provider of the WidePoint NFI 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 NFI 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 NFI 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 Federal Bridge Certificate Policy and this WidePoint NFI SSP CPS, the WidePoint NFI SSP CPS shall take precedence. Except to the extent prohibited by law, in the event of any conflict between this WidePoint NFI SSP CPS or Federal Bridge Certificate Policy, on the one hand, and any WidePoint NFI SSP Subscriber or Subscriber Organization Agreement, or other document issued or agreement entered into by the WidePoint NFI SSP in connection with the performance of services under this WidePoint NFI SSP CPS, on the other hand, Federal Bridge Certificate Policy, or this WidePoint NFI SSP CPS, respectively, shall take precedence. The provisions of this WidePoint NFI SSP CPS cannot be overridden, bypassed, or changed by any document issued or agreement entered into by the WidePoint NFI SSP in connection with the performance of services under this WidePoint NFI 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

All WidePoint NFI SSP Certificate Authorities operating under this WidePoint NFI SSP CPS are required to comply with applicable law.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This WidePoint NFI SSP CPS constitutes the entire agreement between the involved parties concerning the transactions outlined herein, superseding any prior or existing oral or written agreements, communications, understandings, or representations regarding the subject matter. No party relies on any warranties, representations, assurances, or inducements not explicitly stated in this document, and no liability is incurred for any representation or assurance not expressly outlined, unless made fraudulently. Except for liability arising from fraudulent misrepresentation, no party bears responsibility or has a remedy for misrepresentation or untrue statements unless a claim arises from a breach of duty specified in this WidePoint NFI SSP CPS.

9.16.2 Assignment

The parties are prohibited from assigning any rights or obligations under this WidePoint NFI SSP CPS or related agreements without obtaining the written consent of the WidePoint NFI SSP.

9.16.3 Severability

Should it be determined that one section of this WidePoint NFI 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 NFI 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)

Should any legal action or arbitration be commenced in connection with this WidePoint NFI SSP CPS or the documents and agreements contemplated hereby, the prevailing party shall be entitled to recover, in addition to court/arbitration costs, the prevailing party's reasonable attorneys' fees. ANY ARBITRATION, LEGAL SUIT, ACTION OR PROCEEDING ARISING OUT OF OR BASED UPON THIS WIDEPOINT NFI SSP CPS AND/OR THE TRANSACTIONS AND AGREEMENTS CONTEMPLATED HEREBY MAY BE INSTITUTED IN THE FEDERAL OR STATE COURTS OF THE COMMONWEALTH OF VIRGINIA LOCATED IN FAIRFAX, VIRGINIA, AND EACH PARTY IRREVOCABLY SUBMITS TO THE EXCLUSIVE JURISDICTION OF SUCH COURTS IN ANY SUCH SUIT, ACTION OR PROCEEDING. THE PARTIES IRREVOCABLY AND UNCONDITIONALLY WAIVE ANY OBJECTION TO THE LAYING OF VENUE OF ANY ARBITRATION, SUIT, ACTION OR ANY PROCEEDING IN SUCH COURTS AND IRREVOCABLY WAIVE AND AGREE NOT TO PLEAD OR CLAIM IN ANY SUCH COURT THAT ANY SUCH SUIT, ACTION OR PROCEEDING BROUGHT IN ANY SUCH COURT HAS BEEN BROUGHT IN AN INCONVENIENT FORUM.

EACH PARTY ACKNOWLEDGES AND AGREES THAT ANY CONTROVERSY WHICH MAY ARISE UNDER THIS WIDEPOINT NFI SSP CPS OR THE OTHER DOCUMENTS REFERRED TO HEREIN IS LIKELY TO INVOLVE COMPLICATED AND DIFFICULT ISSUES AND, THEREFORE, EACH SUCH PARTY IRREVOCABLY AND UNCONDITIONALLY WAIVES ANY RIGHT IT MAY HAVE TO A TRIAL BY JURY IN RESPECT OF ANY LEGAL ACTION ARISING OUT OF OR RELATING TO THIS WIDEPOINT NFI SSP CPS, THE OTHER DOCUMENTS REFERRED TO HEREIN OR THE TRANSACTIONS CONTEMPLATED HEREBY OR THEREBY.

9.16.5 Force Majeure

Neither Party will be liable for any failure or delay in performing an obligation under this WidePoint NFI 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 NFI 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 NFI SSP 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 NFI SSP PIV-I credential

None of the WidePoint NFI SSP issued certificates, WidePoint NFI 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 NFI SSP certificates issued using profiles specified in the previous version of this WidePoint NFI SSP CPS and Federal Bridge Certificate Policy may be used until expired. All new WidePoint NFI SSP issued certificates shall conform to these profiles.

