WIDEPOINT

NON-FEDERAL ISSUER SHARED SERVICE PROVIDER

CERTIFICATE POLICY

[WP-NC-NFISSP-CP]

Version 3.9

March 16, 2026

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

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

DOCUMENT SIGNATURE PAGE

Luther Eltinge Deyo III ORC9010002290.ID

Digitally signed by Luther Eltinge Deyo III ORC9010002290.ID
Date: 2026.06.05 12:53:56 -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 13:37:20 -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 12:26:13 -04'00'

Richard Webb, WidePoint Corporate Security Auditor

DOCUMENT REVISION HISTORY

Date	Version	Description of Change
2010-04-26	1	CP established in support of PIV-I Non-Federal Issuer requirements, and in conformance to RFC 3647
2010-07-08	2	Updated for cross-certification with FBCA PIV-I requirements
2010-12-06	3	Updated in response to compliance mapping performed against "FPKI Certification Applicant Requirements" by eValid8
2011-01-03	4	Final edits resulting from mapping performed against "FPKI Certification Applicant Requirements" by eValid8
2011-03-08	5	Edits resulting from CPWG review of CP mapping.
2011-03-08	6	Further edits resulting from CPWG review of CP mapping.
2011-06-03	7	Updates in response to CPWG review
2011-08-07	8	Correction of typographical errors (spaces in OID names and OID field removed)
2013-06-05	9	Updates in response to changes resulting from FBCA CP v2.26.
2014-02-18	10	Addition of new WidePoint OIDs to be issued starting 4-1-2014; set date of 3-31-2014 for cessation of issuing RSA OIDs.
2014-09-30	11	Updates to address mapping with FBCA CP.
2016-03-28	12	Updates to reflect WidePoint legal name change to WidePoint: adjust for Cert-on-Device capability; further updates to address mapping w/FBCA CP.
2016-04-28	13	Insert of "Notice" to clarify legal name change and its implication.
2016-07-21	14	Certificate policy description update
2018-08-29	1.2	Annual review and update
2019-03-14	1.3	
2019-07-31	1.3.1	Updates to address comments from FPKI in review of annual audit package.
2020-08-05	1.3.2	Updates to address comments from FPKI in review of annual audit package.
2021-10-21	1.3.3	Updates to address comments from FPKI in review of annual audit package.
2024-06-12	3.5	Updated to be in compliance with Federal Bridge Certificate Authority Certificate Policy v3.5. WidePoint NFI SSP CP version changed to be in line with FBCA CP versioning.
2025-05-05	3.6	Updates to address changes in Federal Bridge Certificate Authority Certificate Policy v3.6.
2025-07-07	3.7	Updates to address changes in Federal Bridge Certificate Authority Certificate Policy v3.7.
2025-09-10	3.8	Updates to address changes in Federal Bridge Certificate Authority Certificate Policy v3.8. Incorporate Annual Audit review findings and discrepancies.
2026-03-16	3.9	Updates to address changes in Federal Bridge Certificate Authority Certificate Policy v3.9. Incorporate Annual Audit review findings and discrepancies.

TABLE OF CONTENTS

1 INTRODUCTION

This document, the WidePoint Non-Federal Issuer Shared Service Provider Certificate Policy, hereafter referred to as the WidePoint NFI SSP CP, defines a number of distinct certificate policies for use by the WidePoint NFI SSP customer community and to promote interoperability with the federal government, state and local governments, organizations and other entities that are compliant and cross-certified with the Federal Bridge Certificate Authority.

This WidePoint NFI SSP CP is written to conform to the requirements and format of the X.509 Certificate Policy for the Federal Bridge Certification Authority Version 3.8, dated August 4, 2025, hereafter referred to as Federal Bridge Certificate Policy. In the event of any policy discrepancies between Federal Bridge Certificate Policy and the WidePoint NFI SSP CP, Federal Bridge Certificate Policy takes precedence.

The user policies apply to certificates issued to Non-Federal employees and affiliated personnel, and devices for the purposes of authentication, signature, and confidentiality. This CP was explicitly designed to support (complement) access to Federal systems that have not been designated national security systems. This CP implements a level of assurance comparable to or greater than the Federal Bridge Certification Authority (FBCA) Medium Assurance Policy.

A PKI that uses this WidePoint NFI SSP CP will provide 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 user policies require subscribers to use FIPS 140 validated cryptographic modules for cryptographic operations and the protection of trusted public keys. The device policy also requires use of FIPS 140 validated cryptographic modules for cryptographic operations and the protection of trusted public keys.

This policy enforces a hierarchical PKI. Any CA that asserts this policy in certificates must obtain prior approval from the WidePoint NFISSP PKI Policy Authority and must be signed by a CA in the WidePoint NFI chain. CAs that issue certificates under this policy may operate simultaneously under other policies. Such CAs must not assert the certificate policy object identifiers in this policy in certificates unless they are issued in accordance with all the requirements of this policy.

Realizing these potential benefits will require the use of digital signatures to verify the identity of both senders and receivers of electronic messages, as well as the integrity of the messages themselves. Use of digital signatures requires the use of public key cryptography and public key certificates to bind an individual public key to an identity.

WidePoint NFI SSP public key certificates may be utilized for non-Federal government and non-government individual identity and device authentications by Federal, state, local, and non-government entities (Relying Parties). Any use of or reference to this WidePoint NFI SSP CP outside of the purview of the WidePoint NFI SSP is specifically prohibited. It is intended that the WidePoint NFI SSP support only interoperability with the Federal Bridge Certificate Authority.

This WidePoint NFI SSP CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) request for comments (RFC) 3647, CP and Certification Practice Statement Framework.

The terms and provisions of this WidePoint NFI CP shall be interpreted under and governed by applicable laws of the Commonwealth of Virginia.

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 CP, 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 CP are further described in Section 1.4.1.1 of both documents.

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

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 CP, 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 CP.

Organization – This term for the purposes of this WidePoint NFI SSP Certificate Policy refers to an entity separate from WidePoint that is approved by the WidePoint NFI SSP to issue certificates under this policy. The Organization shall be approved by the WidePoint NFI SSP Policy Management Authority and shall have their own Certification Practice Statement that meets the requirements of this WidePoint NFI SSP Certificate Policy. These approved Organizations are subject to audits as described in Section 8 of this WidePoint NFI SSP by WidePoint selected auditors.

Note: Throughout this WidePoint NFI SSP CP, the term "Applicant" may be used to describe a WidePoint NFI SSP or Organization 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 or Organization. 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 or the Organization. The use of the term "Applicant" throughout this WidePoint NFI SSP CP will pertain to the time prior to approval for issuance by the WidePoint NFI SSP or Organization. The use of the term "Subscriber" will pertain to the time after approval for issuance by the WidePoint NFI SSP or Organization. In the case where WidePoint NFI SSP or Organization 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 or Organization.

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 policies in this WidePoint NFI SSP CP 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 CP describes the policies 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)

WidePoint NFI SSP certificates contain a registered certificate policy object identifier which may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. The certificate policy object identifier corresponds to the specific type and specific level of assurance for all WidePoint NFI SSP certificates issued under this WidePoint NFI SSP CP, which are available to all Relying Parties. Each WidePoint NFI SSP certificate issued shall assert the appropriate level of assurance in the certificatePolicies extension.

1.1.2 RELATIONSHIP BETWEEN WIDEPOINT NFI SSP CP AND THE WIDEPOINT NFI SSP CPS OR ORGANIZATION CPSS

The WidePoint NFI SSP CP states what assurance can be placed in a certificate issued by a WidePoint NFI SSP Certificate Authority or a subordinate organization Certificate Authority that has been approved to issue under this WidePoint NFI SSP CP. Each organization that is approved under the WidePoint NFI SSP, shall have a WidePoint NFI SSP approved Certification Practice Statement that aligns with this WidePoint NFI SSP. The WidePoint NFI SSP operations are described in the WidePoint NFI SSP CPS.

1.1.3 RELATIONSHIP BETWEEN THE WIDEPOINT NFI SSP CP AND THE FEDERAL BRIDGE CERTIFICATION AUTHORITY CP

The WidePoint NFI SSP is a participant in a Memorandum of Agreement (MOA) with the Federal PKI Policy Authority (FPKIPA), which sets forth the respective responsibilities and obligations of both parties and the mappings between the certificate levels of assurance contained in this WidePoint NFI SSP CP and those in the FBCA CP.

1.1.4 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 CP 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 CP 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 the WidePoint NFI SSP CPS or an organization's CPS that wishes to participate in the WidePoint NFI SSP program.

1.1.5 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 CP. Whenever this is the intended use, this WidePoint NFI SSP CP 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 CP that each one represents:

WP NFI SSP Certificate Policy Name	WP NFI SSP Certificate Policy Oid	FBCA Certificate Policy Oid	LOA
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. Certificate Authority certificates issued by the WidePoint NFI SSP program will assert the certificate policies above for every certificate policy OID that that a WidePoint NFI SSP or an approved organization Certificate Authority 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-mediumHardware
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).

Practice Note: Asserting **id-fpki-certpcy-mediumAssurance** for key management certificates is recommended as it provides implementation flexibility for specific use cases such as mobile devices and key recovery.

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 and WidePoint NFI SSP Registration Authorities are considered the WidePoint NFI SSP Certificate Management Authorities (CMA). Organization Certification Authorities and Organization Registration Authorities are considered the Organization Certificate Management Authorities (CMA). This WidePoint NFI SSP CP will use the term WidePoint NFI SSP CMA when a function may be assigned to either a WidePoint NFI SSP Certificate Authority or a WidePoint NFI SSP Registration Authority or when a requirement and its implementation applies to both. This WidePoint NFI SSP CP will use the term Organization CMA when a function may be assigned to either an Organization Certificate Authority or an Organization Registration Authority or when a requirement and its implementation applies to both.

WidePoint NFI SSP or Organization Certificate Status Services that provide Online Certificate Status Protocol (OCSP) and optional Server-based Certificate Validation Protocol (SCVP) status responses are operated by the WidePoint NFI SSP or Organization and are also considered a part of a WidePoint NFI SSP or Organization CMA. All WidePoint NFI SSP or Organization CMA(s) are operated in compliance with this WidePoint NFI SSP CP 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 OR ORGANIZATION CERTIFICATION AUTHORITIES

The WidePoint NFI SSP is issued a cross-certificate by the Federal Bridge Certificate Policy CA to each WidePoint NFI SSP Root Certificate Authority. The cross-certificate contains a policy mapping extension that maps the WidePoint NFI SSP certificate policies identified in Section 1.2 of this WidePoint NFI SSP CP to the equivalent Federal Bridge Certificate Policy. Each WidePoint NFI SSP Root Certificate Authority is off-line and issues Certificate Authority signing certificates to WidePoint NFI SSP Certificate Authorities or WidePoint NFI SSP PMA approved Organization Certificate Authorities. Certificate authority signing certificates issued by WidePoint NFI SSP Root Certificate Authority will contain a certificate policy extension that contain only the certificate policies identified in Section 1.2 of this WidePoint NFI SSP CP for which the WidePoint NFI SSP CPS or Organization CPS has been approved.

Each WidePoint NFI SSP Certificate Authority or Organization Certificate Authority shall encompass 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 or the Organization security boundary. Each WidePoint NFI SSP Certificate Authority or Organization Certificate Authority generates certificates in accordance with this WidePoint NFI SSP CP and in compliance with the certificate profiles described in Section 10 of this WidePoint NFI SSP CP. Each WidePoint NFI SSP Certificate Authority or Organization Certificate Authority 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 CP. Each approved WidePoint NFI SSP Certificate Authority or Organization 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 or Organization Certificate Authority signing keys
- Ensuring that all aspects of the WidePoint NFI SSP Certificate Authority or Organization Certificate Authority services, operations, and infrastructure related to certificates issued under this WidePoint NFI SSP CP are performed in accordance with the requirements, representations, and warranties of this WidePoint NFI SSP CP.

Each WidePoint NFI SSP Certificate Authority is governed by this WidePoint NFI SSP CP, the WidePoint NFI SSP CPS and the WidePoint System Security Plan. Each WidePoint NFI SSP Certificate Authority 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.

Each Organization Certificate Authority is governed by this WidePoint NFI SSP CP and the Organization CPS.

1.3.4 WIDEPOINT NFI SSP OR ORGANIZATION CARD MANAGEMENT SYSTEMS

Each WidePoint NFI SSP or Organization Card Management System is authorized by the WidePoint NFI SSP to process, issue, and revoke WidePoint NFI SSP or Organization 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 or Organization 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 or Organization 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 Certificate Authority or Organization Certificate Authority. Each WidePoint NFI SSP or Organization CMS's content signing certificate is used by the WidePoint NFI SSP CMS or Organization CMS to digitally sign data elements on WidePoint NFI SSP or Organization PIV-I credentials. Each WidePoint NFI SSP or Organization CMS is also issued a connector certificate with assigned privileges on the corresponding WidePoint NFI SSP Certificate Authority or Organization Certificate Authority for requesting certificate issuance and revocation. Each WidePoint NFI SSP or Organization CMS is considered a WidePoint NFI SSP or Organization Registration Authority and adheres to all the requirements specified for WidePoint NFI SSP or Organization Registration Authorities in this WidePoint NFI SSP CPS. Additionally, privileged users of a WidePoint NFI SSP CMS who can direct the WidePoint NFI SSP or Organization CMS to perform certificate related actions are considered to be WidePoint NFI SSP or Organization Registration Authorities, as described in Section 1.3.4 of this WidePoint NFI SSP CP. In addition, a WidePoint NFI SSP or Organization Card Management System shall not be issued any certificates that express the id-nfissp-pivi-hardware of id-nfissp-pivi-cardAuth certificate policy object identifier.

1.3.5 WIDEPOINT NFI SSP OR ORGANIZATION REGISTRATION AUTHORITIES

WidePoint NFI SSP or Organization Registration Authorities are entities that enter into an agreement with the WidePoint NFI SSP or Organization for the purpose of collecting and submitting digitally signed verification of Applicant and WidePoint NFI SSP or Organization Subscriber identities and information to be entered into public key certificates. WidePoint NFI SSP or Organization Registration Authorities are required to perform their functions in accordance with this WidePoint NFI SSP CP. WidePoint NFI SSP or Organization Registration Authorities register Applicants and WidePoint NFI SSP or Organization Subscribers, approve certificate issuance, and perform key recovery operations. WidePoint NFI SSP or Organization Registration Authorities are further separated into various roles to perform a subset of the Registration Authority functions. These WidePoint NFI SSP NFI SSP or Organization 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 NFI SSP or Organization Registration Authorities issue and revoke certificates that assert all certificate policies identified in Section 1.2 of this WidePoint NFI SSP CPS;
- WidePoint NFI SSP or Organization Registrars perform the registration process associated with WidePoint NFI SSP or Organization PIV-I credentials and approve Applicants and WidePoint NFI SSP or Organization Subscribers credential requests for issuance of a WidePoint NFI SSP or Organization PIV-I credential to an Applicant or WidePoint NFI SSP or Organization Subscriber;
- WidePoint NFI SSP or Organization Issuers reaffirm the identity of the WidePoint NFI SSP or Organization Subscriber who has been approved for issuance of a WidePoint NFI SSP or Organization PIV-I credential by a WidePoint NFI SSP or Organization Registrar and authorize and witness the key generation of the WidePoint NFI SSP or Organization PIV-I credential to the WidePoint NFI SSP or Organization Subscriber; and
- WidePoint NFI SSP or Organization Key Recovery Agents recover escrowed keys in accordance with the stipulations of this WidePoint NFI SSP CP.

WidePoint NFI SSP or Organization Registration Authorities may delegate the identity proofing tasks associated with Trusted Agents to WidePoint NFI SSP or Organization Local Registration Authorities who have been approved by the WidePoint NFI SSP and trained by a WidePoint NFI SSP or Organization Registration Authority on the processes of identity verification and authorization tasks. WidePoint NFI SSP or Organization Local Registration Authorities may be employees of WidePoint NFI SSP or Organization Subscriber organizations. A WidePoint NFI SSP or Organization Local Registration Authority may also serve as a WidePoint NFI SSP or Organization Key Recovery

Official who may process requests for key recovery by WidePoint NFI SSP or Organization Subscribers or third-party requestors and forward those requests to WidePoint NFI SSP or Organization Registration Authorities.

Trusted Agents are individuals who act on behalf of WidePoint NFI SSP or Organization Registration Authorities in performing identity verification and authorization verification tasks on Applicants and WidePoint NFI SSP or Organization Subscribers to the WidePoint NFI SSP. A Trusted Agent is a person authorized to act as a representative of the WidePoint NFI SSP or Organization in providing Applicant or WidePoint NFI SSP or Organization 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 Certificate Authorities or Organization Certificate Authorities or any WidePoint NFI SSP or Organization CMA system or function. Trusted Agents are not Trusted Roles; however, the PKI must document any Trusted Agent authorization requirements to include:

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

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

1.3.6 WidePoint NFI SSP or Organization Certificate Status Servers

WidePoint NFI SSP or Organization Certificate Status Services, hereafter referred to as WidePoint NFI SSP or Organization CSS(s), provide Online Certificate Status Protocol (OCSP) and optional Server-based Certificate Validation Protocol (SCVP) status responses. The WidePoint NFI SSP CSS(s) are operated by the WidePoint NFI SSP or Organization and are also considered a part of a WidePoint NFI SSP NFI SSP or Organization CMA. All WidePoint NFI SSP or Organization CMAs are operated in compliance with this WidePoint NFI SSP CP. Every certificate issued by the WidePoint NFI SSP or Organization is encoded with the location of the WidePoint NFI SSP or Organization 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 WidePoint NFI SSP and Organization Key Recovery Authorities

The WidePoint NFI SSP and Organization shall implement Key Recovery with the applicable requirements for physical, personnel, and procedural security controls, technical security controls, and Compliance Audit applied as follows:

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

1.3.7.1 WidePoint NFI SSP and Organization Key Escrow Database

A WidePoint NFI SSP or Organization 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 NFI SSP or Organization Key Escrow Database also responds to key recovery requests from two or more Key Recovery Agents or self-recovery by a current WidePoint NFI SSP or Organization Subscriber.

Section 5.2.1.2 in this WidePoint NFI SSP CP contains the description of trusted roles required to operate the WidePoint NFI SSP or Organization Key Escrow Database.

1.3.7.2 WidePoint NFI SSP and Organization Data Decryption Server

A WidePoint NFI SSP or Organization Data Decryption Server is an automated system that has the capability to obtain subscriber private keys from the WidePoint NFI SSP or Organization Key Escrow Database or another WidePoint NFI SSP or Organization Data Decryption Server for data monitoring or other purposes (e.g., email inspection). WidePoint NFI SSP or Organization Data Decryption Servers do not provide keys to WidePoint NFI SSP or Organization Subscribers or other Third-Party Requestors. A WidePoint NFI SSP or Organization Data Decryption

Server has access to escrowed key management keys and must meet all security requirements of the Key Encryption Database as outlined in this policy.

Implementation of a WidePoint NFI SSP or Organization Data Decryption Server is optional based on customer organization requirements.

1.3.7.3 WidePoint NFI SSP and Organization Key Recovery Agent

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

A WidePoint or Organization Key Recovery Agent performs the following functions:

- Confirm validity and completeness of requests,
- Recover copies of escrowed keys; and
- Distribute copies of recovered keys to Requestor, with protection as described in Section 4.12.1.2.1.

WidePoint or Organization Key Recovery Agents may additionally conduct requestor identity verification and authorization validation when WidePoint or Organization Key Recovery Officers are not used.

1.3.7.4 WidePoint NFI SSP and Organization Key Recovery Official

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

A WidePoint NFI SSP and Organization Key Recovery Official's responsibilities is to perform the following functions:

- Verify a Requestor's identity and authorization as stated by this policy;
- Assist authorized requestors in building key recovery requests;
- Utilize secure communication for key recovery requests to and responses from the KRA; and
- Participate in the distribution of escrowed keys to the Requestor, ensuring that it occurs as described by the WidePoint NFI SSP or Organization Certification Practice Statement.