The following certificate and CRL profiles are in compliance with the FPKIPA's Federal Bridge Certificate 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 NFI 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 NFI 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 NFI SSP issued certificates including WidePoint NFI SSP CA certificates. WidePoint NFI SSP CSS certificates contain the certificate policy object identifiers for which the delegating WidePoint NFI SSP CA considers the WidePoint NFI SSP CSS to be authoritative.

WidePoint NFI SSP CA certificates and WidePoint NFI SSP Subscriber certificates other than WidePoint NFI 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 NFI SSP Subscriber private key is stored.
- SHA-384 certificate policy object identifiers can be asserted in a WidePoint NFI 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
  - cSubject public key in the certificate is 3072 or 4096 bit RSA or EC P-384
- WidePoint NFI 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 NFI SSP CPS.

A WidePoint NFI SSP certificate shall never contain higher assurance certificate policy object identifier as detailed in Section 1.2 of this WidePoint NFI SSP CPS than those determined using the above rules. A WidePoint NFI 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 NFI 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 NFI 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 NFI SSP Intermediate CA Certificate

Note: This certificate is issued to the WidePoint NFI SSP Intermediate Certificate Authority by the FPKI. Its purpose is to issue certificates to CA servers that will issue end entity certificates. The WidePoint NFI 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 Federal Bridge Certificate 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 NFI SSP INTERMEDIATE [UNIQUE NAME] <#>[2], 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 Federal Bridge Certificate 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 Federal Bridge Certificate 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 NFI SSP CPS as appropriate and per Section 10.3; Policy Qualifier Id=CPS Qualifier: https://ssp.orc.com/WidePointNFISSPCPS.pdf
Basic Constraints	c=yes; cA=True; path length constraint = 0

[2] 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[3]	c=no; [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://repo.fpki.gov/fcpca/fcpcag2.crl

[3] 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 NFI SSP CA CERTIFICATE

Note: These certificates are WidePoint NFI 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 Federal Bridge Certificate Policy CA G#, OU=FPKI, O=U.S. Government,C=US or cn=WIDEPOINT NFI ROOT [UNIQUE NAME] <#>[4], 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 NFI SSP [UNIQUE NAME] <#>[5], o=ORC PKI c=US or cn=[Organization 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 Federal Bridge Certificate 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 Federal Bridge Certificate 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 NFI 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[6]	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

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

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

[6] 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-I CONTENT SIGNING CERTIFICATE

This certificate profile is for the certificate that signs the content that is embedded on each WidePoint NFI SSP PIVI credential. Each WidePoint NFI SSP CMS has its own PIV-I 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 NFI 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 NFI 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[7]	c=no; octet string
subject key identifier[8]	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/

[7] 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.

[8] 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[9]	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=1.3.6.1.4.1.3922.1.1.1.20 {id-orc-nfissp-pivi-contentSigning};

[9] 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-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) 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 NFI 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 NFI 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[10]	c=no; octet string
subject key identifier[11]	c=no; octet string

[10] 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.

[11] 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 UUID. 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[12]	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-orc-nfissp-pivi-hardware};
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}[13]

[12] 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).

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

10.5.5 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) 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 NFI 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 NFI 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[14]	c=no; octet string
subject key identifier[15]	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-I Card encoded as a URI as specified in Section 3 of RFC 4122.

[14] 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.

[15] 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[16]	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=1.3.6.1.4.1.3922.1.1.1.19 {id-orc-nfissp-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}[17]

[16] 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).

[17] 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 NFI 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 NFI 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[18]	c=no; octet string
subject key identifier[19]	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.

[18] 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.

[19] 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[20]	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=1.3.6.1.4.1.3922.1.1.1.3 {id-orc-nfissp-medium} Policy Identifier=1.3.6.1.4.1.3922.1.1.1.12 {id-orc-nfissp-mediumHardware} Policy Identifier=1.3.6.1.4.1.3922.1.1.1.18 {id-orc-nfissp-pivi-hardware} Additional applicable organization 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}[21]

[20] 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).

[21] 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 NFI 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 NFI 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-I, 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[22]	c=no; octet string
subject key identifier[23]	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.

[22] 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.

[23] 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[24]	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=1.3.6.1.4.1.3922.1.1.1.3 {id-orc-nfissp-medium}
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}[25]

[24] 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).

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

10.5.8 NON 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) 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 NFI 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 NFI 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.
authority key identifier[26]	c=no; octet string
subject key identifier[27]	c=no; octet string
subject Alternative Name	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

[26] 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.

[27] 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[28]	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=1.3.6.1.4.1.3922.1.1.1.12 {id-orc-nfissp-mediumHardware}
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}[29]

[28] 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).