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

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 or Organization Subscriber, a third-party from the Subscriber's organization (e.g., supervisor, corporate officer) or a law enforcement officer who is authorized to request recovery of a WidePoint NFI SSP or

Organization Subscriber's escrowed key. Any individual who can demonstrate a reasonably verifiable authority in accordance with the WidePoint NFI SSP or Organization's 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 or Organization Subscriber's supervisory chain or otherwise authorized to obtain the WidePoint NFI SSP or Organization Subscriber's key from the WidePoint NFI SSP or Organization Key Encryption Database. A list of personnel authorized to make such a request is provided to the WidePoint NFI SSP or Organization by the WidePoint NFI SSP or Organization Subscriber's customer organization with those personnel designated as WidePoint NFI SSP or Organization Key Recovery Officials.

1.3.8.2 External Third-Party Requestor

An external Requestor is someone (e.g., investigator) outside the WidePoint NFI SSP or Organization Subscriber's customer organization with an authorized court order or other legal instrument to obtain the decryption private key of the WidePoint NFI SSP or Organization 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 or Organization that clearly and uniquely identifies the WidePoint NFI SSP or Organization 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 or Organization and the WidePoint NFI or Organization SSP Subscriber's customer organizations will appoint authorized personnel and implement this WidePoint NFI SSP CP so that the existing organization policy regarding release of sensitive information can be met.

1.3.9 WIDEPOINT NFI SSP OR ORGANIZATION SUBSCRIBERS

A WidePoint NFI SSP or Organization Subscriber is an entity whose name appears as the subject in a certificate issued by the WidePoint NFI SSP or Organization, and who asserts that they will use the key and the associated certificate in accordance with this WidePoint NFI SSP CP. 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 or Organization Subscribers who will be issued role-based certificates. These certificates identify a specific role on behalf of which the WidePoint NFI SSP or Organization Subscriber is authorized to act rather than the WidePoint NFI SSP or Organization 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 or Organization Subscriber certificate. A specific role may be identified in certificates issued to multiple WidePoint NFI SSP or Organization 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 or Organization 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 or Organization 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 or Organization 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 or Organization PKI Sponsor

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

1.3.12.2 Other Authorities

1.3.12.2.1 WidePoint Corporate Security Auditor

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

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

1.3.12.2.2 External Independent Auditor

The WidePoint NFI SSP retains a nationally recognized firm with expertise in IT Security Auditing and Evaluation as an external independent 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 CP, 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 or Organization Subscriber as a means for the WidePoint NFI SSP or Organization Subscriber to identify themselves electronically to applications and other people. The Identity Certificate type uniquely identifies the WidePoint NFI SSP or Organization Subscriber and allows for the WidePoint NFI SSP or Organization 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 or Organization Subscriber.*

Encryption Certificates *– This certificate type is issued to a WidePoint NFI SSP or Organization Subscriber as a means for the WidePoint NFI SSP or Organization 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 or Organization Subscriber whenever they receive a signature certificate. Encryption certificates are escrowed as part of the issuance process of the WidePoint NFI SSP or Organization 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 or Organization CSS, as described in Section 1.3 of this WidePoint NFI SSP CP, 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 or Organization 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 or Organization Certificate Authority that signed it.*

The following certificate types are specific to the WidePoint NFI SSP or Organization 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.*

***PIV-I Card Authentication Certificates** – This certificate type is only issued to a WidePoint NFI SSP or Organization PIV-I Credential and uniquely identifies the FIPS 201-3 compliant card that holds the WidePoint NFI SSP or Organization issued card authentication certificate. This certificate type does not contain any Personally Identifiable Information (PII) data about the WidePoint NFI SSP or Organization Subscriber to whom the WidePoint NFI SSP or Organization 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 or Organization CMS, as described in Section 1.3.3 of this WidePoint NFI SSP CP, to sign the data elements (i.e. the content) that is captured during the issuance process for a WidePoint NFI SSP or Organization PIV-I Credential and that will be stored on the credential. This certificate type identifies the name of the WidePoint NFI SSP or Organization CMS that controls the issuance process for WidePoint NFI SSP or Organization 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 or Organization 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 or Organization 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 or Organization 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 or Organization 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 may contain an authentication certificate that asserts a certificate policy of* ***id-orc-nfissp-mediumHardware*** *and a key usage that only asserts Digital Signature****,*** *an identity certificate that asserts a certificate policy of* ***id-orc-nfissp-mediumHardware*** *and a key usage that only asserts Digital Signature and Non-Repudiation, and an encryption certificate that asserts a certificate policy of* ***id-orc-nfissp-medium*** *and a key usage that only asserts KeyEncipherment. The identity proofing performed for the Medium 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 CP.*

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 or Organization 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 or Organization 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 or Organization 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 known to the Applicant or the WidePoint NFI SSP or Organization Subscriber. Additional features of the WidePoint NFI SSP or Organization 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 or Organization Subscriber as part of a previous WidePoint NFI SSP or Organization PIV-I Credential issuance are also recovered to the new WidePoint NFI SSP or Organization PIV-I Credential for decrypting previously encrypted information by the WidePoint NFI SSP or Organization Subscriber.*

Elevated Privileges Credential – *This credential is a companion credential to a WidePoint NFI SSP or Organization Subscriber who holds an existing WidePoint NFI SSP or Organization 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 or Organization 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 or Organization 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 CP. Personnel, physical, procedural, and technical security controls, as described in this WidePoint NFI SSP CP, 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 CP, 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 or Organization 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 or Organization 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 or Organization can only assert the certificate policy value of **id-orc-nfissp-medium** for human WidePoint NFI SSP or Organization 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 or Organization Subscriber has generated their private keys in the presence of a WidePoint NFI SSP or Organization Registration Authority or WidePoint NFI SSP or Organization 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 or Organization). 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 or Organization 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 or Organization 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 or Organization PIV-I Credentials and their associated WidePoint NFI SSP or Organization 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 or Organization PIV-I Credential. Card Authentication PIV-I Assurance certificates issued by the WidePoint NFI SSP or Organization can only assert the certificate policy value of **id-orc-nfissp-pivi-cardAuth** and may only be issued to WidePoint NFI SSP or Organization PIV-I Credentials through a WidePoint NFI SSP or Organization 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 or Organization Subscriber has generated their private keys in the presence of a WidePoint NFI SSP or Organization Issuer upon completion of the WidePoint NFI SSP or Organization 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 or Organization can only assert the certificate policy value of **id-orc-nfissp-pivi-hardware** and may only be issued to WidePoint NFI SSP or Organization PIV-I Credentials through a WidePoint NFI SSP or Organization 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 or Organization PIV-I credential and may not be used for any other purpose. WidePoint NFI SSP or Organization Content Signing PIV-I certificates are only issued to a WidePoint NFI SSP or Organization CMS as required by this WidePoint NFI SSP CP and Federal Bridge Certificate Policy. Content Signing PIV-I Assurance certificates are only issued to a WidePoint NFI SSP or Organization CMS by the WidePoint NFI SSP or Organization 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 CP, 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 WidePoint NFI SSP or Organization CPS Suitability for the Policy

WidePoint NFI SSP shall determine suitability of the WidePoint NFI SSP or Organization 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 or Organization 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 or Organization 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 3.8 dated August 4, 2025. 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 and approved Organizations shall operate and maintain repositories in support of WidePoint NFI SSP and Organization Subscribers and Relying Parties and their use and acceptance of certificates issued by the WidePoint NFI SSP or Organization. The location of any publication is available to Subscribers and Relying Parties as stipulated in the WidePoint NFI SSP or Organization CPS.

Information in WidePoint NFI SSP or Organization Repositories shall be protected in accordance with the provisions of this WidePoint NFI SSP CP, the Federal Bridge Certificate Policy, and other referenced documents such as Public Law 093-579 Privacy Act of 1974 Title 5 United States Code §552a.

The WidePoint NFI SSP or Organization Repository shall be responsible for:

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

The WidePoint NFI SSP or Organization Repository location shall be specified in the WidePoint NFI SSP or Organization CPS. The WidePoint NFI SSP or Organization Repository shall maintain 99% overall availability and limit 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

All WidePoint NFI SSP or Organization Certificate Authority certificates and all human and device certificates shall contain valid Uniform Resource Identifiers (URIs) that are publicly accessible, for the purposes of certification path building and for revocation checking.

The WidePoint NFI SSP shall publish all Certificate Authority certificates that it issues from the WidePoint NFI SSP Root Certificate Authorities for WidePoint NFI SSP Subordinate Certificate Authorities and approved Organization Certificate Authorities in a file available via a publicly accessible HTTP URI. This URI must be asserted in the Subject Information Access (SIA) extension in all valid certificates issued to the Certificate Authority. The file shall be a certs-only Cryptographic Message Syntax file that has an extension of .p7c.

All WidePoint NFI SSP issued Certificate Authority certificates shall be published by the WidePoint NFI SSP or Organization Subordinate Certificate Authority in a file available via a publicly accessible HTTP URI. This URI must be asserted in the Authority Information Access (AIA) extension in all valid certificates issued by the WidePoint NFI SSP or Organization Subordinate Certificate Authority. The repository must:

- contain a binary (DER encoded) certs-only Cryptographic Message Syntax file that has an extension of .p7c and a http response content type header of 'application/pkcs7-mime', or
- contain a single binary (DER encoded) certificate that has an extension of .cer and a http response content type header of 'application/pkix-cert'.

The certs-only Cryptographic Message Syntax format is preferred as it allows flexibility for inclusion of multiple certificates.

All WidePoint NFI SSP or Organization Subordinate Certificate Authorities shall publish the latest CRL covering all unexpired certificates from that Certificate Authority via a publicly accessible HTTP URI until such time as all issued certificates have expired. The URI shall be asserted in the CRL distribution point extension of all certificates issued by that Certificate Authority, except for OCSP responder certificates that include the id-pkix-ocsp-nocheck extension.

WidePoint NFI SPP or Organization Certificate Status Servers provide status information about certificates on behalf of a WidePoint NFI SPP or Organization Certificate Authority through on-line transactions.

WidePoint NFI SPP or Organization Certificate Authorities that support PIV-I shall include a Certificate Status Server in the form of a delegated Online Certificate Status Protocol (OCSP) service, as described in [RFC 6960], to provide on-line status information for WidePoint NFI SPP or Organization Subscriber certificates via a publicly accessible HTTP URI in the AIA extension.

Pre-generated OCSP responses may be created by the WidePoint NFI SSP or Organization Certificate Status Servers 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 or Organization CRLs.

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

2.2.2 PUBLICATION OF WIDEPOINT NFI SSP OR ORGANIZATION CERTIFICATE AUTHORITY INFORMATION

The WidePoint NFI SSP or Organization Repository shall be publicly accessible that is available to all WidePoint NFI SSP or Organization Subscribers and relying parties that contains:

- All certificates issued to WidePoint NFI SSP or Organization Certificate Authorities;
- A copy of the current Federal Bridge Certificate Policy CP, a copy of the WidePoint NFI SSP CP as well as including any waivers granted to the WidePoint NFI SSP by the FPKIPA;
- A copy of the WidePoint NFI SSP or Organization annual PKI Compliance Audit Letter; and,

- An abridged version of the approved WidePoint NFI SSP or Organization 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 or Organization:
  - 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 CP.

2.3 TIME OR FREQUENCY OF PUBLICATION

This WidePoint NFI SSP CP and any subsequent changes are made publicly available within thirty (30) days of approval.

Publication requirements for CRLs are provided in Sections 4.9.7 and 4.9.12.

2.4 ACCESS CONTROLS ON REPOSITORIES

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

There shall be no access controls on the reading of repository information, including certificates and CRLs. Updating the WidePoint NFI SSP or Organization Repository shall be restricted to specific trusted roles, as described in Section 5.2.1 of this WidePoint NFI SSP CP, using certificate authenticated access control over TLS. The WidePoint NFI SSP or Organization shall protect any and all repository information not intended for public dissemination or modification. Access controls shall include:

- Access to WidePoint NFI SSP or Organization systems and system components shall be limited to the appropriate trusted roles as described in Section 5.2.1 of this WidePoint NFI SSP CP and shall be protected by strong authentication methods.
- User authentication shall be via certificate authentication (or User ID and password when appropriate) and data encryption shall be used, as stipulated in this WidePoint NFI SSP CPS.
- WidePoint NFI SSP or Organization personnel in trusted roles as identified in Section 5.2.1 of this WidePoint NFI SSP CPS shall be trained in accordance with the requirements of the trusted role.
- The WidePoint or Organization Corporate Security Auditor determines and periodically reviews user access rights.
- WidePoint NFI SSP or Organization certificates that contain the universally unique identifier (UUID) in the subject alternative name extension, or any other certificate field shall be restricted from publication to the WidePoint NFI SSP or Organization Repository or any public repository.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 TYPES OF NAMES

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

All WidePoint NFI SSP or Organization Certificate Authority certificates issued by WidePoint NFI SSP Root Certificate Authorities will include a non-NULL subject DN. All certificates issued by the WidePoint NFI SSP or Organization Certificate Authorities to end entities will include a non-NULL subject DN. WidePoint NFI SSP or Organization Registration Authorities will ensure by visual inspection on the WidePoint NFI SSP or Organization Certificate Authorities 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 or Organization under this WidePoint NFI SSP CP shall 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 or Organization 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 or Organization shall be assigned either a geo-political name or an Internet domain component name. Device names shall 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 shall identify a specific role on behalf of which one or more WidePoint NFI SSP or Organization Subscribers shall be authorized to act rather than the WidePoint NFI SSP or Organization 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 WidePoint NFI SSP or Organization Subscriber certificates, use of the Subscriber common name shall be prohibited, instead a serialNumber=UUID shall be required. PIV-I Card Authentication certificates shall indicate whether or not the WidePoint NFI SSP or Organization 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** shall indicate whether or not the WidePoint NFI SSP or Organization 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 or Organization CA Name>, {Base DN}

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

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

The {Base DN} for Organization is defined as: 'o=<Organization CA Name>, c=US'.

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

WidePoint NFI SSP or Organization 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 or Organization 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 or Organization 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 or Organization Subscriber certificates shall 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 or Organization Subscriber certificates shall identify the person or object to which they are assigned.

Within the DN structure of certificates issued by the WidePoint NFI SSP or Organization to WidePoint NFI SSP or Organization Subscribers, the Common Name, hereafter referred to as CN, shall represent the WidePoint NFI SSP or Organization Subscriber in a way that is easily understandable for humans. For human and device Subscribers, the CN shall take the form identified in Section 3.1.1 of this WidePoint NFI SSP CP. Additionally, the DN shall accurately reflect organizational structures within the directory information tree.

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

3.1.3 Anonymity or Pseudonymity of Subscribers

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

The WidePoint NFI SSP or Organization shall not issue anonymous or pseudonymous certificates.

Role-based certificates may be issued by the WidePoint NFI SSP or Organization to support internal operations. WidePoint NFI SSP or Organization Certificate Authorities may also issue role-based certificates that identify subjects by their organizational roles, as described in Section 3.2.3.2 of this WidePoint NFI SSP CP.

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 PIV-I certificate UUID names are specified in [RFC 4122].

3.1.5 Uniqueness of Names

The WidePoint NFI SSP or Organization operating under this WidePoint NFI SSP CP shall comply with uniqueness of names; including X.500 DNs. The WidePoint NFI SSP or Organization Certificate Authorities shall share a single public directory information tree for the publication of certificates issued by the WidePoint (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 shall be responsible for ensuring name uniqueness in certificates issued by the WidePoint NFI SSP or Organization for all certificates issued under this WidePoint NFI SSP CP.

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 or Organization issued certificates. The WidePoint NFI SSP or Organization will not knowingly issue a certificate from the WidePoint NFI SSP or Organization 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 certificate issued under this WidePoint NFI SSP CP contains a name that has infringed the referenced ruling, the WidePoint NFI SSP or Organization shall revoke the previous issued certificates in accordance with Section 4.9.1 of this WidePoint NFI SSP CP and the WidePoint NFI SSP or Organization CPS.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

For Applicants and WidePoint NFI SSP or Organization 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 or Organization shall authenticate the Applicant or WidePoint NFI SSP or Organization 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.

Practice Note: For signature keys, this may be done by the entity using its private key to sign a value and providing that value to the CA. The CA must then validate the signature using the party's public key. The WidePoint NFI SSP may allow other mechanisms that are at least as secure as those cited here.

In the case where key generation is performed under the CA or RA's direct control, proof of possession is not required (e.g., key management certificates generated in a system allowing key escrow).

3.2.2 Authentication of Organization Identity

Requests for Certificate Authority certificates from the WidePoint NFI SSP must include the organization name, address, and documentation of the existence of the organization. Before issuing WidePoint NFI SSP Certificate Authority certificates, the WidePoint NFI SSP PMA shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the organization.

Before issuing WidePoint NFI SSP or Organization Subscriber certificates on behalf of an affiliated organization, the issuing Certificate Authority must verify the authority of requesting representatives.

3.2.3 Authentication of Individual Identity

For each certificate issued, the WidePoint NFI SSP or Organization shall authenticate the identity of the individual requestor. In addition to the processes described below, WidePoint NFI SSP or Organization Subscriber certificates may be issued on the basis of an electronically authenticated request, using a valid signature or authentication certificate and associated private key, with the following restrictions:

- The assurance level of the new certificate must be the same or lower than the assurance level of the certificate used to authenticate the request;
- Identity information in the new certificate must match the identity information from the signature or authentication certificate;
- The expiration date of the new certificate shall not exceed the next required initial identity authentication date associated with the certificate used to authenticate the request.
- The next required initial identity authentication date remains unchanged in the event of a new certificate issuance based on electronic authentication.

3.2.3.1 Authentication of Human Subscribers

For Applicants and WidePoint NFI SSP or Organization Subscribers, the WidePoint NFI SSP or Organization, and/or associated Registration Authorities must ensure that the applicant or Subscriber's identity information is verified in accordance with the process established by this WidePoint NFI SSP CP and the WidePoint NFI SSP or Organization CPS. Process information depends upon the certificate level of assurance and must be addressed in the WidePoint NFI SSP or Organization CPS.

The Certificate Authorities and/or the Registration Authorities operating in accordance with this WidePoint NFI SSP CP must record the information set forth below for issuance of each certificate:

- The identity of the person performing the identification and either;
  - A signed declaration by that person that he or she verified the identity of the applicant as required using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.
  - An auditable record linking the authentication of the person performing the identification to their verification of each Applicant.
- If in-person or supervised remote identity proofing is done, a unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- If supervised remote identity proofing is done for a WidePoint NFI SSP or Organization PIV-I credential, the identity proofing process must capture biometrics that include, at a minimum, the fingerprints to the extent physically possible and the facial image.
- If electronic authentication is done, a unique identifying number(s) from the signature or authentication certificate must be retained (e.g., certificate, serial number, thumbprint, SKI, public key, etc.)
- The date of the verification; and either:
  - An auditable record indicating the applicant accepted the certificate; or
  - A declaration of identity signed by the applicant using a handwritten signature or appropriate digital signature (see Practice Note) and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

Practice Note: In those cases, in which the individual is in possession of a valid digital signature credential of equal or higher level of assurance or the signature certificate is generated immediately upon authentication of the applicant's identity, the applicant may sign the declaration of identity and certificate of acceptance using the digital credential. In the latter case, if the applicant fails to sign the declaration of identity, then the certificate must be revoked.

The table below summarizes the identification requirements for each level of assurance available under this WidePoint NFI SSP CP:

Assurance Level	Identification Requirements
Medium (All policies)	Identity must be established by in-person or supervised remote proofing before the Registration Authority, Trusted Agent or an entity certified by a State or Federal Entity as being authorized to confirm identities; information provided must be verified to ensure legitimacy. A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement. Credentials required are one Federal Government-issued Picture I.D., one REAL ID Act compliant picture ID2, or two Non-Federal Government I.D.s, one of which must be a photo I.D. Any credentials presented must be unexpired. PIV-I identity must be verified in accordance with the requirements specified for issuing PIV in Section 2.7 of [FIPS 201] For PIV-I, the use of an in-person antecedent is not applicable.

The WidePoint NFI SSP or Organization CPS must indicate what actors, roles, responsibilities and activities are leveraged when relying on in-person antecedent to support identity proofing (e.g., agreement with a professional organization to use a member identification number and associated provided point of contact information as antecedent, or electronic authentication using a medium or above certificate being traced back to the initial identity proofing event).

For all levels of assurance except PIV-I: If an applicant is unable to perform face-to-face, either in-person or supervised remote, registration (e.g., a network device), the applicant may be represented by a trusted person already issued a digital certificate by the Entity. The trusted person will present information sufficient for registration at the level of the certificate being requested, for both himself/herself and the applicant who the trusted person is representing

For Medium Assurance Levels: An entity certified by a State or Federal Entity as being authorized to confirm identities may perform in-person authentication on behalf of the Registration Authority and may be considered a Trusted Agent. The certified entity forwards the information collected from the applicant directly to the RA in a secure manner. Packages secured in a tamper-evident manner by the certified entity satisfy this requirement; other secure methods are also acceptable. Such authentication does not relieve the Registration Authority of its responsibility to verify the presented data.

For PIV-I Certificates: PIV-I Hardware certificates must be issued only to human subscribers. The following biometric data must be collected during the identity proofing and registration process, and must be formatted in accordance with [NIST SP 800-76-2] (see Appendix A):

- 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

In the event an applicant is denied a credential based on the results of the identity proofing process, the Entity must provide a mechanism for appeal or redress of the decision.

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 or Organization must not be shared and must be issued to individual subscribers and protected in the same manner as individual certificates.

The WidePoint NFI SSP or Organization must record 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 or Organization at the same or higher assurance level as the role based certificate.

The procedures for issuing role-based tokens must comply with all other stipulations of this WidePoint NFI SSP or Organization 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 or Organization 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 or Organization 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 or Organization Subscribers. The WidePoint NFI SSP or Organization through the WidePoint NFISSP or Organization 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 or Organization Subscribers who have access to use of the private key, and accounting for which WidePoint NFI SSP or Organization Subscriber had control of the key at what time.
- The subjectName DN must 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 must be provided to, and retained by, the WidePoint NFI SSP or Organization; and
- The procedures for issuing tokens for use in shared key applications must comply with all other stipulations of this WidePoint NFI SSP or Organization 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. The sponsor is responsible for the security of the private key and for providing the following registration information:

- 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 the WidePoint NFI SSP or Organization to communicate with the PKI sponsor when required.

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. The WidePoint NFI SSP or Organization Certification Practice Statement describes the procedures to ensure that certificate accountability is maintained.

The registration information must be verified to an assurance level commensurate with the certificate assurance level being requested. For certificates that assert a certificate policy mapped to the **id-orc-nfissp-mediumDevice** or **id-orc-nfissp-mediumDeviceHardware** policies, registration information must be verified commensurate with the Medium assurance level. Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

- 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 or Organization certificates shall 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

The WidePoint NFI SSP or Organization must validate the requestor's authority to act in the name of the organization before issuing organizational certificates. The WidePoint NFI SSP will validate the requestor's authority through verification of the WidePoint NFI SSP PKI Point of Contact documentation, the Organizational

Affiliation signed documentation and that there is a current contractual agreement between the WidePoint NFI SSP and the Requestor's Organization prior to issuance of any approval for issuance of any Subordinated Organization Certificate Authority Certificates.

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 certificate authority 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 or Organization Subscriber PIV-I identity shall be 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 from initial registration.

In the event a WidePoint NFI SSP or Organization 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 or Organization 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 or Organization 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 shall require the steps for initial registration, as outlined in Section 3.2.3.1 of this WidePoint NFI SSP CP unless identity can be verified through the use of biometrics on file through the chain of trust defined in [FIPS 201] typically through presentation of fingerprints to the WidePoint NFI SSP or Organization Card Management System that will do a fingerprint comparison to the presented credential while in the presence of a WidePoint or Organization Registrar or Issuer. A WidePoint NFI SSP or Organization Subscriber who has had their certificate revoked shall revert to being an Applicant and shall be unknown to the WidePoint NFI SSP or Organization in terms of applying for certificate requests from the WidePoint NFI SSP or Organization in the future.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

All revocation request for WidePoint NFI SSP or Organization Certificate Authorities must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's public key, regardless of whether or not the associated private key has been compromised.

3.5 IDENTIFICATION AND AUTHENTICATION FOR KEY RECOVERY REQUEST

3.5.1 KEY RECOVERY AGENT AUTHENTICATION

WidePoint NFI SSP Key Recovery Agents shall authenticate to a WidePoint NFI SSP or Organization Key Encryption Database or a WidePoint NFI SSP or Organization Data Decryption Server using a public key certificate issued by a WidePoint NFI SSP or Organization. When a public key certificate is used, it must be on a FIPS 140 level 2 or higher

validated hardware cryptographic module. The assurance level of the certificate must be the same as or greater than that of the certificate whose corresponding private key is being recovered.

3.5.2 Key Recovery Official Authentication

A WidePoint NFI SSP or Organization Key Recovery Official must authenticate to the A WidePoint NFI SSP or Organization Key Recovery Agent using a public key certificate issued by the WidePoint NFI SSP or Organization. The assurance level of the certificate must be the same as or greater than that of the certificate whose corresponding private key is being recovered.

3.5.3 WidePoint NFI SSP Subscriber Key Recovery Request Authentication

The WidePoint NFI SSP or Organization Subscriber identity must be established as specified in Section 3.3.1 above. Alternatively, if the authentication cannot be verified using the public key certificates issued by the WidePoint NFI SSP or Organization and for at least the given certificate policy assurance level, then the identity validation can use the steps outlined in Section 3.2.3.1.

For automated self-recovery, the WidePoint NFI SSP or Organization Subscriber must be authenticated to the WidePoint NFI SSP or Organization Key Encryption Database using a valid public key certificate. The assurance level of the Subscriber certificate must be equal to or greater than that of the certificate whose corresponding private key is being recovered.

3.5.4 Third-Party Key Recovery Request Authentication

The WidePoint NFI SSP or Organization Key Recovery Agent or the WidePoint NFI SSP or Organization Key Recovery Official must verify the identity and authorization of the Requestor prior to initiating the key recovery request.

Third-Party Requestor identity authentication must be commensurate with the assurance level of the certificate associated with the key being recovered. Identity must be established using one of the following methods:

- Procedures specified in Section 3.2.3 for authentication of an individual identity during initial registration for the specified certificate policy assurance level (an assurance level equal to or greater than the assurance level of the certificate whose corresponding private key is being recovered).
- Certificate-based authentication (e.g., digitally signed e-mail or client-authenticated TLS) that can be verified using current, valid (i.e., un-revoked) public key certificates at the requested certificate policy assurance level (an assurance level equal to or greater than the assurance level of the certificate whose corresponding private key is being recovered).

3.5.5 WidePoint NFI SSP Data Decryption Server Authentication

A WidePoint NFI SSP or Organization Data Decryption Server must authenticate to a WidePoint NFI SSP or Organization Key Encryption Database directly using a public key certificate issued by the WidePoint NFI SSP or Organization. The assurance level of the certificate issued to a WidePoint NFI SSP or Organization Data Decryption Server must be the same as or greater than that of the highest assurance level encryption certificates issued by the WidePoint NFI SSP or Organization.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

The certificate application process for the WidePoint NFI SSP or Organization must provide sufficient information to:

- Establish the Applicant's authorization by sponsoring organization to obtain a certificate. See Section 3.2.3 for requirements.
- Establish and record the identity of the Applicant. See Section 3.2.3 for requirements.
- Obtain the Applicant's public key and verify the Applicant's possession of the private key. See Section 3.2.3 for requirements.
- Verify the information included in the certificate.

These steps may be performed in any order, but all must be completed before certificate issuance.

This section specifies requirements for initial application for certificate issuance.

Organizations seeking to sign their certificate authority certificates through the WidePoint NFI SSP must fulfill the application requirements as specified by the WidePoint NFI SSP PMA. The WidePoint NFI SSP PMA acts on the application and, upon making a determination to issue a certificate establishes a Memorandum of Agreement with the Organization. The WidePoint NFI SSP identifies the Organization's authorized representatives, provides the appropriate certificate policies and authorizes the WidePoint NFI SSP to issue the certificate authority to the Organization.

The WidePoint NFI SSP or Organization may issue certificates to trusted personnel where necessary for the internal operations of the WidePoint NFI SSP or Organization's PKI Infrastructure.

4.1.1 WHO CAN SUBMIT A CERTIFICATE APPLICATION

The following persons may initiate the Certificate application process:

Potential Subscriber	Authorized Initiator
Unaffiliated Individual	Potential Subscriber only
Business Representative	Sponsoring Organization or potential Subscriber
State and Local Government Employee	Sponsoring Organization or potential Subscriber
Devices	Sponsor responsible for the device receiving the certificate
Organization (Signed CA certificate)	Sponsor with signature authority from the Organization

4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES

All communications supporting the certificate application and issuance process must be authenticated and protected from modification. Communications may be electronic or out-of-band.

Any electronic communication of shared secrets must be protected.

Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair must be used.

Out-of-band communications must protect the confidentiality and integrity of the data.

WidePoint NFI SSP or Organization Subscribers are responsible for providing accurate information on their certificate applications.

Organizations applying for certificate authority signing certificates are responsible for providing accurate information on their certificate applications. Upon issuance, each Organization certificate authority certificate

issued by the WidePoint NFI SSP Root Certificate Authorities is manually checked to ensure each field and extension is properly populated with the correct information before the certificate is delivered to the Organization.

If databases or other sources are used to confirm WidePoint NFI SSP or Organization Subscriber attributes, then these sources and associated information sent to the WidePoint NFI SSP or Organization require:

- An auditable chain of custody is in place when information is obtained through one or more information sources.
- All data received be protected and securely exchanged in a confidential and tamper evident manner and protected from unauthorized access.

4.2 Certificate Application Processing

Information in certificate applications must be verified as accurate before certificates are issued. The WidePoint NFI SSP or Organization CPS must specify procedures to verify information in certificate applications in accordance with this WidePoint NFI SSP CP.

4.2.1 Performing Identification and Authentication Functions

For the WidePoint NFI SSP or Organization, the identification and authentication of the WidePoint NFI SSP or Organization Subscriber must meet the requirements specified for Subscriber authentication as specified in Sections 3.2 and 3.3 of this WidePoint NFI SSP CP. The WidePoint NFI SSP or Organization must identify the components of the WidePoint NFI SSP or Organization (e.g., Certificate Authority or Registration Authority) that are responsible for authenticating the WidePoint NFI SSP or Organization Subscriber's identity in each case.

4.2.2 Approval or Rejection of Certificate Applications

For WidePoint NFI SSP or Organization, WidePoint NFI SSP or Organization CPS shall identify the person or organizational body that may accept or reject a certificate application.

4.2.3 Time to Process Certificate Applications

The entire process from Applicant or WidePoint NFI SSP or Organization Subscriber appearing before a WidePoint NFI SSP or Organization Registration Authority, a WidePoint NFI SSP or Organization Local Registration Authority, or a Trusted Agent for identity verification to certificate issuance must take no more than 90 days. All certificate requests shall be verified by a WidePoint NFI SSP or Organization Registration Authority or a WidePoint NFI SSP or Organization Local Registration Authority prior to issuance to confirm that the issuance would be within the 90-day window described above and shall 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

The WidePoint NFI SSP or Organization verifies the source of a certificate request before issuance. WidePoint NFI SSP or Organization Certificate Authority certificates created by the WidePoint NFI SSP are checked to ensure that all fields and extensions are properly populated.

For issuance of all certificate types and assurance levels, the WidePoint NFI SSP or Organization must:

- Verify the identity of the requestor.
- Verify the authority of the requestor and the integrity of the information in the certificate request.
- Verify all attribute information received from a WidePoint NFI SSP or Organization Subscriber before inclusion in a certificate.
- Build and sign a certificate if all certificate requirements have been met (in the case of a WidePoint NFI SSP or Organization Registration Authority, have the WidePoint NFI SSP or Organization Certificate Authority sign the certificate).

- Make the certificate available to the WidePoint NFI SSP or Organization Subscriber after confirming that the WidePoint NFI SSP or Organization Subscriber has formally acknowledged the obligations described in Section 9.6.3.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The WidePoint NFI SSP PMA shall notify the Organization Point of Contact of the issuance of an Organization Certificate Authority certificate from the WidePoint NFI SSP Root Certificate Authorities.

Practice Note: Where notification is not an integral component of the issuance process, CAs should proactively notify subscribers that certificates have been generated.

Upon successful completion of the WidePoint NFI SSP or Organization Subscriber identification and authentication process in accordance with this WidePoint NFI SSP CP, the WidePoint NFI SSP or Organization CPS shall detail the notification methods to the WidePoint NFI SSP or Organization Subscriber.

For WidePoint NFI SSP or Organization PIV-I Subscribers, the WidePoint NFI SSP or Organization must inform the WidePoint NFI SSP or Organization Subscriber of the creation of a certificate and make the certificate available to the WidePoint NFI SSP or Organization Subscriber.

4.4 Certificate Acceptance

Before a WidePoint NFI SSP or Organization Subscriber can make effective use of its private key, the WidePoint NFI SSP or Organization Subscriber must accept the responsibilities defined in Section 9.6.3 of this WidePoint NFI SSP CP and the WidePoint NFI SSP or Organization CPS by accepting the Subscriber agreement.

4.4.1 Conduct Constituting Certificate Acceptance

A handwritten or digital signature by the WidePoint NFI SSP or Organization Subscriber or the WidePoint NFI SSP or Organization Sponsor shall be obtained during the WidePoint NFI SSP or Organization certificate application process and lack of objection to published certificate constitutes certificate acceptance by the WidePoint NFI SSP or Organization Subscriber or the WidePoint NFI SSP or Organization Sponsor. The WidePoint NFI SSP or Organization Subscriber or WidePoint NFI SSP or Organization Sponsor signature shall be collected prior to the issuance of any WidePoint NFI SSP or Organization certificate in accordance with the procedures specified in this WidePoint NFI SSP CP and the WidePoint NFI SSP or Organization CPS and before the WidePoint NFI SSP or Organization Subscriber or the WidePoint NFI SSP or Organization Sponsor shall make effective use of the private key associated with the certificate issued by the WidePoint NFI SSP or Organization. As part of the issuance process of WidePoint NFI SSP or Organization PIV-I credentials, the WidePoint NFI SSP or Organization Subscriber must accept the issued certificate during the issuance process by accepting the Subscriber obligations prior to completion of the PIV-I issuance process. This acceptance requires the WidePoint NFI SSP 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 or Organization Subscriber.

4.4.2 Publication of the Certificate by the WidePoint NFI SSP Or Organization

The WidePoint NFI SSP or Organization Certificate Authority certificates and WidePoint NFI SSP or Organization Subscriber certificates shall be published to the WidePoint NFI SSP or Organization repositories as defined in Section 2.1 and whose contents are defined by Section 2.2 of this WidePoint NFI SSP CP. Certificates that contain UUID in the subject alternative name extension, such as PIV-I Authentication or Card Authentication Certificates, shall not 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 WidePoint NFI SSP or Organization to Other Entities

The WidePoint NFI SSP shall notify the FPKIPA at least two weeks prior to a request for the issuance of a new WidePoint NFI SSP or Organization Certificate Authority certificate from the Federal Bridge Certificate Policy CA or for subordinate Certificate Authorities issued by the WidePoint NFI SSP Root Certificate Authorities for the

WidePoint NFI SSP or Organization. In addition, notification shall be provided to the FPKIPA when the new WidePoint NFI SSP or Organization Certificate Authority certificates are published and activated.

4.5 Key Pair and Certificate Usage

4.5.1 WidePoint NFI SSP or Organization Subscriber Private Key and Certificate Usage

WidePoint NFI SSP or Organization Subscribers must protect their private keys from access by other parties.

The WidePoint NFI SSP or Organization Subscriber and the WidePoint NFI SSP or Organization Sponsor in the case of device certificates shall attest to their obligations as specified in Section 9.6.3 of this WidePoint NFI SSP CP. 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 or Organization will publicly post a summary of this WidePoint NFI SSP CP 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 or Organization and use of certificates issued to WidePoint NFI SSP or Organization 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 or Organization issued certificate. Additional Relying Party obligations are stipulated in Section 9.6.4 of this WidePoint NFI SSP CP.

4.6 Certificate Renewal

Renewing a certificate means creating a new certificate with a new serial number where all certificate subject information, including the subject public key and subject key identifier, remain unchanged.

The new certificate may have an extended validity period and may include new issuer information (e.g., different CRL distribution point, AIA and/or be signed with a different issuer key).

Once renewed, the old certificate may or may not be revoked, but must not be used for requesting further renewals, re-keys, or modifications.

4.6.1 Circumstances for Certificate Renewal

The WidePoint NFI SSP or Organization shall accept requests for certificate renewal pursuant to the following circumstances for all certificate policies except PIV-I:

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

WidePoint NFI SPP or Organization Subscriber PIV-I certificates must not be renewed, except during recovery from Certificate Authority key compromise as specified in Section 5.7.3 of this WidePoint NFI SSP CP. In such cases, the renewed certificate must expire as specified in the original WidePoint NFI SPP or Organization Subscriber PIV-I certificate.

WidePoint NFI SSP or Organization Certificate Authority certificates and Delegated OCSP responder certificates may be renewed so long as the aggregated lifetime of the private key does not exceed the requirements specified in Section 6.3.2 of this WidePoint NFI SSP CP.

4.6.2 Who May Request Renewal

The WidePoint NFI SSP PMA may request renewal of WidePoint NFI SSP Root Certificate Authority cross-certificates to the FPKIMA.

For other WidePoint NFI SSP or Organization Certificate Authority certificates and Delegated OCSP responder certificates, the operating authority defined in the WidePoint NFI SSP or Organization CPS may request renewal.

For Organizations that support renewal under this WidePoint NFI SSP CP, subscriber renewal requests must be accepted only from certificate subjects, PKI Sponsors or Registration Authorities. Additionally, the WidePoint NFI SSP or Organization may perform renewal of WidePoint NFI SSP or Organization Subscriber certificates without a corresponding request, such as when the WidePoint NFI SSP or Organization Certificate Authority re-keys.

4.6.3 Processing Certificate Renewal Requests

For the WidePoint NFI SSP Root Certificate Authorities, cross-certificate renewal for reasons other than re-key of the WidePoint NFI SSP Root Certificate Authority must be approved by the FPKIPA.

When a WidePoint NFI SSP or Organization Certificate Authority re-keys, it may renew the certificates it has issued.

When certificates are renewed as a result of CA key compromise, as described in Section 4.6.1, the WidePoint NFI SSP or Organization Certificate Authority or WidePoint NFI SSP or Organization Registration Authority must verify all certificates issued since the date of compromise were issued appropriately. If the certificate cannot be verified, then it must not be renewed .

4.6.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2 of this WidePoint NFI SSP CP.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

See Section 4.4.1 of this WidePoint NFI SSP CP.

4.6.6 Publication of the Renewal Certificate by the CA

See Section 4.4.2 of this WidePoint NFI SSP CP.

4.6.7 Notification of Certificate Issuance by the CA to other Entities

See Section 4.4.3 of this WidePoint NFI SSP CP.

4.7 Certificate Re-Key

Re-key is identical to renewal except the new certificate must have a different subject public key (and serial number).

WidePoint NFI SSP or Organization Subscribers must identify themselves for the purpose of re-keying as required in Section 3.3.1.

Once re-keyed, the old certificate may or may not be revoked, but must not be reused for requesting further re-keys, renewals, or modifications.

4.7.1 Circumstances for Certificate Re-Key

Circumstances requiring certificate re-key include nearing the maximum usage period of a private key, certificate expiration, loss or compromise, issuance of a new hardware token, and hardware token failure.

Section 6.3.2 of this WidePoint NFI SSP CP establishes maximum usage periods for private keys for both WidePoint NFI SSP Root Certificate Authorities and WidePoint NFI SSP or Organization Certificate Authorities and WidePoint NFI SSP or Organization Subscribers.

4.7.2 Who May Request Certification of a New Public Key

For WidePoint NFI SSP or Organization Certificate Authority certificates and Delegated OCSP responder certificates, the corresponding operating authority may request re-key of its own certificate to the WidePoint NFI SSP PMA.

WidePoint NFI SSP or Organization Subscribers with a currently valid certificate may request re-key of the certificate. WidePoint NFI SSP or Organization Certificate Authorities and WidePoint NFI SSP or Organization Registration Authorities may request certification of a new public key on behalf of a WidePoint NFI SSP or Organization Subscriber. The human sponsor of a device may request re-key of the device certificate.

4.7.3 Processing Certificate Re-Keying Requests

Before performing re-key, the WidePoint NFI SSP or Organization Certificate Authority must identify and authenticate the requestor by performing the identification processes defined in Section 3.2 or Section 3.3 of this WidePoint NFI SSP CP.