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

10.5.9 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 NFI 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 NFI 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 NFI 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[30]	c=no; octet string
subject key identifier[31]	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.

[30] 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.

[31] 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[32]	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=1.3.6.1.4.1.3922.1.1.1.37 {id-orc-nfissp-mediumDevice} Policy Identifier=1.3.6.1.4.1.3922.1.1.1.38 {id-orc-nfissp-mediumDeviceHardware} Additional applicable organization specific policies may be asserted.

10.5.9.1 Domain Controller Certificate

This certificate type is used for Microsoft Domain Controllers and is required to enable smart card logon through a WidePoint NFI SSP signature or WidePoint NFI 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
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.

[32] 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).

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}[33]	c=no; BMPString: DomainController; The actual extension value in HEX: 1E200044006F006D00610069006E0043006F006E00740072006F006C006C0065 0072

10.5.9.2 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>

10.5.9.3 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 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>

[33] Field is specific to Domain controller certificates, may not appear in other device certificates

10.5.10 DELEGATED OCSP RESPONDER CERTIFICATE

Note: This profile is used only for WidePoint NFI SSP CSSs responder certificates. The WidePoint NFI 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 NFI 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 NFI 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 NFI SSP CA's public key information)
Subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the WidePoint NFI 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: 1.3.6.1.4.1.3922.1.1.1.3 {id-orc-nfissp-medium} 1.3.6.1.4.1.3922.1.1.1.12 {id-orc-nfissp-mediumHardware} 1.3.6.1.4.1.3922.1.1.1.37 {id-orc-nfissp-mediumDevice} 1.3.6.1.4.1.3922.1.1.1.38 {id-orc-nfissp-pivi-hardware} 1.3.6.1.4.1.3922.1.1.1.19 {id-orc-nfissp-pivi-cardAuth} 1.3.6.1.4.1.3922.1.1.1.38 {id-orc-nfissp-mediumDevice-hardware} 1.3.6.1.4.1.3922.1.1.1.20 {id-orc-nfissp-pivi-contentSigning} Additional applicable organization specific policy OIDs may be asserted.

10.5.11 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 NFI 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
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.

Field	Subordinate CA CRL Value
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 Federal Bridge Certificate Policy public key information)

10.5.12 OCSP REQUEST FORMAT

OCSP requests are not expected to be signed. WidePoint NFI 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 NFI SSP CA certificate and the end entity certificate issued by that WidePoint NFI SSP CA.
Signature	Not Required
Extensions	Not Required

10.5.13 OCSP RESPONSE FORMAT

See RFC2560 for detailed syntax. The following table lists which fields are populated by a WidePoint NFI 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[34], thisUpdate, nextUpdate[35],
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

[34] If the certificate is revoked, the OCSP Responder will provide revocation time and revocation reason from CRL entry and CRL entry extension.

[35] The OCSP Responder will use thisUpdate and nextUpdate from CA CRL.

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 APPENDIX B: CARD MANAGEMENT SYSTEM REQUIREMENTS

PIV-I Cards are issued and managed through information systems called Card Management Systems (CMSs). The complexity and use of these trusted systems may vary. Nevertheless, the WidePoint NFI SSP or Organization have a responsibility to ensure a certain level of security from the WidePoint NFI SSP or Organization Card Management Systems that manage the token on which their certificates reside, and to which they issue certificates for the purpose of signing PIV-I Cards. This appendix provides additional requirements to those found above that apply to WidePoint NFI SSP or Organization Card Management Systems that are trusted under this WidePoint NFI SSP CP.

The Card Management Master Key must be maintained in a FIPS 140-3 Level 2 Cryptographic Module and conform to [NIST SP 800-78-4] requirements. Diversification operations must also occur on the Hardware Security Module (HSM). Use of these keys requires PIV-I Hardware or commensurate. Activation of the Card Management Master Key must require strong authentication of Trusted Roles. Card management must be configured such that only the authorized WidePoint NFI SSP or Organization Card Management System can manage issued cards.

The PIV-I identity proofing, registration and issuance process must adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV-I credential without the cooperation of another authorized person.

Individual personnel must be specifically designated to the four Trusted Roles defined in Section 5.2.1 of this WidePoint NFI SSP CP. Trusted Role eligibility and Rules for separation of duties follow the requirements for Medium assurance in Section 5 of this WidePoint NFI SSP CP.

All personnel who perform duties with respect to the operation of the WidePoint NFI SSP or Organization Card Management System must receive comprehensive training. Any significant change to WidePoint NFI SSP or Organization Card Management System operations must have a training (awareness) plan, and the execution of such plan must be documented.