Digitally signed Subscriber re-key requests must be validated before the re-key requests are processed.

4.7.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2 of this WidePoint NFI SSP CP.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

See Section 4.4.1 of this WidePoint NFI SSP CP.

4.7.6 Publication of the Re-Keyed Certificate by the CA

See Section 4.4.2 of this WidePoint NFI SSP CP.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3 of this WidePoint NFI SSP CP.

4.8 Certificate Modification

Modifying a certificate means creating a new certificate that has the same or a different key and a different serial number, and that differs in one or more other fields from the old certificate. Once modified, the old WidePoint NFI SSP or Organization issued certificate may or may not be revoked, but must not be reused for requesting further renewals, re-keys, or modifications.

4.8.1 Circumstances for Certificate Modification

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

A WidePoint NFI SSP or Organization Subscriber certificate may be modified if some characteristics have changed such as name change due to marriage, e-mail address, etc.

4.8.2 Who May Request Certificate Modification

The WidePoint NFI SSP PMA may request certificate modification for current cross-certificates issued to the WidePoint NFI SSP Root Certificate Authorities.

For WidePoint NFI SSP or Organization Certificate Authority certificates and Delegated OCSP responder certificates, the corresponding operating authority may request modification of its own certificate to the WidePoint NFI SSP PMA.

WidePoint NFI SSP or Organization Subscribers with a currently valid certificate may request modification of the certificate. WidePoint NFI SSP or Organization Certificate Authorities and WidePoint NFI SSP or Organization Registration Authorities may request modification on behalf of a WidePoint NFI SSP or Organization Subscriber. The human sponsor of a device may request re-key of the device certificate.

4.8.3 Processing Certificate Modification Requests

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 of this WidePoint NFI SSP CP continue to apply.

The WidePoint NFI SSP performs certificate modification at the direction of the WidePoint NFI SSP PMA. The WidePoint NFI SSP PMA may also perform certificate modification at the request of the WidePoint NFI SSP or Organization for Certificate Authorities for the following reasons:

- Modification of SubjectInfoAccess (SIA) extension; or
- Minor name changes (e.g., change CA1 to CA2) as part of key rollover procedures.

For the WidePoint NFI SSP or Organization, proof of all subject information changes must be provided to the WidePoint NFI SSP or Organization Registration Authority or other designated agent and verified before the modified certificate is issued. If the modified certificate is issued with a new (different) public key, the additional requirements specified in Section 4.7.3 in this WidePoint NFI SPP CP must also apply.

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2 of this WidePoint NFI SSP CP.

4.8.5 Conduct Constituting Acceptance of a Modified Certificate

See Section 4.4.1 of this WidePoint NFI SSP CP.

4.8.6 Publication of the Modified Certificate by the CA

See Section 4.4.2 of this WidePoint NFI SSP CP.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3 of this WidePoint NFI SSP CP.

4.9 Certificate Revocation and Suspension

Revocation requests to the WidePoint NFI SSP or Organization must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised.

All WidePoint NFI SSP or Organization Certificate Authorities must publish Certificate Revocation Lists, hereafter referred to as CRLs. The WidePoint NFI SSP PMA must notify the FPKIPA at least two weeks prior to the revocation of any WidePoint NFI SSP or Organization Certificate Authority certificate, whenever possible. For emergency revocation, WidePoint NFI SSP or Organization Certificate Authority must follow the notification procedures in Section 5.7 in this WidePoint NFI SSP CP.

4.9.1 Circumstances for Revocation

A certificate must be revoked when the binding between the subject and the subject's public key defined within the certificate is no longer considered valid. Examples of circumstances that invalidate the binding are:

- Identifying information or affiliation components of any names in the certificate becomes invalid. Examples include:
  - WidePoint NFI SSP or Organization Subscriber no longer affiliated with sponsoring entity.
  - A wild card certificate has been issued with a name where the WidePoint NFI SSP or Organization PKI Sponsor does not exercise control of the entire namespace associated with the wild card certificate.
- Privilege attributes asserted in the WidePoint NFI SSP or Organization Subscriber's certificate are reduced.
- The WidePoint NFI SSP or Organization Subscriber can be shown to have violated the stipulations of its Subscriber agreement.

- There is reason to believe the private key has been compromised.
- The WidePoint NFI SSP or Organization Subscriber or other authorized party (as defined in the WidePoint NFI SSP or Organization CPS) asks for their certificate to be revoked.
- The failure of a WidePoint NFI SSP or Organization Certificate Authority to adequately adhere to the requirements of this WidePoint NFI SSP CP or the approved WidePoint NFI SSP or Organization CPS.

There are three circumstances under which certificate authority certificates issued by the WidePoint NFI SPP will be revoked:

- The WidePoint NFI SSP PMA requests an WidePoint NFI SSP Certificate Authority certificate be revoked.
- The WidePoint NFI SSP PMA receives an authenticated request from a previously designated official of the Organization responsible for the Certificate Authority.
- The WidePoint NFI SSP or Organization Operational personnel determine that an emergency has occurred that may impact the integrity of the certificates issued by the WidePoint NFI SSP or Organization. Under such circumstances, the following individuals may authorize immediate certificate revocation:
  - The WidePoint NFI SSP PMA Chair, or
  - Other personnel as designated by the WidePoint NFI SSP PMA Chair.

The WidePoint NFI SSP PMA must meet as soon as practicable to review the emergency revocation.

The WidePoint NFI SSP or Organization must, at a minimum, revoke certificates for the reason of key compromise upon receipt of an authenticated request from an appropriate entity.

For certificates that express an organizational affiliation, the WidePoint NFI SSP or Organization must require that the organization inform the WidePoint NFI SSP or Organization of any changes in the subscriber affiliation. If the affiliated organization no longer authorizes the affiliation of a WidePoint NFI SSP or Organization Subscriber, the WidePoint NFI SSP or Organization must revoke any certificates issued to that WidePoint NFI SSP or Organization Subscriber containing the organizational affiliation. If an organization terminates its relationship with a WidePoint NFI SSP or Organization such that it no longer provides affiliation information, the WidePoint NFI SSP or Organization must revoke all certificates affiliated with that organization.

If it is determined that revocation is required, the associated certificate must be revoked and placed on the CRL. Revoked certificates must be included on all new publications of the certificate status information until the certificates expire.

4.9.2 WHO CAN REQUEST A REVOCATION

The following authorized parties may request a revocation of a WidePoint NFI SSP or Organization certificate:

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

If any individual has reason to believe that a WidePoint NFI SSP or Organization issued certificate private key has been compromised, that individual is required to notify the WidePoint NFI SSP or Organization of the compromise suspicion. It is the responsibility of the WidePoint NFI SSP or Organization, in particular a WidePoint NFI SSP or Organization Registration Authority, to investigate the information and determine if certificate revocation is warranted, based on communications with either the WidePoint NFI SSP or Organization Subscriber that is identified by the suspected compromised certificate or an organization representative such as the WidePoint NFI SSP or Organization PKI Point of Contact for that organization or an employee of the organization who has been duly appointed as a WidePoint NFI SSP or Organization Local Registration Authority for the WidePoint NFI SSP or Organization. The WidePoint NFI SSP or Organization Registration Authority shall verify the WidePoint NFI SSP

Subscriber Name, organization affiliation and email address associated with the certificate to be revoked. If there is ambiguity, the WidePoint NFI SSP or Organization shall 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 or Organization Registration Authority shall document the reasons for the revocation and shall revoke the certificates identified in the revocation request. The WidePoint NFI SSP or Organization shall send a written notice and brief explanation for the revocation to the WidePoint NFI SSP or Organization Subscriber unless directed otherwise by the FPKIPA, the WidePoint NFI SSP PMA or a court of competent jurisdiction.

4.9.3 PROCEDURE FOR REVOCATION REQUEST

Revocation requests of human or device WidePoint NFI SSP or Organization Subscriber certificates may be made through 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). The acceptable methods for revocation requests shall be defined in the WidePoint NFI SSP or Organization CPS.

The WidePoint NFI SSP or Organization must revoke certificates upon receipt of sufficient evidence of compromise or loss of the WidePoint NFI SSP or Organization Subscriber's corresponding private key. Where WidePoint NFI SSP or Organization Subscribers use hardware tokens, but excluding PIV-I certificates, revocation is optional if all the following conditions are met:

- the revocation request was not for key compromise;
- the cryptographic module does not permit the user to export the signature private key;
- the WidePoint NFI SSP or Organization Subscriber surrendered the token to the WidePoint NFI SSP or Organization;
- the token was zeroized or destroyed promptly upon surrender;
- the token has been protected from malicious use between surrender and zeroization or destruction.

For PIV-I and in all other cases not identified above, revocation of the certificates is mandatory. Even where all the above conditions have been met, revocation of the associated certificates is recommended.

The WidePoint NFI SSP or Organization must collect and destroy PIV-I Cards from WidePoint NFI SSP or Organization Subscribers whenever the cards are no longer valid, whenever possible. The WidePoint NFI SSP or Organization must record destruction of PIV-I Cards.

If it is determined that a private key used to authorize the issuance of one or more certificates may have been compromised, all certificates directly or indirectly authorized by that private key since the date of actual or suspected compromise must be revoked or must be verified as appropriately issued.

4.9.4 REVOCATION REQUEST GRACE PERIOD

The revocation request grace period is the time available to the WidePoint NFI SSP or Organization Subscriber within which the subscriber must make a revocation request after reasons for revocation have been identified.

In the case of key compromise, the WidePoint NFI SSP or Organization are required to request revocation within one hour of confirmation of the compromise.

WidePoint NFI SSP or Organization Subscriber certificates shall be revoked upon request as soon as the need can be verified. A WidePoint NFI SSP or Organization Subscriber, or their sponsoring organization's WidePoint NFI SSP or Organization PKI Point of Contact or an Organization executive with approval authority if the Organization PKI Point of Contact is unavailable for any reason, WidePoint NFI SSP or Organization personnel must request revocation from the WidePoint NFI SSP or Organization as soon as the need for revocation has been determined.

4.9.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

WidePoint NFI SSP or Organization Certificate Authorities operating under this WidePoint NFI SSP Certificate Policy are revoked once all necessary notification periods have elapsed.

All WidePoint NFI SSP or Organization Certificate Authorities shall process revocation requests as quickly as practical upon receipt of an authenticated revocation request but as an operating practice within two hours or receipt. The WidePoint NFI SSP or Organization Subscriber, or their sponsoring organization, must request revocation from WidePoint NFI SSP or Organization as soon as the need for revocation has been determined. Revocation requests for WidePoint NFI SSP PIV-I credentials shall be processed immediately upon receipt by the WidePoint NFI SSP or Organization Card Management System which then authenticates to the appropriate WidePoint NFI SSP or Organization Certificate Authority and revokes the certificates associated with the WidePoint NFI SSP or Organization Subscriber PIV-I credential. All revocations requests received within two hours of the next CRL issuance shall 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 CP.

4.9.6 Revocation Checking Requirements for Relying Parties

It is the responsibility of the Relying Party to verify that WidePoint NFI SSP or Organization 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 or Organization 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 or Organization Subscriber certificate against the CRL, of the WidePoint NFI SSP or Organization Certificate Authority that issued the WidePoint NFI SSP or Organization 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 or Organization Subscriber certificate or make an informed decision to accept the risk, responsibility, and consequences for using a WidePoint NFI SSP or Organization Subscriber certificate whose authenticity cannot be guaranteed to the standards of the WidePoint NFI SSP or Organization CPS, this WidePoint NFI SSP CP, and Federal Bridge Certificate Policy.

The following text shall be included in the WidePoint NFI SSP or Organization Subscriber Agreement and posted on the WidePoint NFI SSP or Organization 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

For this WidePoint NFI SSP CP, CRL issuance encompasses both CRL generation and publication.

CRLs shall be published periodically, even if there are no changes to be made, to ensure timeliness of information. CRLs may be issued more frequently than specified below.

WidePoint NFI SSP or Organization Certificate Authorities that issue certificates to subscribers or operate online must issue CRLs at least once every 24 hours, and the nextUpdate time in the CRL may be no later than 48 hours after issuance time (i.e., the thisUpdate time).

For WidePoint NFI SSP or Organization Certificate Authorities that are operated in an off-line manner, routine CRLs may be issued less frequently than specified above if the WidePoint NFI SSP or Organization Certificate Authority only issues:

- Certificate Authority Certificates
- (optionally) Certificate Status Server certificates, and
- (optionally) end user certificates solely for the administration of a WidePoint NFI SSP or Organization Certificate Authority, and
- (optionally) end user certificates that contain the contentSigning EKU.

An offline WidePoint NFI SSP or Organization Certificate Authority may incorporate locally attached network equipment such as an HSM or storage array. The WidePoint NFI SSP or Organization Certificate Authority system

and any such locally attached network equipment must be completely isolated (air-gapped) from all other networks and computing systems.

However, the interval between routine CRLs shall not exceed 35 days.

All WidePoint NFI SSP or Organization Certificate Authorities must meet the requirements specified in section 4.9.12 of this WidePoint NFI SPP CP.

4.9.8 MAXIMUM LATENCY FOR CRLS

For WidePoint NFI SSP or Organization Certificate Authorities that operate online, CRLs must be published within 4 hours of generation.

For WidePoint NFI SSP or Organization Certificate Authorities that operate offline, pre-generated CRLs intended for publication more than 4 hours after generation must be protected in the same manner as the WidePoint NFI SSP or Organization Certificate Authority. All pre-generated CRLs not yet published must be securely destroyed whenever the WidePoint NFI SSP or Organization Certificate Authority revokes any certificate. The WidePoint NFI SSP or Organization CPS must describe protections and processes used for generation and protection of any pre-generated CRLs.

Furthermore, each CRL must be published no later than the time specified in the nextUpdate field of the previously issued CRL for same scope.

Note: If pre-generation of CRLs is implemented, the thisUpdate field will be the date of generation.

4.9.9 ONLINE REVOCATION/STATUS CHECKING AVAILABILITY

The latency of certificate status information must meet or exceed the requirements for CRL issuance stated in 4.9.7 in this WidePoint NFI SSP CP.

OCSP services must be designed and implemented so as to provide 99% availability overall and limit scheduled down-time to 0.5% annually, with resources sufficient to provide a response time of ten (10) seconds or less under normal operating conditions.

For WidePoint NFI SSP or Organization Subscriber PIV-I certificates, WidePoint NFI SSP or Organization Certificate Authorities must support on-line status checking via OCSP [RFC 6960].

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 or Organization must support CRLs. Client software using on-line revocation checking need not obtain CRLs.

4.9.11 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE

A WidePoint NFI SSP or Organization Certificate Authority may use other methods to publicize the certificates it has revoked. Any alternative method must meet the following requirements:

- The alternative method must be described in the WidePoint NFI SSP or Organization CPS.
- The alternative method must provide authentication and integrity services commensurate with the assurance level of the certificate being verified.
- The alternative method must meet the issuance and latency requirements for CRLs stated in Sections 4.9.7 and 4.9.8 of this WidePoint NFI SSP CP.

4.9.12 SPECIAL REQUIREMENTS RELATED TO KEY COMPROMISE

For WidePoint NFI SSP or Organization Certificate Authority, when a certificate is revoked because of compromise, or suspected compromise, of a private key, an emergency CRL must be published within 18 hours after notification.

4.9.13 Circumstances for Suspension and Restoration

The WidePoint NFI SSP or Organization does not support certificate suspension for Certificate Authorities covered by this WidePoint NFI SSP CP. WidePoint NFI SSP or Organization 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 of this WidePoint NFI SSP CP. In addition, WidePoint NFI SSP or Organization CMSs must be 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

For the WidePoint NFI SSP or Organization that supports suspension and restoration, those authorized to request suspension and restoration of a certificate must be identified in the WidePoint NFI SSP or Organization CPS.

4.9.15 Procedure for Suspension Requests

For the WidePoint NFI SSP or Organization that supports suspension and restoration, all suspended certificate serial numbers must be populated on a full CRL within a timeframe specified in Section 4.9.7 of this WidePoint NFI SSP CP. The reason code CRL entry extension shall be populated with "certificateHold." Restored certificate serial numbers must not be present on the next full CRL published by the WidePoint NFI SSP or Organization Certificate Authority.

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 must include:

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

If a WidePoint NFI SSP or Organization Certificate Authority or a WidePoint NFI SSP or Organization Card Management System conducts certificate suspensions and restorations in an automated fashion (e.g., without a formal request outlined above), the circumstances or parameters associated with those automated suspensions and restorations must be documented in the WidePoint NFI SSP or Organization CPS.

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

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

4.9.16 Limits on Suspension Period

For WidePoint NFI SSP or Organization Certificate Authorities that support suspension, the maximum time period a certificate may be suspended must be specified in the WidePoint NFI SSP or Organization CPS. The WidePoint NFI SSP or Organization CPS must describe in detail how this maximum suspension period is enforced. If the WidePoint

NFI SSP or Organization Subscriber has not removed the certificate from hold (suspension) within that period, the certificate must be revoked. Certificates must not 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

See Section 4.9.9 for OCSP.

If additional certificate status services are supported, they must be described in the WidePoint NFI SSP or Organization CPS.

4.10.1 OPERATIONAL CHARACTERISTICS

Where applicable this must be described in the WidePoint NFI SSP or Organization CPS.

4.10.2 SERVICE AVAILABILITY

Where applicable this must be described in the WidePoint NFI SSP or Organization CPS.

4.10.3 OPTIONAL FEATURES

Where applicable this must be described in the WidePoint NFI SSP or Organization CPS.

4.11 END OF SUBSCRIPTION

Subscription to the WidePoint NFI SSP is synonymous with the validity period of the WidePoint NFI SSP or Organization Subscriber's certificate issued by a WidePoint NFI SSP or Organization Certificate Authority. The subscription ends when the WidePoint NFI SSP or Organization 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 or Organization must support key escrow and recovery for private keys associated with encryption certificates.

4.12.1 KEY ESCROW AND RECOVERY POLICY AND PROCEDURES

WidePoint NFI SSP or Organization Certificate Authority private keys shall never be escrowed.

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

WidePoint NFI SSP or Organization Subscriber signature keys shall never escrowed.

4.12.1.1 Key Escrow Process and Responsibilities

WidePoint NFI SSP or Organization Subscriber private keys (i.e., decryption private keys) associated with a key management certificate must be securely escrowed by a WidePoint NFI SSP or Organization Key Encryption Database. The WidePoint NFI SSP or Organization must ensure that the keys are escrowed successfully prior to issuance of the key management certificates.

WidePoint NFI SSP or Organization Subscriber private keys must be protected during transit and storage using cryptography at least as strong as the key being escrowed.

WidePoint NFI SSP or Organization Subscribers must be notified that the private keys associated with their encryption certificates will be escrowed.

Practice Note: Escrowed keys must be protected at no less than the level of security in which they are generated, delivered, and protected by the subscriber.

Under no circumstances will a WidePoint NFI SSP or Organization Subscriber signature key be escrowed.

4.12.1.2 Key Recovery Process and Responsibilities

Communications between the various key recovery participants (WidePoint NFI SSP or Organization Key Encryption Databases, WidePoint NFI SSP or Organization Data Decryption Servers, WidePoint NFI SSP or Organization Key Recovery Agent, WidePoint NFI SSP or Organization Key Recovery Official, Requestor, and WidePoint NFI SSP or Organization Subscriber) must be secured from protocol threats such as disclosure, modification, replay, and substitution. The strength of all cryptographic protocols must be equal to or greater than that of the keys they protect.

During delivery, WidePoint NFI SSP or Organization escrowed keys must be protected against disclosure to any party except the Requestor.

When any mechanism that includes a shared secret (e.g., a password) is used to protect the key in transit, the mechanism must ensure that the Requestor and the transmitting party are the only holders of this shared secret.

WidePoint NFI SSP or Organization Subscribers may use electronic or manual means to request their own escrowed keys from the WidePoint NFI SSP or Organization. The WidePoint NFI SSP or Organization Subscriber may submit the request to the WidePoint NFI SSP or Organization Key Encryption Database, WidePoint NFI SSP or Organization Key Recovery Agent or WidePoint NFI SSP or Organization Key Recovery Official. If the request is made electronically, the WidePoint NFI SSP or Organization Subscriber must digitally sign the request or authenticate to a recovery service using an associated authentication or signature certificate with an assurance level equal to or greater than that of the escrowed key. Manual requests must be made in person and include proper identity verification by the WidePoint NFI SSP or Organization Key Recovery Agent in accordance with Section 3.2.3.1 of this WidePoint NFI SSP CP.

Third-Party Requestors may use electronic or manual means to request the WidePoint NFI SSP or Organization Subscribers' escrowed keys. The Requestor must submit the request to the WidePoint NFI SSP or Organization Key Recovery Agent or WidePoint NFI SSP or Organization Key Recovery Official. If the request is made electronically, the Requestor must digitally sign the request using a trusted authentication or signature certificate, as determined by the WidePoint NFI SSP or Organization, with an assurance level equal to or greater than that of the escrowed key. Manual requests must include proper identity verification by the WidePoint NFI SSP or Organization Key Recovery Agent in accordance with Section 3.2.3.1 of this WidePoint NFI SSP CPS.

WidePoint NFI SSP or Organization Data Decryption Servers must use electronic means to request WidePoint NFI SSP or Organization Subscribers' escrowed keys. Requests must be authenticated as specified in Section 3.5.5 in this WidePoint NFI SSP CP.

Third party key recovery in and of itself does not require revocation of a WidePoint NFI SSP or Organization Subscriber certificate. This does not prohibit WidePoint NFI SSP or Organization Subscribers from requesting revocation of their own certificates for any reason.

4.12.1.2.1 Key Recovery Through WidePoint NFI SSP or Organization Key Recovery Agent

WidePoint NFI SSP or Organization Key Recovery Agents must provide access to a copy of an escrowed key only in response to a properly authenticated and authorized key recovery request. Such access requires the actions of at least two WidePoint NFI SSP or Organization Key Recovery Agents. All copies of escrowed keys must be protected using two-person control procedures during recovery and delivery to the authenticated and authorized Requestor. Split key or password procedures are considered adequate two-person controls, provided they comply with technical controls in Section 6.2.2 of this WidePoint NFI SSP CP.

Practice Note: A combination of physical, procedural, and technical security controls can be used to enforce continuous two-person control during recovery and delivery of escrowed keys. The WidePoint NFI SSP or Organization Key Recovery Systems should be designed to maximize the ability to enforce two-person control technically.

WidePoint NFI SSP or Organization Key Recovery Agents are not required to notify subscribers of a third-party key recovery.

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

4.12.1.2.2 Automated Self-Recovery

A current WidePoint NFI SSP or Organization Subscriber's escrowed keys may be provided directly to the Subscriber without imposition of two-person control requirements. WidePoint NFI SSP or Organization Key Encryption Databases must only provide escrowed keys to current WidePoint NFI SSP or Organization Subscribers without two-person control upon:

- Verifying that the authenticated identity of the requestor is the same as the WidePoint NFI SSP or Organization Subscriber associated with the escrowed keys being requested;
- Sending notification to the WidePoint NFI SSP or Organization Subscriber of all attempts (successful or unsuccessful) to recover the WidePoint NFI SSP or Organization Subscriber's escrowed keys that are made by entities claiming to be the WidePoint NFI SSP or Organization Subscriber. If the WidePoint NFI SSP or Organization Key Encryption Database does not have information (e.g., an e-mail address) necessary to send notification to the WidePoint NFI SSP or Organization Subscriber of a key recovery request, then the WidePoint NFI SSP or Organization Key Encryption Database must not provide the WidePoint NFI SSP or Organization Subscriber with the requested key material using the automated recovery process

Practice Note: Where possible, the e-mail address will be from the subject alternative name field of the certificate being recovered.

- 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 escrowed keys are encrypted during transmission using cryptography of equal or greater strength than provided by the escrowed key.

4.12.1.2.3 Key Recovery During Token Issuance

When a WidePoint NFI SSP or Organization Subscriber is issued a new certificate on a hardware token, private key management keys for the WidePoint NFI SSP or Organization Subscriber may be recovered as part of the issuance process as long as the WidePoint NFI SSP or Organization Key Encryption Database uses secure means, such as Global Platform Secure Channel Protocol, to inject the key history onto the hardware token directly.

The hardware token shall meet FIPS 140 Level 2 hardware requirements and the key shall be injected into the token such that it is not thereafter exportable.

4.12.1.2.4 Key Recovery by Data Decryption Server

A WidePoint NFI SSP or Organization Data Decryption Server or organization Data Decryption Server must be under two-person control, as is required for any WidePoint NFI SSP or Organization Certificate Authority or WidePoint NFI SSP or Organization Key Encryption Database. The WidePoint NFI SSP or Organization Key Encryption Database must performs the following activities prior to releasing the key:

- Authenticating the Requestor as a legitimate WidePoint NFI SSP or Organization Data Decryption Server.
- Verifying that the WidePoint NFI SSP 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 or Organization Key Recovery Agent, WidePoint NFI SSP or Organization Key Recovery Official or another trusted role from accessing WidePoint NFI SSP or Organization Subscriber encryption keys, a combination of physical, procedural, and technical security controls must be used to enforce continuous two-person control on the WidePoint NFI SSP or Organization Data Decryption Servers. The WidePoint NFI SSP or Organization Data Decryption Servers must be designed to maximize the ability to enforce two-person control technically.

4.12.1.3 Who can Submit a Key Recovery Application

WidePoint NFI SSP or Organization Subscribers may request recovery of their own escrowed keys. Key recovery may also be requested by internal Third-Party Requestor permitted by the Issuing Organization policy, and by authorized external Third-Party Requestors (e.g., law enforcement personnel with a court order from a competent court).

4.12.1.3.1 Requestor Authorization Validation

A WidePoint NFI SSP or Organization Key Recovery Agent or a WidePoint NFI SSP or Organization Key Recovery Official, as an intermediary for the WidePoint NFI SSP or Organization Key Recovery Agent, must validate the authorization of the Requestor. WidePoint NFI SSP or Organization Key Recovery Agents should consult with Issuing Organization management and/or legal counsel, as appropriate.

Issuing Organizations must determine internal notification requirements for External Third-Party key recovery requests and account for situations where the law requires the WidePoint NFI SSP or Organization Key Encryption Database to release the WidePoint NFI SSP or Organization Subscriber's private key without organizational notification.

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

4.12.1.3.2 WidePoint NFI SSP or Organization Subscriber Authorization Validation

Current WidePoint NFI SSP or Organization Subscribers are authorized to recover their own escrowed key material.

4.12.1.3.3 WidePoint NFI SSP or Organization Key Recovery Agent Authorization Validation

The WidePoint NFI SSP or Organization Key Encryption Database must verify that the individual WidePoint NFI SSP or Organization Key Recovery Agent has the appropriate privileges to obtain the keys for the identified WidePoint NFI SSP or Organization Subscriber's affiliated organization.

4.12.1.3.4 WidePoint NFI SSP or Organization Key Recovery Official Authorization Validation

The WidePoint NFI SSP or Organization Key Encryption Database or the WidePoint NFI SSP or Organization Key Recovery Agent must verify that the WidePoint NFI SSP or Organization Key Recovery Official is authorized to request keys for the identified WidePoint NFI SSP or Organization Subscriber.

4.12.1.3.5 Data Decryption Server Authorization Validation

A WidePoint NFI SSP or Organization Key Encryption Database shall verify that a WidePoint NFI SSP or Organization Data Decryption Service recovery request falls within the organizational scope for which the WidePoint NFI SSP or 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

WidePoint NFI SSP or Organization Certificate Authority equipment must be protected from unauthorized access while the cryptographic module is installed and activated. The WidePoint NFI SSP or Organization Certificate Authority must implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. WidePoint NFI SSP or Organization Certificate Authority cryptographic tokens must be protected against theft, loss, and unauthorized use.

All the physical control requirements specified below apply equally to all WidePoint NFI SSP or Organization Certificate Authorities, and any remote workstations used to administer the WidePoint NFI SSP or Organization Certificate Authorities except where specifically noted.

5.1.1 SITE LOCATION AND CONSTRUCTION

The location and construction of the facility housing WidePoint NFI SSP or Organization Certificate Authority equipment, as well as sites housing remote workstations used to administer the WidePoint NFI SSP or Organization Certificate Authorities, must be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, must provide robust protection against unauthorized access to all WidePoint NFI SSP or Organization Certificate Authority equipment and records.

5.1.2 PHYSICAL ACCESS

5.1.2.1 Physical Access for WidePoint NFI SSP or Organization Certificate Authority Equipment

The WidePoint NFI SSP or Organization Certificate Authority equipment, to include remote workstations used to administer the WidePoint NFI SSP or Organization Certificate Authorities, must always be protected from unauthorized access. The security mechanisms must be commensurate with the level of threat in the equipment environment. Since the WidePoint NFI SSP or Organization must plan to issue certificates at all levels of assurance, it is operated and controlled on the presumption that it will be issuing at least one High Assurance certificate.

The physical security requirements pertaining to WidePoint NFI SSP or Organization Certificate Authorities that issue Medium, Medium Hardware, or High assurance certificates:

- Ensure no unauthorized access to the hardware is permitted.
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers.
- Ensure manual or electronic monitoring for unauthorized intrusion at all times.
- Ensure an access log is maintained and inspected periodically.
- Require two-person physical access control to both the cryptographic module and computer systems.

Practice Note: Multiparty physical access control to WidePoint NFI SSP or Organization Certificate Authority equipment can be achieved by any combination of two or more trusted roles (see Section 5.2.2) as long as the tasks being conducted are segregated in accordance with the requirements and duties defined for each trusted role. As an example, a Certificate Authority Administrator and a System Administrator might access the site housing the WidePoint NFI SSP or Organization Certificate Authority equipment to perform a tape backup, but only the System Administrator may perform the tape backup.

Removable cryptographic modules, activation information used to access or enable cryptographic modules, and other sensitive WidePoint NFI SSP or Organization Certificate Authority equipment must be placed in secure containers when not in use. Activation data must be either memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module and must not be stored with the cryptographic module or removable hardware associated with remote workstations used to administer the WidePoint NFI SSP or Organization Certificate Authority.

A security check of the facility housing the WidePoint NFI SSP or Organization Certificate Authority equipment or remote workstations used to administer the WidePoint NFI SSP or Organization Certificate Authorities operating under this WidePoint NFI SSP CP must occur if the facility is to be left unattended. At a minimum, the check must verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when "open" and secured when "closed"; and for offline WidePoint NFI SSP or Organization Certificate Authorities, that all equipment other than the repository is shut down).
- Any security containers are properly secured.
- Physical security systems (e.g., door locks, vent covers) are functioning properly.
- The area is secured against unauthorized access.

A person or group of persons must be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance must be maintained. If the facility is not continuously attended, the last person to depart must initial a sign-out sheet that indicates the date and time and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.2.2 Physical Access for WidePoint NFI SSP or Organization Registration Authority Equipment

WidePoint NFI SSP or Organization Registration Authority equipment must be protected from unauthorized access while the cryptographic module is installed and activated. The WidePoint NFI SSP or Organization Registration Authority must implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms must be commensurate with the level of threat in the WidePoint NFI SSP or Organization Registration Authority equipment environment.

5.1.2.3 Physical Access for WidePoint NFI SSP or Organization Certificate Status Services Equipment

Physical access control requirements for WidePoint NFI SSP or Organization Certificate Status Services equipment that has signing capability must meet the WidePoint NFI SSP or Organization Certificate Authority physical access requirements specified in Section 5.1.2.1 of this WidePoint NFI SSP CP. WidePoint NFI SSP or Organization Certificate Status Services equipment that does not have a private signing key and only distribute pre-generated OCSP responses are not required to meet these requirements.

5.1.2.4 Physical Access for WidePoint NFI SSP or Organization Card Management System Equipment

Physical access control requirements for WidePoint NFI SSP or Organization Card Management System equipment containing a PIV-I content signing key must meet the WidePoint NFI SSP or Organization Certificate Authority physical access requirements specified in Section 5.1.2.1 of this WidePoint NFI SSP CP.

5.1.2.5 Physical Access for WidePoint NFI SSP or Organization Key Encryption Database Equipment

Physical access control requirements for WidePoint NFI SSP or Organization Key Encryption Database equipment that store private keys must meet the WidePoint NFI SSP or Organization Certificate Authority physical access requirements specified in Section 5.1.2.1 of this WidePoint NFI SSP CP.

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

Physical access control requirements for any WidePoint NFI SSP or Organization Data Decryption Server equipment that store private keys must meet the WidePoint NFI SSP or Organization Certificate Authority physical access requirements specified in Section 5.1.2.1 of this WidePoint NFI SSP CP.

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

WidePoint NFI SSP or Organization Key Recovery Agent or WidePoint NFI SSP or Organization Key Recovery Official equipment must be protected from unauthorized access while the cryptographic module is installed and activated. The WidePoint NFI SSP or Organization Key Recovery Agent or WidePoint NFI SSP or Organization Key Recovery Official must implement physical access controls to reduce the risk of equipment tampering even when the

cryptographic module is not installed and activated. These security mechanisms must be commensurate with the level of threat in the equipment environment.

5.1.3 POWER AND AIR CONDITIONING

The WidePoint NFI SSP or Organization Certificate Authority must have sufficient alternative power supply in the event of a primary power source failure to either maintain WidePoint NFI SSP or Organization Certificate Authority operations or, at a minimum, prevent loss of data. The repositories (containing WidePoint NFI SSP or Organization Certificate Authority certificates, CRLs, and pre-generated OCSP responses) must be provided with uninterrupted power sufficient for a minimum of six (6) hours operation in the absence of commercial power, to maintain availability and avoid denial of service.

5.1.4 WATER EXPOSURE

WidePoint NFI SSP or Organization Certificate Authority equipment must be installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors).

Water exposure from fire prevention and protection measures (e.g., sprinkler systems) are excluded from this requirement.

5.1.5 FIRE PREVENTION AND PROTECTION

The WidePoint NFI SSP or Organization must comply with local commercial building codes for fire prevention and protection.

5.1.6 MEDIA STORAGE

Sensitive WidePoint NFI SSP or Organization Certificate Authority media must be stored to protect it from accidental damage (water, fire, electromagnetic) and unauthorized physical access.

5.1.7 WASTE DISPOSAL

Sensitive media and documentation that are no longer needed for operations must be destroyed in a secure manner. For example, sensitive paper documentation must be shredded, burned, or otherwise rendered unrecoverable.

5.1.8 OFF-SITE BACKUP

WidePoint NFI SSP or Organization Certificate Authority backups sufficient to recover from system failure must be made on a periodic schedule. Backups must be performed and stored off-site not less than once per week. At least one full backup copy must be stored at an off-site location separate from the WidePoint NFI SSP or Organization Certificate Authority equipment. Only the latest full backup need to be retained. The backup must be stored at a site with physical and procedural controls commensurate to that of the operational WidePoint NFI SSP or Organization Certificate Authority.

For offline WidePoint NFI SSP or Organization Certificate Authorities, the backup must be performed each time the system is turned on or once per week, whichever is less frequent.

Requirements for WidePoint NFI SSP or Organization Certificate Authority private key backup are specified in Section 6.2.4 of this WidePoint NFI SSP CP.

5.2 PROCEDURAL CONTROLS

5.2.1 TRUSTED ROLES

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The personnel selected to fill these roles must be extraordinarily responsible or the integrity of the WidePoint NFI SSP or Organization Certificate Authority is weakened. The functions performed in these roles form the basis of trust for the entire WidePoint NFI SSP or Organization PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion. An auditable record must be

created identifying when personnel are added or removed from a trusted role, as well as who added or removed them from the role. The individual who authorized the role assignment, or any series of role assignments over a given period of time, must also be traceable via audit and archive records.

Trusted Role appointments must be documented and archived as defined in Section 5.4 and Section 5.5 of this WidePoint NFI SSP CP.

5.2.1.1 Certification Authority Trusted Roles

The requirements of this policy are defined in terms of four roles; implementing Organizations under this WidePoint NFI SSP CP may define additional roles provided the following separation of duties are enforced.

1. Administrator – authorized to install, configure, and maintain the WidePoint NFI SSP or Organization Certificate Authority, or, optionally, WidePoint NFI SSP or Organization Key Encryption Database or WidePoint NFI SSP or Organization Data Decryption Server; establish and maintain system accounts; configure audit parameters; and generate PKI component keys.
2. Officer – authorized to request, approve, or perform certificate issuance, revocations, or key recovery, as appropriate.
3. Auditor – authorized to review, maintain, and archive audit logs.
4. Operator – authorized to perform system backup and recovery.

Administrators do not issue certificates to WidePoint NFI SSP or Organization Subscribers.

These four roles are employed at the WidePoint NFI SSP or Organization Certificate Authority, WidePoint NFI SSP or Organization Card Management System, WidePoint NFI SSP or Organization Key Encryption Database, WidePoint NFI SSP or Organization Data Decryption Server, and WidePoint NFI SSP or Organization Certificate Status Server locations as appropriate. Separation of duties must comply with Section 5.2.4 and requirements for two-person control with Section 5.2.2 of this WidePoint NFI SSP CP, regardless of the titles and numbers of Trusted Roles.

5.2.1.2 Registration Authority Trusted Roles

A WidePoint NFI SSP or Organization Registration Authority may be considered an Officer as defined in Section 5.2.1.1 of this WidePoint NFI SSP CP and is responsible for:

- verifying initial identity, as described in Section 3.2;
- entering WidePoint NFI SSP or Organization Subscriber information, and verifying correctness;
- securely communicating requests to and responses from the WidePoint NFI SSP or Organization Certificate Authority;
- receiving and distributing WidePoint NFI SSP or Organization Subscriber certificates;

The WidePoint NFI SSP or Organization Registration Authority role is highly dependent on implementation and local requirements. The responsibilities and controls for WidePoint NFI SSP or Organization Registration Authorities shall be explicitly described in the WidePoint NFI SSP or Organization CPS of a WidePoint NFI SSP or Organization Certificate Authority if the WidePoint NFI SSP or Organization Certificate Authority uses a WidePoint NFI SSP or Organization Registration Authority.

5.2.2 Number of Persons Required for Task

Two or more persons are required for WidePoint NFI SSP or Organization Certificate Authorities operating under this WidePoint NFI SSP CP:

- WidePoint NFI SSP or Organization Certificate Authority, WidePoint NFI SSP or Organization Key Encryption Database or WidePoint NFI SSP or Organization Data Decryption Server key generation.
- WidePoint NFI SSP or Organization Certificate Authority signing key activation.
- WidePoint NFI SSP or Organization Certificate Authority, WidePoint NFI SSP or Organization Key Encryption Database or WidePoint NFI SSP or Organization Data Decryption Server private key backup.

Where multiparty control is required, at least one of the participants must be an Administrator. All participants must serve in a trusted role as defined in Section 5.2.1 of this WidePoint NFI SSP CP. Multiparty control for logical access must not be achieved using personnel that serve in the Auditor Trusted Role.

5.2.3 Identification and Authentication for Each Role

An individual must identify and authenticate before being permitted to perform any actions set forth above for that role or identity.

5.2.4 Roles Requiring Separation of Duties

Individual personnel must be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume only one of the Officer, Administrator, and Auditor roles, but any individual may assume the Operator role. The WidePoint NFI SSP or Organization Certificate Authority, WidePoint NFI SSP or Organization Card Management System, and WidePoint NFI SSP or Organization Registration Authority software and hardware must identify and authenticate its users and must ensure that no user identity can assume both an Administrator and an Officer role, assume both the Administrator and Auditor roles, or assume both the Auditor and Officer roles. No individual may have more than one identity.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

All persons filling trusted roles must be selected on the basis of loyalty, trustworthiness, and integrity. For the WidePoint NFI SSP and Organizations operating under this WidePoint NFI SSP CP, each person filling a trusted role must satisfy at least one of the following:

- The person must be a citizen of the country where the WidePoint NFI SSP or Organization Certificate Authority is located; or
- For PKIs operated on behalf of multinational governmental organizations, the person must be a citizen of one of the member countries; or
- For PKIs located within the European Union, the person must be a citizen of one of the member States of the European Union; or
- For PKIs other than the FBCA and Federal Agency PKIs, the person must have a security clearance equivalent to U.S. Secret or higher issued by a NATO member nation or major non-NATO ally as defined by the International Traffic in Arms Regulation (ITAR) – 22 CFR 120.32; or
- For WidePoint NFI SSP or Organization Registration Authority personnel only, in addition to the above, the person may be a citizen of the country where the WidePoint NFI SSP or Organization Registration Authority is located.