Audit log files must be generated for all events relating to the security of the WidePoint NFI SSP or Organization Card Management System must be treated the same as those generated by the WidePoint NFI SSP or Organization Certificate Authority (see Sections 5.4 and 5.5 of this WidePoint NFI SSP CP).

A formal configuration management methodology must be used for installation and ongoing maintenance of the WidePoint NFI SSP or Organization Card Management System. Any modifications and upgrades to the WidePoint NFI SSP or Organization Card Management System must be documented and controlled. There must be a mechanism for detecting unauthorized modification to the WidePoint NFI SSP or Organization Card Management System.

The WidePoint NFI SSP or Organization Card Management System must have document incident handling procedures that are approved by the head of the organization responsible for operating the WidePoint NFI SSP or Organization Card Management System. If the WidePoint NFI SSP or Organization Card Management System is compromised, all certificates issued to the WidePoint NFI SSP or Organization Card Management System must be revoked, if applicable. The damage caused by the WidePoint NFI SSP or Organization Card Management System compromise must be assessed and all Subscriber certificates that may have been compromised must be revoked, and WidePoint NFI SSP or Organization Subscribers must be notified of such revocation. The WidePoint NFI SSP or Organization Card Management System must be re-established.

All Trusted Roles who operate a WidePoint NFI SSP or Organization Card Management System must be allowed access only when authenticated using a method commensurate with PIV-I Hardware.

14 APPENDIX C: IN-PERSON ANTECEDENT

This Appendix describes the baseline requirements for an in-person antecedent identity proofing event. An Antecedent event is an in-person proofing event that occurred previously and may suffice as meeting the in-person identity proofing requirements for a new certificate. The requirement for antecedent is identical to in-person identity proofing in Section 3.2 with the exception of using an historical in-person ID proofing event, and reliance on an on-going relationship. Hence, a proposed antecedent process must:

1. meet the thoroughness (rigor) of the in-person event,
2. provide supporting ID proofing artifacts or substantiate the applicant through an existing relationship, and
3. bind the individual to the asserted identity.

The Antecedent process may be appropriate when the applicant has no reasonable access to a Registration Authority or other Enrollment facility. The Antecedent process requires that the applicant – an employee, member, or associate – has an on-going relationship with the Sponsor and that an equivalent in-person identity proofing event was conducted with the Sponsor on some previous date. The Sponsor must attest to the validity of the individual's claimed identity through this existing relationship and provide details concerning the antecedent identity proofing event, including the date of the event, unique applicant identity information and existing artifacts from the event, if any, to the RA.

The following outlines specific requirements for the antecedent identity proofing and credential issuance process.

4. Identity Proofing Relationships
   - The Sponsor of the applicant must have a contractual relationship with the Entity PKI.
   - The Sponsor must have an established relationship with the applicant. The relationship must be sufficient to enable the RA to, with a high degree of certainty, verify that the person seeking the PKI certificate is the same person that was identity proofed.
   - The Sponsor's application must contain a description of the relationship with the applicant describing the initial identity proofing or qualifications and the on-going relationship.
5. Antecedent in-person identity proofing event
   - The Applicant must have provided a National Government-issued Picture I.D., or two Non-National Government I.D.s, one of which was a photo I.D. (e.g., Driver's License) during the antecedent identity proofing event. The identity of the entity providing confirmation of the antecedent identity proofing process must be captured in an auditable record.
6. Registration Authority (RA)

The RA must base its decision concerning the validity of the applicant's claimed identity on the information provided via the Antecedent identity proofing process and verification that the applicant is the same individual.

   - The RA must record the date of the antecedent in-person identity proofing event as provided by the Sponsor.
   - The RA must obtain the historical artifacts from the Antecedent event, if any.
   - The RA must be able to verify the applicant matches the individual who participated in the Antecedent proofing process.
7. Information source requirements.
   - The Antecedent process must ensure that all data received by the RA from the Sponsor is validated, protected, and securely exchanged.
   - All participants must store and exchange private information in a confidential and tamper evident manner protected from unauthorized access.

8. Binding the certificate request to the identity.

The process to bind the claimed identity to the specific certificate request must provide commensurate levels of assurance with the certificate being issued.

- A Sponsor for the applicant must provide the Entity PKI with initial contact information, (e.g., name, email address, phone number, sponsoring organization).
- The PKI must use the Sponsor provided information to contact the applicant.

15 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	Federal Bridge Certificate 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 19, 2019. https://csrc.nist.gov/publications/detail/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/publications/detail/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.

16 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

17 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	Fills the role of a Subscriber for non-human system components or organizations that are named as public key certificate subjects and is responsible for meeting the obligations of Subscribers as defined throughout this document.
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]