5.3.2 Background Check Procedures

WidePoint NFI SSP or Organization Certificate Authority personnel must receive a favorable adjudication after undergoing a background investigation covering the following areas:

- Employment;
- Education;
- Place of residence;
- Law Enforcement; and
- References.

The period of investigation must cover at least the last five years for each area, excepting the residence check which must cover at least the last three years. Regardless of the date of award, the highest educational degree must be verified.

Adjudication of the background investigation must be performed by a competent adjudication authority using a process consistent with [Executive Order 12968] or equivalent.

For Federal employees and cleared contractors:

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

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

In all cases, the reinvestigation period for a Trusted Role background check must not exceed 10 years. If a Trusted Role's national security eligibility, suitability determination, or PIV eligibility is ever suspended or revoked during their appointment, all CA accesses must be revoked until the security eligibility, suitability determination, or PIV eligibility is reinstated or a separate investigation is completed and adjudicated.

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

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the WidePoint NFI SSP or Organization Certificate Authority or WidePoint NFI SSP or Organization Registration Authority must receive comprehensive training.

Training must be conducted in the following areas:

- WidePoint NFI SSP or Organization Certificate Authority (or WidePoint NFI SSP or Organization Registration Authority) security principles and mechanisms;
- WidePoint NFI SSP or Organization Key Recovery System security principles and mechanisms;
- All PKI software versions in use on the WidePoint NFI SSP or Organization Certificate Authority (or WidePoint NFI SSP or Organization Registration Authority) system;
- All PKI duties they are expected to perform;
- Disaster recovery and business continuity procedures; and
- Stipulations of the WidePoint NFI SSP CP and the WidePoint NFI SSP or Organization CPS.

Documentation must be maintained identifying all personnel who received training and the level of training completed.

5.3.4 Retraining Frequency and Requirements

Individuals responsible for PKI roles must be aware of changes in the WidePoint NFI SSP or Organization Certificate Authority operation. Any significant change to the operations must have a training (awareness) plan, and the execution of such plan must be documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

Documentation must be maintained identifying all personnel who received retraining and the level of retraining completed.

5.3.5 Job Rotation Frequency and Sequence

Job rotation is optional. Any job rotation frequency and sequencing procedures must provide for continuity and integrity of the WidePoint NFI SSP or Organization Certificate Authority services.

Job rotation must not violate role separation. All access rights associated with a previous role must be terminated.

All job rotations must be documented. Individuals assuming an auditor trusted role must not audit their own work from a previous role.

5.3.6 Sanctions for Unauthorized Actions

A WidePoint NFI SSP or Organization Certificate Authority must take appropriate administrative and disciplinary actions against personnel who have performed actions involving the WidePoint NFI SSP or Organization Certificate Authority or its WidePoint NFI SSP or Organization Registration Authorities that are not authorized in the WidePoint NFI SSP CP, the WidePoint NFI SSP or Organization CPS, or other documented procedures.

5.3.7 Independent Contractor Requirements

Contractors fulfilling Trusted Roles must be subject to all personnel requirements stipulated in the corresponding policy.

PKI vendors who provide any services must establish procedures to ensure that any subcontractors perform in accordance with the WidePoint NFI SSP CP and the WidePoint NFI SSP or Organization CPS.

5.3.8 Documentation Supplied to Personnel

Documentation sufficient to define duties and procedures for each trusted role must be provided to the personnel filling that role.

5.4 Audit Logging Procedures

The objective of audit log processing is to review all actions to ensure they are made by authorized parties and for legitimate reasons.

At a minimum, audit records must be generated for all applicable events identified in Section 5.4.1 of this WidePoint NFI SSP CP and must be available during audit reviews and third-party audits. For a WidePoint NFI SSP or Organization Certificate Authority operated in a virtual environment, audit records must be generated for all applicable events on application software and all system software layers.

Where possible, the security audit logs must be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism must be used. All security audit logs, both electronic and non-electronic, must be retained and made available during compliance audits. Implementation and documentation of automated tools must describe how relevant events and anomalies are recorded.

Audit record reviews should be performed using an automated process and must include verification that the logs have not been tampered with, an inspection of log entries, and a root cause analysis for any alerts or irregularities.

A record of the review, all significant events, and any actions taken as a result of these reviews must be explained in an audit log summary. This review summary must be retained as part of the long-term archive.

All WidePoint NFI SSP or Organization Key Encryption Database audit records of unsuccessful key recoveries must be analyzed to determine the cause and to ensure that the WidePoint NFI SSP or Organization Key Recovery System is operating correctly and securely and is not vulnerable to unauthorized use.

Real-time alerts are neither required nor prohibited by this WidePoint NFI SSP CP.

5.4.1 Types of Events Recorded

All security auditing capabilities of CA operating system and CA applications required by this CP must be enabled during installation. At a minimum, each audit record must include the following (either recorded automatically or manually for each auditable event):

- What type of event occurred;
- Date and time when the event occurred;
- Where the event occurred (e.g., on what systems or in what physical locations);
- Source of the event;
- Outcome of the event to include success or failure; and
- Identity of any individuals, subjects, or objects/entities associated with the event.

Any request or action requiring the use of a private key controlled by the WidePoint NFI SSP or Organization Certificate Authority is an auditable event.

If out-of-band processes are used for authorization of certificate issuance, external artifacts from the process (e.g., forms, emails, etc.) must be recorded.

Practice Note: Events related to WidePoint NFI SSP or Organization Certificate Authority certificate issuance may be different from those related to WidePoint NFI SSP or Organization Subscriber certificate issuance.

The WidePoint NFI SSP and Organization Certificate Authority and WidePoint NFI SSP and Organization Key Recovery System must record the events identified in the table below, where applicable to the application, environment, or both. Where these events cannot be electronically logged, electronic audit logs must be supplemented with physical logs as necessary.

SECURITY AUDIT:

- Any changes to the Audit parameters, e.g., audit frequency, type of event audited.
- Any attempt to delete or modify the Audit logs.

IDENTIFICATION AND AUTHENTICATION:

- Platform or WidePoint NFI SSP or Organization Certificate Authority application level authentication attempts.
- The value of maximum authentication attempts has changed.
- The number of unsuccessful authentication attempts exceeds the maximum authentication attempts during user login.
- An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts.
- An Administrator changes the type of authenticator, e.g., from smart card login to password.

DATA ENTRY AND OUTPUT:

- Any additional event that is relevant to the security of the CA (such as remote or local data entry or data export); must be documented.

KEY GENERATION:

- Whenever the WidePoint NFI SSP or Organization Certificate Authority generates a key (not mandatory for single session or one-time use symmetric keys).

PRIVATE KEY LOAD AND STORAGE:

- The loading of WidePoint NFI SSP or Organization Certificate Authority, WidePoint NFI SSP or Organization Registration Authority, WidePoint NFI SSP or Organization Certificate Status Services, WidePoint NFI SSP or Organization Card Management System, or other keys used by the WidePoint NFI SSP or Organization Certificate Authority in the lifecycle management of certificates.
- All access to certificate subject private keys retained within the CA for key recovery purposes.

TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE:

- Any changes to public keys used by components of the WidePoint NFI SSP or Organization Certificate Authority to authenticate other components or authorize certificate lifecycle requests (e.g., WidePoint NFI SSP or Organization Registration Authority or WidePoint NFI SSP or Organization Card Management System trust stores).

PRIVATE AND SECRET KEY EXPORT:

- The export of private and secret keys (keys used for a single session or message are excluded).

CERTIFICATE REGISTRATION:

- All records related to certificate request authorization, approval and signature, whether generated directly on the WidePoint NFI SSP or Organization Certificate Authority or generated by a related external system or process.

CERTIFICATE REVOCATION:

- All certificate revocation requests

CERTIFICATE STATUS CHANGE APPROVAL:

- All records, including request, authorization, approval and execution related to certificate status changes (e.g., revocation, suspension, or restoration) whether generated directly on the WidePoint NFI SSP or Organization Certificate Authority or generated by a related external system or process.

CA CONFIGURATION:

- Any security-relevant changes to the configuration of the WidePoint NFI SSP or Organization Certificate Authority. The specific configuration items relevant to the environment in which the WidePoint NFI SSP or Organization Certificate Authority operates must be identified and documented.

ACCOUNT ADMINISTRATION:

- Roles and users are added or deleted.
- The access control privileges of a user account or a role are modified.

CERTIFICATE PROFILE MANAGEMENT:

- All changes to the certificate profile

CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT:

- All changes to the certificate revocation list profile.

MISCELLANEOUS:

- All records of authentication, authorization, recovery, agreement and delivery of key management keys to a key recovery requestor.
- Record of an individual being added or removed from a trusted role, and who added or removed them from the role.
- All records of authentication, authorization, recovery, agreement and delivery of key management keys to a key recovery requestor.
- Installation of the Operating System
- Installation of the WidePoint NFI SSP or Organization Certificate Authority
- Installing hardware cryptographic modules
- Removing hardware cryptographic modules
- Destruction of cryptographic modules
- System startup
- Logon attempts to WidePoint NFI SSP or Organization Certificate Authority applications
- Receipt of Hardware/Software
- Attempts to set passwords
- Attempts to modify passwords
- Backing up WidePoint NFI SSP or Organization Certificate Authority internal database
- Restoring WidePoint NFI SSP or Organization Certificate Authority internal database
- Records of manipulation of critical files (e.g., creation, renaming, moving), critical files will vary between installation, and must be identified in the relevant documentation
- The date and time any WidePoint NFI SSP or Organization Certificate Authority artifact is posted to a public repository
- Access to WidePoint NFI SSP or Organization Certificate Authority internal database
- All certificate compromise notification requests
- Loading tokens with certificates
- Shipment and receipt of tokens containing key material, or tokens that allow access to key material (e.g., HSM operator cards)
- Zeroizing tokens
- Re-key of a WidePoint NFI SSP or Organization Certificate Authority

- Configuration changes to a WidePoint NFI SSP or Organization Certificate Authority server involving:
  - Hardware
  - Software
  - Operating system
  - Patches
  - Security Profiles

PHYSICAL ACCESS / SITE SECURITY:

- Personnel access to room housing a WidePoint NFI SSP or Organization Certificate Authority.
- Access to a WidePoint NFI SSP or Organization Certificate Authority server.
- Known or suspected violations of physical security.

ANOMALIES:

- Software Error conditions.
- Software check integrity failures.
- Equipment failure.
- Electrical power outages.
- Uninterruptible Power Supply (UPS) failure.
- Network service or access failures that could affect certificate trust.
- Violations of WidePoint NFI SSP Certificate Policy.
- Violations of WidePoint NFI SSP or Organization Certification Practice Statement.
- Resetting Operating System clock.

5.4.2 FREQUENCY OF PROCESSING LOG

Audit records must be reviewed at least once every month for online WidePoint NFI SSP or Organization Certificate Authorities. For offline WidePoint NFI SSP or Organization Certificate Authorities, the audit logs must be reviewed when the system is activated or every 30 days, whichever is later. WidePoint NFI SSP or Organization Certificate Status Authority, WidePoint NFI SSP or Organization Card Management System, WidePoint NFI SSP or Organization Identity Management System and WidePoint NFI SSP or Organization Key Recovery System audit log processing frequency shall align with the WidePoint NFI SSP or Organization Certificate Authority audit log processing frequency.

5.4.3 RETENTION PERIOD FOR AUDIT LOG

Audit records must be accessible until reviewed, in addition to specific records being archived as described in Section 5.5 of this WidePoint NFI SSP CP.

Practice Note: OMB M-21-31 requires that Federal agencies maintain all audit records in active storage for a minimum of 12 months from generation.

5.4.4 PROTECTION OF AUDIT LOG

System configuration and operational procedures must be implemented together to ensure that only authorized individuals may move or archive audit records and that audit records are not modified.

Collection of the audit records from the WidePoint NFI SSP or Organization Certificate Authority system must be performed by, witnessed by or under the control of trusted roles who are different from the individuals who, in combination, command the WidePoint NFI SSP or Organization Certificate Authority signature key.

For WidePoint NFI SSP or Organization Registration Authority systems, the individual authorized to move or archive records may not hold a WidePoint NFI SSP or Organization Registration Authority Trusted Role.

Procedures must be implemented to protect audit records from deletion or destruction before they are reviewed. as described in Section 5.4.2 of this WidePoint NFI SSP CP. To protect the integrity of audit records, they must be transferred to a backup environment distinct from the environment where the audit records are generated.

5.4.5 AUDIT LOG BACKUP PROCEDURES

Audit records and audit summaries must be backed up at least monthly. If audit records are stored locally in the system where the events occur, they must be transferred to a backup environment and protected as described in Section 5.4.4 of this WidePoint NFI SSP CP. The backup procedure may be automated or manual, but must occur no less frequently than the audit log review described in Section 5.4.2 of this WidePoint NFI SSP CP.

The process for transferring the audit records to the backup environment must be documented.

5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)

The audit log collection system may or may not be external to the WidePoint NFI SSP or Organization Certificate Authority system or WidePoint NFI SSP or Organization Key Recovery System. Automated audit processes must be invoked at system (or application) startup and cease only at system (or application) shutdown. Audit collection systems must be configured such that security audit data is protected against loss (e.g., overwriting or overflow of automated log files).

If an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, operations must be suspended until the problem has been remedied.

5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT

There is no requirement to notify a subject that an event was audited. Real-time alerts are neither required nor prohibited by this policy.

5.4.8 VULNERABILITY ASSESSMENTS

WidePoint NFI SSP or Organization Certificate Authorities must perform routine vulnerability assessments of the security controls described in the applicable policy.

Automated vulnerability scans, if executed, should be run no less frequently than required by the risk rating of the component.

The methodology, tools and frequency of the vulnerability assessment must be documented.

Practice Note: The audit data should be reviewed by the auditor trusted role for events such as repeated failed actions, requests for privileged information, attempted access of system files, requests for escrowed keys, attempted access of escrowed keys, unauthenticated responses, and other suspicious or unusual activity. Auditor trusted roles should check for continuity of the audit data.

5.5 RECORDS ARCHIVAL

WidePoint NFI SSP or Organization Certificate Authorities and WidePoint NFI SSP or Organization Key Recovery Systems must comply with their respective records retention policies in accordance with whatever laws apply to those entities.

The primary objective of the WidePoint NFI SSP or Organization archive is to prove the validity of any certificate (including those revoked or expired) issued by the WidePoint NFI SSP or Organization in the event of dispute regarding the use of the certificate.

The primary objective of the WidePoint NFI SSP or Organization Key Recovery System archive is reconstruction of key recovery activities, in case of dispute. Examples of disputes may include:

- Validation of key recovery requests.
- Validation of the identity of the recipient of an escrowed key.
- Verification of authorization to obtain the escrowed key copy.
- Verification of transfer of custody of escrowed keys to an authorized Requestor; and
- Establishment of the circumstances under which a copy of the escrowed key was provided.

5.5.1 TYPES OF EVENTS ARCHIVED

The At a minimum, the following data must be recorded for archive as specified for each assurance level:

- WidePoint NFI SSP Certificate Policy
- WidePoint NFI SSP or Organization Certification Practice Statement / WidePoint NFI SSP or Organization Key Recovery Practice Statement
- Contractual obligations
- Other agreements concerning operations of WidePoint NFI SSP or Organization Certificate Authorities and WidePoint NFI SSP or Organization Key Recovery Systems
- System and equipment configuration
- Modifications and updates to system or configuration
- All records related to certificate request authorization, approval and signature, whether generated directly on the WidePoint NFI SSP or Organization Certificate Authority or generated as part of a related external system or process
- All records related to certificate status changes (e.g., revocation, suspension, or restoration) whether generated directly on a WidePoint NFI SSP or Organization Certificate Authority or generated as part of a related external system or process
- All certificates issued and/or published
- Record of re-key
- All records related to certificate status changes (e.g., revocation, suspension, or restoration) whether generated directly on the CA or generated as part of a related external system or process
- WidePoint NFI SSP or Organization Subscriber identity authentication data as per Section 3.2.3 of this WidePoint NFI SSP CP
- Documentation of receipt and acceptance of certificates (if applicable)
- WidePoint NFI SSP or Organization Subscriber agreements
- Documentation of receipt of tokens
- All certificates issued or published
- Record of WidePoint NFI SSP or Organization Certificate Authority Re-key
- Other data or applications to verify archive contents
- Audit summary reports generated by internal reviews and documentation generated during third party audits
- Any changes to the Audit parameters, e.g., audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs
- Whenever WidePoint NFI SSP or Organization Certificate Authorities generate a key (not mandatory for single session or one-time use symmetric keys)

- All access to certificate subject private keys retained for key recovery purposes
- Changes to trusted public keys used or published by WidePoint NFI SSP or Organization Certificate Authorities including certificates used for trust between WidePoint NFI SSP or Organization Certificate Authorities and other components such as WidePoint NFI SSP or Organization Card Management Systems, WidePoint NFI SSP or Organization Registration Authorities, etc.
- The export of private and secret keys (keys used for a single session or message are excluded)
- The approval or rejection of a certificate status change request
- Record of an individual being added or removed from a trusted role, and who added or removed them from the role
- Evidence of qualification for Trusted Agents and the associated validity period(s) for which they are authorized to act as Trusted Agents
- Destruction of cryptographic modules
- All certificate compromise notifications
- Remedial action taken as a result of violations of physical security
- Violations of this WidePoint NFI SSP CP
- Violations of the WidePoint NFI SSP or Organization Certification Practice Statement / WidePoint NFI SSP or Organization Key Recovery Practice Statement

5.5.2 Retention Period for Archive

Archive retention periods begin at the key generation event for any WidePoint NFI SSP or Organization Certificate Authority. For WidePoint NFI SSP or Organization Certificate Authorities that leverage key-rollover procedures a new retention period begins for each subsequent key generation event.

WidePoint NFI SSP or Organization Certificate Authorities will maintain all archived records related to that WidePoint NFI SSP or Organization Certificate Authority, in an accessible fashion, for 3 years after WidePoint NFI SSP or Organization Certificate Authority expiration or WidePoint NFI SSP or Organization Certificate Authority termination.

Individual WidePoint NFI SSP or Organization Registration Authority records associated with certificate request authorization, certificate revocation, subscriber authentication, or subscriber certificate acceptance must be maintained for a minimum of 3 years after the subject certificate expiration date. Issuance of new certificates with extended validity periods (i.e., renewal, rekey or modification) supported by existing subscriber authentication records (i.e., authentication using an existing valid certificate) will result in a new retention period for those initial records, based on the new certificate expiration date.

Practice Note: WidePoint NFI SSP or Organization Registration Authority archive records can be retained for as long as business purposes require; however, this policy does not waive any organizational policies that may require the destruction of such records or otherwise limit their retention periods.

Practice Note: If the archive records are maintained separately from the WidePoint NFI SSP or Organization Certificate Authority, communication processes may be required to determine when archive records are no longer needed based on related public certificates.

WidePoint NFI SSP or Organization Registration Authority system operations audit records, that include any IT resources that facilitate WidePoint NFI SSP or Organization Registration Authority functions, must maintain relevant archives for a minimum of 3 years after WidePoint NFI SSP or Organization Registration Authority system replacement or termination.

5.5.3 Protection of Archive

Only Auditor trusted roles, as described in Section 5.2 of this WidePoint NFI SSP CP, or other personnel specifically authorized by the WidePoint NFI SSP or Organization, are permitted to add or delete records from the archive. Deletion of records identified in Section 5.5.1 of this WidePoint NFI SSP CP before the end of the retention period

is not permitted under any circumstances. The contents of the archive must not be released except in accordance with Sections 9.3 and 9.4 of this WidePoint NFI SSP CP.

Archive media must be stored in a safe, secure storage facility geographically separate from the WidePoint NFI SSP or Organization Certificate Authority in accordance with its records retention policies. The transfer process between the backup environment and archive location must be documented.

In order to ensure that records in the archive may be referenced when required, the WidePoint NFI SSP or Organization Certificate Authority must do one of the following:

- Maintain the hardware or software required to process or read the archive records, or
- Define a process to transfer records to a new format or medium when the old format or medium becomes obsolete and verify the integrity of the records after transfer.

5.5.4 Archive Backup Procedures

If the WidePoint NFI SSP or Organization chooses to back up its archive records, the WidePoint NFI SSP or Organization CPS or a referenced document must describe how the records are backed up and managed.

5.5.5 Requirements for Time-Stamping of Records

WidePoint NFI SSP or Organization Certificate Authority archive records must have accurate timestamps when they are added to the archive.

The time precision must be such that the sequence of events can be determined.

The WidePoint NFI SSP or Organization CPS or WidePoint NFI SSP or Organization KRPS must describe how system clocks used for timestamping are maintained in synchrony with an authoritative time standard

5.5.6 Archive Collection System (Internal vs. External)

Archive data may be collected in any expedient manner but must be documented in the WidePoint NFI SSP or Organization CPS/WidePoint NFI SSP or Organization KRPS.

5.5.7 Procedures to Obtain and Verify Archive Information

Procedures detailing how to create, verify, package, transmit, and store archive information must be included in this WidePoint NFI SSP CP, WidePoint NFI SSP or Organization CPS, or WidePoint NFI SSP or Organization KRPS.

Copies of records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents.

5.6 KEY CHANGEOVER

Each WidePoint NFI SSP or Organization Certificate Authority's signing key must have a validity period as described in Section 6.3.2 of this WidePoint NFI SSP CP. Prior to the end of a WidePoint NFI SSP or Organization Certificate Authority's signing key validity period, a new WidePoint NFI SSP or Organization Certificate Authority must be established or a re-key on the existing WidePoint NFI SSP or Organization Certificate Authority must be performed. This is referred to as key changeover. From that time on, only the new key is used to sign WidePoint NFI SSP or Organization Certificate Authority and WidePoint NFI SSP or Organization Subscriber certificates. The old private key may continue to be used to sign CRLs and OCSP Responder certificates. If the old private key is used to sign OCSP Responder certificates or CRLs that cover certificates signed with that key, the old key must be retained and protected.

After all certificates signed with the old key have expired or been revoked, the WidePoint NFI SSP or Organization Certificate Authority may issue a final long-term CRL using the old key, with a nextUpdate time past the validity period of all issued certificates. This final CRL must be available for all relying parties until the validity period of all issued certificates has passed. Once the last CRL has been issued, the old private signing key of the WidePoint NFI SSP or Organization Certificate Authority may be destroyed.

When a WidePoint NFI SSP or Organization Certificate Authority performs a key changeover and thus generates a new public key, the WidePoint NFI SSP or Organization Certificate Authority must notify all WidePoint NFI SSP or Organization Certificate Authorities, WidePoint NFI SSP or Organization Registration Authorities, and WidePoint NFI SSP or Organization Subscribers that rely on the WidePoint NFI SSP or Organization Certificate Authority's certificate that it has been changed. The WidePoint NFI SSP or Organization Certificate Authority must do one of the following:

- Generate key rollover certificate, where the new public key is signed by the old private key, and vice versa or
- Obtain a new WidePoint NFI SSP or Organization Certificate Authority certificate for the new public key from each issuer of the current WidePoint NFI SSP or Organization Certificate Authority certificate(s).

5.7 COMPROMISE AND DISASTER RECOVERY

The WidePoint NFI SSP or Organization must have an incident handling process, which documents any security incidents. Security incidents may include violation or threat of violation to the system, improper usage, malicious or anomalous activity and violations of the WidePoint NFI SSP or Organization CPS or this WidePoint NFI SSP CP.

5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

WidePoint NFI SSP PMA and the FPKIPA must be notified within 24 hours if a WidePoint NFI SSP or Organization Certificate Authority experiences the following:

- suspected or detected compromise of the WidePoint NFI SSP or Organization systems.
- physical or electronic penetration of WidePoint NFI SSP or Organization systems.
- successful denial of service attacks on WidePoint NFI SSP or Organization components.
- any incident preventing any WidePoint NFI SSP or Organization Certificate Authority from issuing a CRL prior to the nextUpdate time of the previous CRL.
- suspected or detected compromise of a WidePoint NFI SSP or Organization CSS; or
- suspected or detected compromise of a WidePoint NFI SSP or Organization Registration Authority.

The notification must include preliminary remediation analysis.

Once the incident has been resolved, the WidePoint NFI SSP or Organization shall provide notification directly to the FPKIPA which includes detailed measures taken to remediate the incident. The notice must include the following:

1. Which WidePoint NFI SSP or Organization components were affected by the incident.
2. The WidePoint NFI SSP or Organization's interpretation of the incident.
3. Who is impacted by the incident.
4. When the incident was discovered.

5. A complete list of all certificates that may have been issued erroneously or are not compliant with this WidePoint NFI SSP CP/ WidePoint NFI SSP or Organization CPS as a result of the incident.
6. A statement that the incident has been fully remediated.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

When computing resources, software, and/or data are corrupted, the WidePoint NFI SSP or Organization Certificate Authorities must respond as follows:

- Before returning to operation, ensure that the system's integrity has been restored
- If the WidePoint NFI SSP or Organization Certificate Authority signature keys are not destroyed, CA operation must be reestablished, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in Section 4.9.7 of this WidePoint NFI SSP CP.
- If the WidePoint NFI SSP or Organization Certificate Authority signature keys are destroyed, CA operation must be reestablished as quickly as possible, giving priority to the generation of a new WidePoint NFI SSP or Organization Certificate Authority key pair.

In the event of an incident as described above, the WidePoint NFI SSP or Organization must post a notice on its web page identifying the incident and provide notification to the FPKIPA. See Section 5.7.1 of this WidePoint NFI SSP CP for contents of the notice.

5.7.3 Entity Private Key Compromise Procedures

5.7.3.1 WidePoint NFI SSP or Organization Certificate Authority Private Key Compromise Procedures

In the event of a WidePoint NFI SSP or Organization Certificate Authority private key compromise, the following operations must be performed:

- The WidePoint NFI SSP or Organization must immediately inform the FPKIPA and any entities known to be distributing the WidePoint NFI SSP or Organization Certificate Authority certificate (e.g., in a root store).
- The WidePoint NFI SSP or Organization Certificate Authority must request revocation of any certificates issued to the compromised WidePoint NFI SSP or Organization Certificate Authority.
- The WidePoint NFI SSP or Organization Certificate Authority must generate new keys in accordance with Section 6.1.1.1 of this WidePoint NFI SSP CP.

If the WidePoint NFI SSP or Organization Certificate Authority distributed the public key in a Trusted Certificate, the WidePoint NFI SSP or Organization Certificate Authority must perform the following operations:

- Generate a new Trusted Certificate.
- Securely distribute the new Trusted Certificate as specified in Section 6.1.4 of this WidePoint NFI SSP CP.
- Initiate procedures to notify WidePoint NFI SSP or Organization Subscribers of the compromise.

WidePoint NFI SSP or Organization Subscriber certificates issued prior to compromise of the WidePoint NFI SSP or Organization Certificate Authority private key may be renewed automatically by the WidePoint NFI SSP or Organization Certificate Authority under the new key pair (see Section 4.6) or the WidePoint NFI SSP or Organization Certificate Authority may require WidePoint NFI SSP or Organization Subscribers to repeat the initial certificate application process.

The WidePoint NFI SSP PMA shall also investigate and report to the FPKIPA what caused the compromise or loss.

5.7.3.2 WidePoint NFI SSP or Organization KRS Private Key Compromise Procedures

In the event that the WidePoint NFI SSP or Organization Key Encryption Database or WidePoint NFI SSP or Organization Data Decryption Server is compromised or is suspected to be compromised, the following operations must be performed:

- The WidePoint NFI SSP or Organization shall notify the FPKIPA of the compromise
- Provide detail concerning the root cause, operational impact, and initial remediation actions
- Determine the extent of the compromise

- Gain concurrence from the FPKIPA and the WidePoint NFI SSP PMA on planned resolution. This may include revocation of certificates associated with the compromised private keys stored in the WidePoint NFI SSP or Organization Key Encryption Database or WidePoint NFI SSP or Organization Data Decryption Server.

If a WidePoint NFI SSP or Organization Key Recovery Agent or WidePoint NFI SSP or Organization Key Recovery Officer certificate is revoked due to compromise, the potential exists for some WidePoint NFI SSP or Organization or Organization Subscribers' escrowed keys to have been exposed during a recovery process, the following operations must be performed:

- Audit record review by the audit administrator to identify all potentially exposed escrowed keys.
- Revocation of each of the potentially exposed escrowed keys, according to procedures specified in Section 4.9.3 of this WidePoint NFI SSP CP, to include Subscriber notification of the revocation
- Reissuance of the WidePoint NFI SSP or Organization Key Recovery Agent or WidePoint NFI SSP or Organization Key Recovery Officer authentication certificate

5.7.4 Business Continuity Capabilities After a Disaster

The WidePoint NFI SSP or Organization repository system must be deployed to provide 24-hour, 365 day per year availability with high levels of repository reliability.

WidePoint NFI SSP or Organization Certificate Authorities must have recovery procedures in place to reconstitute the WidePoint NFI SSP or Organization Certificate Authority after failure.

In the case of a disaster whereby the WidePoint NFI SSP or Organization Certificate Authority installation is physically damaged and all copies of the WidePoint NFI SSP or Organization Certificate Authority signature key are destroyed as a result, the WidePoint NFI SSP PMA and the FPKIPA must be notified at the earliest feasible time, and the WidePoint NFI SSP PMA must take whatever action it deems appropriate.

5.8 CA or RA Termination

In the event the decision is made to terminate WidePoint NFI SSP operations, the following must be accomplished prior to termination:

- Notify all Organizations operating under this WidePoint NFI SSP CP.
- Revoke any issued certificates that have not expired
- Generate and publish a final long term CRL with a nextUpdate time past the validity period of all issued certificates. This final CRL must be available for all relying parties until the validity period of all issued certificates has passed.
- Once the last CRL has been issued, destroy the private signing key(s) of the WidePoint NFI SSP Certificate Authorities.
- Transfer all archive data to an archival facility.

Organizations operating under this WidePoint NFI SSP CP will be given as much advance notice as circumstances permit and attempts to provide alternative sources of interoperation will be sought.

Whenever possible, the WidePoint NFI SSP PMA must be notified at least two weeks prior to the termination of any WidePoint NFI SSP or Organization Certificate Authority. For emergency termination, WidePoint NFI SSP or Organization Certificate Authorities must follow the notification procedures in Section 5.7 of this WidePoint NFI SSP CP. Whenever possible, the WidePoint NFI SSP PMA will notify the FPKIPA at least two weeks prior to the termination of any WidePoint NFI SSP or Organization Certificate Authority operating under this WidePoint NFI SSP Certificate Policy.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

Key generation for keys generated under this WidePoint NFI SSP CP must be performed using a FIPS approved method or equivalent international standard. Key generation events should 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 or Organization.

6.1.1.1 WidePoint NFI SSP or Organization Certificate Authority Key Pair Generation

Cryptographic keying material used to sign certificates, CRLs or status information by WidePoint NFI SSP or Organization Certificate Authorities shall be generated in FIPS 140-3 Security Level 3 Hardware validated cryptographic modules or modules validated under equivalent international standards.

WidePoint NFI SSP or Organization Certificate Authority key pair generation must create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure must be detailed enough to show that appropriate role separation was used. Multiparty control is required for WidePoint NFI SSP or Organization Certificate Authority key pair generation for WidePoint NFI SSP or Organization Certificate Authority operating at the Medium or Medium Hardware levels of assurance, as specified in Section 5.2.2 of this WidePoint NFI SSP CP. An independent third party shall validate the execution of the key generation procedures, either by witnessing the key generation or by examining the signed and documented record of the key generation.

Practice Note: If the audit trail identifies and documents any failures or anomalies in the key generation process, along with the corrective action taken, the key generation process need not be restarted but may continue.

6.1.1.2 WidePoint NFI SSP or Organization Subscriber Key Pair Generation

WidePoint NFI SSP or Organization Subscriber key pair generation may be performed by the WidePoint NFI SSP or Organization Subscriber, WidePoint NFI SSP or Organization Certificate Authority, or WidePoint NFI SSP or Organization Registration Authority. If the WidePoint NFI SSP or Organization Certificate Authority or WidePoint NFI SSP or Organization Registration Authority generates subscriber key pairs, the requirements for key pair delivery specified in Section 6.1.2 of this WidePoint NFI SSP CP, Private Key Delivery to Subscriber, must also be met. Key generation shall be performed using a FIPS-approved method or equivalent international standard.

For WidePoint NFI SSP or Organization PIV-I, all keys, except for key management, must be generated on the card. (See Appendix A.)

For Medium Hardware and Medium Assurance, an independent third party must validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation.

For all other certificates at the Medium Hardware assurance level, WidePoint NFI SSP or Organization Subscriber key generation must be performed using a validated hardware cryptographic module as specified in Section 6.2.1. For Medium assurance, either validated software or validated hardware cryptographic modules must be used for key generation as specified in Section 6.2.1 of this WidePoint NFI SSP CP.

6.1.1.3 WidePoint NFI SSP or Organization Certificate Status Services Key Pair Generation

Cryptographic keying material used by WidePoint NFI SSP or Organization Certificate Status Services to sign status information must be generated in FIPS 140-3 Security Level 2 validated cryptographic modules as specified in Section 6.2.1 of this WidePoint NFI SSP CP.

6.1.1.4 WidePoint NFI SSP or Organization PIV-I Content Signing Key Pair Generation

Cryptographic keying material used by WidePoint NFI SSP or Organization Card Management Systems or devices for PIV-I Content Signing must be generated in FIPS 140-3 Security Level 2 validated cryptographic modules as specified in Section 6.2.1 of this WidePoint NFI SSP CP.

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER

If WidePoint NFI SSP or Organization Subscribers generate their own key pairs, then there is no need to deliver private keys, and this section does not apply.

When WidePoint NFI SSP or Organization Certificate Authorities or WidePoint NFI SSP or Organization Registration Authorities generate keys on behalf of the Subscriber, then the private key must be delivered securely to the WidePoint NFI SSP or Organization Subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases, the following requirements must be met:

- Anyone who generates a private signing key for a WidePoint NFI SSP or Organization Subscriber must not retain any copy of the key after delivery of the private key to the Subscriber.
- The private key must be protected from activation, compromise, or modification during the delivery process.
- The WidePoint NFI SSP or Organization Subscriber must acknowledge receipt of the private key(s).
- Delivery must be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct WidePoint NFI SSP or Organization Subscribers.
    - For hardware modules, accountability for the location and state of the module must be maintained until the WidePoint NFI SSP or Organization Subscriber accepts possession of it.
    - For electronic delivery of private keys, the key material must be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data must be delivered using a separate secure channel.
    - For shared key applications, organizational identities, and network devices, see also Section 3.2 of this WidePoint NFI SSP CP.

The WidePoint NFI SSP or Organization Certificate Authority must maintain a record of the WidePoint NFI SSP or Organization Subscriber acknowledgement of receipt of the token.

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

For WidePoint NFI SSP or Organization Certificate Authorities issuing certificates that assert policies in this WidePoint NFI SSP CP, the following requirements apply:

- Where key pairs are generated by the WidePoint NFI SSP or Organization Subscriber or WidePoint NFI SSP or Organization Registration Authority, the public key and the WidePoint NFI SSP or Organization Subscriber's identity must be delivered securely to the WidePoint NFI SSP or Organization Certificate Authority for certificate issuance.
- The delivery mechanism must bind the WidePoint NFI SSP or Organization Subscriber's verified identity to the public key. If cryptography is used to achieve this binding, it must be at least as strong as the WidePoint NFI SSP or Organization Subscriber key pair.

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

Self-signed root WidePoint NFI SSP Root Certificate Authority certificates must be conveyed to relying parties in a secure fashion to preclude substitution attacks. Acceptable methods include:

Secure distribution of the certificate through secure out-of-band mechanisms;

Download the certificate from a WidePoint NFI SSP operated web site secured with a currently valid certificate and subsequent comparison of the hash of the certificate against a hash value made available via authenticated out-of-band sources (note that hashes posted in-band along with the certificate are not acceptable as an authentication mechanism)

Practice Note: Other methods that preclude substitution attacks may be considered acceptable.

6.1.5 KEY SIZES

This WidePoint NFI SSP CP 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 or Organization Certificate Authority certificates that expire on or before December 31, 2030	WidePoint NFI SSP or Organization 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 or Organization Subscriber certificates that expire on or before December 31, 2030	WidePoint NFI SSP or Organization 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 or Organization Subscriber certificates associated with WidePoint NFI SSP or Organization PIV-I Subscriber must contain public keys and algorithms that conform to [NIST SP 800-78].

Use of Transport Layer Security (TLS) or another protocol providing similar security to accomplish any of the requirements of this WidePoint NFI SSP CP must require at a minimum AES (128 bits) or equivalent for the symmetric key, and at least 2048-bit RSA or equivalent for the asymmetric keys. After December 31, 2030, use of TLS or another protocol providing similar security to accomplish any of the requirements of this WidePoint NFI SSP CP must require at a minimum AES (128 bits) or equivalent for the symmetric key, and at least 3072-bit RSA or equivalent for the asymmetric keys.

WidePoint NFI SSP or Organization Key Encryption Database and WidePoint NFI SSP or Organization Data Decryption Service keys must be at equal to or stronger than the keys being escrowed.

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

For RSA, the WidePoint NFI SSP or Organization Certificate Authority shall perform partial public key validation as specified in NIST SP 800-89 (section 5.3.3).

For ECC, public keys must fall within curves defined in Section 7.1.3. Additionally, the WidePoint NFI SSP or Organization Certificate Authority should 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)

Public keys that are bound into certificates must be certified for use in signing or encrypting, but not both, except as specified below. The use of a specific key is determined by the key usage extension in the X.509 certificate.

All certificates must include a critical Key Usage extension.

- Certificates to be used only for authentication must set only the digitalSignature bit.
- Certificates to be used by Human Subscribers for digital signatures must set the digitalSignature and nonRepudiation bits.
- Certificates that have the nonRepudiation bit set, must not have keyEncipherment bit or keyAgreement bit set.

- Certificates to be used for encryption (RSA) must set the keyEncipherment bit.
- Certificates to be used for key agreement (ECC) must set the keyAgreement bit.
- WidePoint NFI SSP or Organization Certificate Authority certificates must set only cRLSign and keyCertSign bits.

Keys associated with WidePoint NFI SSP or Organization Certificate Authority certificates must be used only for signing certificates and CRLs.

Keys associated with Device WidePoint NFI SSP or Organization Subscriber certificates may be used for digital signature (including authentication), encryption, or both. Except for OCSP Responder certificates, device certificates must not assert the nonRepudiation bit.

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 or Organization Subscribers two key pairs, one for key management and one for digital signature and authentication.

For all WidePoint NFI SSP or Organization Subscriber certificates issued after June 30, 2019, the Extended Key Usage extension must always be present. Extended Key Usage OIDs must be consistent with key usage bits asserted. The Extended Key Usage extension must not contain anyExtendedKeyUsage {2.5.29.37.0}.

WidePoint NFI SSP or Organization PIV-I Content Signing certificates 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 [PIV-I Profile]).

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 cryptographic modules is [FIPS 140], Security Requirements for Cryptographic Modules. A FIPS 140 Level 1 or higher validated cryptographic module must be used for all cryptographic operations.

Cryptographic modules must be minimally validated to the FIPS 140 level identified in this section , with the exception of Hardware Subscriber Key Management Key(s) only for key recovery and when dictated by extenuating circumstances put for by a Third-Party Requestor in alignment with legal or technical requirements. Additionally, the WidePoint NFI SSP or Organization reserves the right to review technical documentation associated with any cryptographic modules under consideration for use by the WidePoint NFI SSP or Organization.

The table below summarizes the minimum FIPS 140 requirements for cryptographic modules; higher levels may be used.

Assurance Level	WidePoint NFI SSP or Organization Certificate Authority	WidePoint NFI SSP or Organization Card Management System and Certificate Status Service	WidePoint NFI SSP or Organization Subscriber	WidePoint NFI SSP or Organization Registration Authority
Medium	Level 3 (Hardware)	Level 2 (Hardware)	Level 1	Level 2 (Hardware)
PIV-I Card Authentication	Level 3 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)
Medium Hardware	Level 3 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware) Level 1*	Level 2 (Hardware)

			(Key Recovery)	
Practice Note – All instances of recovered keys should be destroyed as early as practicable in consultation with the Third-Party Recovery Requestor (e.g., after required data has been decrypted). See Sections 4.12 and 6.2.6 for additional key recovery requirements to include secure transport.				

*When necessary for completing an authenticated and authorized Third-Party key recovery request (e.g., in support of an investigation) Hardware Subscriber key management keys can only be recovered into a Level 1 module or an encrypted file (.p12 or .pfx) provided there is organizational approval based on the acceptance of risk to data encrypted with the associated public keys.

WidePoint NFI SSP or Organization Subscriber PIV-I Cards must be issued using card stock that has been tested and approved by the FIPS 201 Evaluation Program and listed on the GSA Approved Products List (APL). Card stock that has been removed from the APL may continue to be issued for no more than one year after GSA approved replacement card stock is available. WidePoint NFI SSP or Organization Subscriber PIV-I cards issued using the deprecated card stock may continue to be used until the current subscriber certificates expire, unless otherwise notified by the WidePoint NFI SSP PMA.

For hardware tokens associated with WidePoint NFI SSP or Organization Subscriber PIV-I, see Appendix A for additional requirements.

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

6.2.1.1 Custodial Subscriber Key Stores

Custodial Subscriber Key Stores hold keys for a number of WidePoint NFI SSP or Organization Subscriber certificates in one location. When a collection of private keys for WidePoint NFI SSP or Organization Subscriber certificates are held in a single location, there is a higher risk associated with compromise of that cryptographic module than that of a single Subscriber.

Cryptographic modules for Custodial Subscriber Key Stores must be no less than FIPS 140 Level 2 Hardware.

In addition, authentication to the Cryptographic Device in order to activate the private key associated with a given certificate requires authentication commensurate with the assurance level of the certificate.

6.2.2 Private Key Multi-person Control

Use of a WidePoint NFI SSP or Organization Certificate Authority private signing key and WidePoint NFI SSP or Organization Certificate Status Service private signing key must require action by multiple persons at Medium and Medium Hardware Assurance as set forth in Section 5.2.2 of this WidePoint NFI SSP CP.

WidePoint NFI SSP or Organization PIV-I Content Signing key activation must require the same multiparty control established for the WidePoint NFI SSP or Organization Certificate Authority (see Section 5.2.2 of this WidePoint NFI SSP CP).

6.2.3 Private Key Escrow

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

Human Subscriber key management keys may be escrowed to provide key recovery as described in Section 4.12.1 of this WidePoint NFI SSP CP.

WidePoint NFI SSP or Organization Subscriber private signature keys must not be escrowed.

WidePoint NFI SSP or Organization Subscriber private dual use keys must not be escrowed. If a device has a separate key management key certificate, the key management private key may be escrowed.

6.2.4 Private Key Backup

All backups of WidePoint NFI SSP or Organization Certificate Authority, WidePoint NFI SSP or Organization Certificate Status Services, and WidePoint NFI SSP or Organization PIV-I Content Signing private signature keys

must be accounted for and protected under the same multi-person control as the original signature key. At least one copy of the WidePoint NFI SSP or Organization Certificate Authority private signature key must be stored off site.

For all other keys, backup, when permitted, must provide security controls consistent with the protection provided by the original cryptographic module. Backed up private signature key(s) must not be exported or stored in plaintext form outside the cryptographic module.

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

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

* WidePoint NFI SSP or Organization 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 or Organization Subscriber's control.

6.2.5 PRIVATE KEY ARCHIVAL

WidePoint NFI SSP or Organization Certificate Authority private signature keys and WidePoint NFI SSP or Organization Subscriber private signature keys must not be archived.

WidePoint NFI SSP or Organization Certificate Authorities may maintain an archive of escrowed WidePoint NFI SSP or Organization Subscriber private key management keys. Such archives must be protected in accordance with Sections 4.12, 5.1, 5.2, and 6.2.1 of this WidePoint NFI SSP CP.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

A WidePoint NFI SSP or Organization Certificate Authority private key must not exist in plain text outside the cryptographic module. WidePoint NFI SSP or Organization Certificate Authority, WidePoint NFI SSP or Organization Certificate Status Service and WidePoint NFI SSP or Organization PIV-I Content Signing private signature keys may be exported from the cryptographic module only to perform WidePoint NFI SSP or Organization Certificate Authority key backup procedures as described in Section 6.2.4 of this WidePoint NFI SSP CP.

If any private key is transported from one cryptographic module to another, to include key recovery operations, the private key must be protected using a FIPS approved algorithm and at a bit strength commensurate with the key being transported. Private keys must never exist in plaintext form outside the cryptographic module boundary.

Private or symmetric keys used to encrypt other private keys for transport must be protected from disclosure.

6.2.7 Private Key Storage on Cryptographic Module

No stipulation beyond that specified in [FIPS-140].

6.2.8 Method of Activating Private Key

Cryptographic modules must be protected from unauthorized access. WidePoint NFI SSP or Organization Subscriber private key activation requirements are detailed in the following table:

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

After use, the cryptographic module must be deactivated via a manual logout procedure, or automatically after a period of inactivity as defined in the WidePoint NFI SSP or Organization CPS. WidePoint NFI SSP or Organization Certificate Authority Hardware cryptographic modules must be physically secured per requirements in Section 5.1 of this WidePoint NFI SSP CP when not in use.

6.2.10 Method of Destroying Private Key

Individuals in trusted roles must destroy all copies of WidePoint NFI SSP or Organization Certificate Authority, WidePoint NFI SSP or Organization Registration Authority and WidePoint NFI SSP or Organization Certificate Status Service private signature keys and activation data (e.g., operator card set or tokens) when they are no longer needed. WidePoint NFI SSP or Organization Subscribers either must surrender their cryptographic modules to WidePoint NFI SSP or Organization Certificate Authority / WidePoint NFI SSP or Organization Registration Authority personnel for destruction or destroy their private signature keys when they are no longer needed, or when the certificates to which they correspond expire or are revoked.

6.2.11 Cryptographic Module Rating

See Section 6.2.1 of this WidePoint NFI SSP CP.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Public key archival must be in accordance with Section 5.5 of this WidePoint NFI SSP CP.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

A WidePoint NFI SSP or Organization Certificate Authority private key may be used to sign CRLs and OCSP responder certificates for the entire usage period. All certificates signed by a specific WidePoint NFI SSP or Organization Certificate Authority key pair must expire before the end of that key pair's usage period.

Key	Private Key	Certificate
WidePoint NFI SSP Root Certificate Authority certificate	30 years	30 years
WidePoint NFI SSP or Organization Certificate Authority certificate	10 years	10 years
WidePoint NFI SSP or Organization Subscriber Authentication	3 years	3 years
WidePoint NFI SSP or Organization Subscriber Signature	3 years	3 years
WidePoint NFI SSP or Organization Subscriber Encryption	Unrestricted	3 years
WidePoint NFI SSP or Organization Subscriber PIV-I Card Authentication	3 years	3 years
WidePoint NFI SSP or Organization PIV-I Content Signer	3 years	9 years*
WidePoint NFI SSP or Organization Code Signing	3 years	8 years
WidePoint NFI SSP or Organization OCSP Responder	3 years	120 days
WidePoint NFI SSP or Organization Device	3 years	3 years

* Expiration of the WidePoint NFI SSP or Organization Content Signing certificate must be later than the expiration of the WidePoint NFI SSP or Organization Subscriber certificates on the same PIV-I credential.

WidePoint NFI SSP or Organization Subscriber certificates on a PIV-I card must expire no later than the expiration date of the PIV-I hardware token on which they reside.

The validity period of the WidePoint NFI SSP or Organization Subscriber certificate must not exceed the routine re-key Identity Requirements as specified in Section 3.3.1 of this WidePoint NFI SSP CP.

Practice Note: WidePoint NFI SSP or Organization Certificate Authority signing key usage is determined in the context of the length of the validity periods of the certificates issued to and by the WidePoint NFI SSP or Organization Certificate Authority.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data used to unlock WidePoint NFI SSP or Organization Certificate Authority or WidePoint NFI SSP or Organization Subscriber private keys, in conjunction with any other access control, must have an appropriate level of strength for the keys or data to be protected. Where the WidePoint NFI SSP or Organization Certificate Authority uses passwords as activation data for the **CA** signing key, at a minimum the activation data must be changed upon WidePoint NFI SSP or Organization Certificate Authority re-key.

For Medium Assurance and above, WidePoint NFI SSP or Organization Registration Authority and WidePoint NFI SSP or Organization Subscriber activation data may be user-selected. The strength of the activation data must meet or exceed the requirements for authentication mechanisms stipulated for Level 2 in [FIPS 140].

For WidePoint NFI SSP or Organization Subscriber PIV-I, in the event activation data can be reset by an issuer after a card is locked, authentication of the subscriber is required. This authentication must be conducted in accordance with FIPS 201, Section 2.9.3.

6.4.2 Activation Data Protection

Data used to unlock private keys must be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data must be:

- memorized
- biometric in nature,
- contained within an organizationally approved device or software tool (e.g., password manager) that leverages encryption commensurate with the bit-strength of the key it activates, or
- physically recorded and secured at the level of assurance associated with the activation of the cryptographic module and must not be stored with the cryptographic module.

Practice Note: For [FIPS 140] level 2 and higher modules, the protection mechanism should include an ability to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts to protect against repeated guessing attacks, as set forth in this WidePoint NFI SSP Certificate Policy.

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

6.4.3 Other Aspects of Activation Data

WidePoint NFI SSP or Organization Certificate Authorities must define any other aspects of Activation Data in the WidePoint NFI SSP or Organization CPS under this WidePoint NFI SSP CP.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

For WidePoint NFI SSP or Organization Certificate Authorities, WidePoint NFI SSP or Organization Key Encryption Databases, and WidePoint NFI SSP or Organization Data Decryption Services the computer security functions listed below are required. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The WidePoint NFI SSP or Organization Certificate Authority and its ancillary parts must include the following functionality (these functions pertain to all system software layers, where applicable):

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- generate and archive audit records for all transactions; (see Section 5.4 of this WidePoint NFI SSP CP)
- enforce domain integrity boundaries for security critical processes;
- require use of cryptography for session communication and database security;
- require self-test security-related certificate authority services;
- require a trusted path for identification of all users;
- provide residual information protection; and
- require recovery from key or system failure.

For WidePoint NFI SSP or Organization Certificate Status Services, the computer security functions listed below are required (these functions pertain to all system software layers, where applicable):

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- enforce domain integrity boundaries for security critical processes;
- provide residual information protection; and
- require recovery from key or system failure.

For remote workstations used to administer the WidePoint NFI SSP or Organization Certificate Authorities, WidePoint NFI SSP or Organization Key Encryption Databases, and WidePoint NFI SSP or Organization Data Decryption Services, the computer security functions listed below are required:

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- generate and archive audit records for all transactions; (see Section 5.4 of this WidePoint NFI SSP CP)
- enforce domain integrity boundaries for security critical processes;
- provide residual information protection; and
- require recovery from system failure.

All communications between any PKI trusted role and the WidePoint NFI SSP or Organization Certificate Authority must be authenticated and protected from modification.

6.5.2 COMPUTER SECURITY RATING

WidePoint NFI SSP or Organization Certificate Authorities must identify any Computer Security Rating requirements in the WidePoint NFI SSP or Organization CPS.

6.6 LIFE-CYCLE TECHNICAL CONTROLS

6.6.1 SYSTEM DEVELOPMENT CONTROLS

The System Development Controls for WidePoint NFI SSP or Organization Certificate Authorities (including any remote workstations used to administer the WidePoint NFI SSP or Organization Certificate Authority) and WidePoint NFI SSP or Organization Registration Authorities are as follows:

- Where open source software has been utilized, the applicant must demonstrate that security requirements were achieved through software verification and validation and structured development/life-cycle management.
- Hardware and software used to administer or operate the WidePoint NFI SSP or Organization Certificate Authority must be procured and shipped in a fashion to reduce the likelihood that any component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).
- Custom hardware and software must be developed in a controlled environment, and the development process must be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.
- The WidePoint NFI SSP or Organization Certificate Authority hardware and software, including all system software layers, must be dedicated to operating and supporting the WidePoint NFI SSP or Organization Certificate Authority (i.e., the systems and services dedicated to the issuance and management of certificates). There must be no other applications, hardware devices, network connections, or component software installed which are not part of the WidePoint NFI SSP or Organization Certificate Authority operation, administration, monitoring and security compliance of the system. WidePoint NFI SSP or Organization Certificate Authority hardware and system software layers may support multiple WidePoint NFI SSP or Organization Certificate Authorities and their supporting systems, provided all systems have comparable security controls and are dedicated to the support of the WidePoint NFI SSP or Organization Certificate Authority in compliance of this WidePoint NFI SSP CP and the WidePoint NFI SSP or Organization CPS.
- Proper care must be taken to prevent malicious software from being loaded onto the WidePoint NFI SSP or Organization Certificate Authority equipment. All applications required to perform the operation of the WidePoint NFI SSP or Organization Certificate Authority must be obtained from documented sources. Except for Offline WidePoint NFI SSP or Organization Certificate Authorities, WidePoint NFI SSP or Organization Certificate Authority and WidePoint NFI SSP or Organization Registration Authorities hardware and software must be scanned for malicious code on first use and periodically thereafter.
- Hardware and software updates must be purchased or developed in the same manner as original equipment and be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of the WidePoint NFI SSP or Organization Certificate Authority system as well as any modifications and upgrades must be documented and controlled. There must be a mechanism for detecting unauthorized modification to WidePoint NFI SSP or Organization Certificate Authority software or configuration. The WidePoint NFI SSP or Organization Certificate Authority software, when first loaded, must be verified as being that supplied from the vendor, with no modifications, and be the version intended for use. The WidePoint NFI SSP or Organization Certificate Authority must periodically verify the integrity of the software.

6.6.3 Life-Cycle Security Controls

WidePoint NFI SSP or Organization Certificate Authorities operating under this WidePoint NFI SSP CP must identify any Life Cycle Security Control requirements in the WidePoint NFI SSP or Organization CPS.

6.7 Network Security Controls

This section does not apply to offline WidePoint NFI SSP or Organization Certificate Authorities.

A network guard, firewall, or filtering router must protect network access to WidePoint NFI SSP or Organization Certificate Authority and WidePoint NFI SSP or Organization Key Recovery System equipment. The network guard, firewall, or filtering router must limit services allowed to and from the WidePoint NFI SSP or Organization Certificate Authority and WidePoint NFI SSP or Organization Key Recovery System equipment to those required to perform WidePoint NFI SSP or Organization Certificate Authority and WidePoint NFI SSP or Organization Key Recovery System functions.

Protection of WidePoint NFI SSP or Organization Certificate Authority and WidePoint NFI SSP or Organization Key Recovery System equipment must be provided against known network attacks. All unused network ports and services must be turned off. Any network software present on the WidePoint NFI SSP or Organization Certificate

Authority and WidePoint NFI SSP or Organization Key Recovery System equipment must be necessary to the functioning of the WidePoint NFI SSP or Organization Certificate Authority application.

Any boundary control devices used to protect the local area network on which PKI equipment is hosted must deny all but the necessary services to the PKI equipment.

WidePoint NFI SSP or Organization Registration Authorities, WidePoint NFI SSP or Organization Card Management Systems, repositories, WidePoint NFI SSP or Organization Certificate Status Services, and remote workstations used to administer the WidePoint NFI SSP or Organization Certificate Authorities must employ appropriate network security controls. Networking equipment must turn off unused network ports and services. Any network software present must be necessary to the function of the equipment.

Any remote workstation used to administer the WidePoint NFI SSP or Organization Certificate Authority must be configured for mutual authentication. The remote workstation to WidePoint NFI SSP or Organization Certificate Authority communications, to include WidePoint NFI SSP or Organization Certificate Authority boundary control devices, must incorporate data integrity and confidentiality services. The remote workstation to WidePoint NFI SSP or Organization Certificate Authority network communications must be encrypted and must not be vulnerable to replay or machine-in-the-middle attacks. If mutual authentication is shared secret based, the shared secret must be changed at least annually, must be randomly generated, and must have entropy commensurate with the cryptographic strength of certificates issued by the PKI being administered.

Once the connection is established between the remote workstation and the WidePoint NFI SSP or Organization Certificate Authority or boundary control devices, the WidePoint NFI SSP or Organization Certificate Authority must permit remote administration only after successful multi-factor authentication of the Trusted Role at a level of assurance commensurate with that of the WidePoint NFI SSP or Organization Certificate Authority.

6.8 TIME-STAMPING

Asserted times must be accurate to within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events, see Section 5.4.1 of this WidePoint NFI SSP CP.

7 CERTIFICATE, CRL, AND OCSP PROFILES

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

7.1 CERTIFICATE PROFILE

PIV-I authentication, card authentication and content signing certificates must conform to the relevant profile worksheets in the [FBCA-PROF].

All other certificates must be compatible with X.509 Certificate and CRL Extensions Profile [FBCA-PROF].

7.1.1 VERSION NUMBERS(S)

Certificates must be of type X.509 v3 (populate version field with integer "2").

7.1.2 CERTIFICATE EXTENSIONS

For all WidePoint NFI SSP or Organization Certificate Authorities, use of standard certificate extensions must comply with [RFC 5280].

WidePoint NFI SSP or Organization Certificate Authorities that issue PIV-I Certificates must comply with relevant worksheets from [FBCAPROF].

Practice Note: For WidePoint NFI SSP or Organization Certificate Authorities that issue PIV-I certificates, the associated CSS certificates must also comply with [FBCA-PROF].

WidePoint NFI SSP or Organization Certificate Authorities certificates must not include critical private extensions.

When used in WidePoint NFI SSP or Organization Subscriber certificates, critical private extensions must be interoperable in their intended community of use.

WidePoint NFI SSP or Organization Certificate Authorities and WidePoint NFI SSP or Organization Subscriber certificates may include any extensions as specified by [RFC 5280] in a certificate, but must include those extensions required by this WidePoint NFI SSP CP. Any optional or additional extensions must not conflict with the applicable certificate and CRL profiles identified in Section 7.1 of this WidePoint NFI SSP CP.

7.1.3 ALGORITHM OBJECT IDENTIFIERS

Certificates issued by the WidePoint NFI SSP or Organization must identify the signature algorithm using one of the following OIDs:

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]). The following are the approved hash algorithms:

id-sha256	{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)
id-sha384	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 2 } (2.16.840.1.101.3.4.2.2)
id-sha512	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3 } (2.16.840.1.101.3.4.2.3)

Certificates must use the following OIDs to identify the algorithm associated with the subject key:

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}

Where non-CA certificates issued on behalf of federal agencies contain an elliptic curve public key, the parameters must be specified as one of the following named 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 or Organization shall certify only public keys associated with the crypto-algorithms identified above and shall only use the signature crypto-algorithms described above to sign certificates, certificate revocation lists and WidePoint NFI SSP or Organization Certificate Status Services OCSP responses.

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

7.1.4 NAME FORMS

Where required as set forth in Section 3.1.1 of this WidePoint NFI SSP CP, the subject and issuer fields of the base certificate must be populated with an X.500 Distinguished Name. Distinguished names must be composed of standard attribute types, such as those identified in [RFC 5280].

7.1.5 NAME CONSTRAINTS

Name constraints may be asserted in WidePoint NFI SSP or Organization Certificate Authority certificates.

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER

All certificates issued by the WidePoint NFI SSP or Organization must include a certificate policies extension asserting one or more of the certificate policy OID(s) appropriate to the level of assurance with which it was issued. See Section 1.2 of this WidePoint NFI SSP CP for specific OIDs.

WidePoint NFI SSP or Organization shall not assert the FBCA CP OIDs in any certificates the WidePoint NFI SSP or Organization issues, except in the subject Domain field of the policyMappings extension of the certificates issued to FBCA establishing an equivalency between an FBCA OID and an OID in this WidePoint NFI SSP CP.

WidePoint NFI SSP or Organization certificates shall assert at least one certificate policy OID as specified in Section 1.2 of this WidePoint NFI SSP CP in the certificate policies extension.

Certificates issued for PIV-I card authentication or PIV-I content signing must not express any other policy OIDs.

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

7.1.7 USAGE OF POLICY CONSTRAINTS EXTENSION

WidePoint NFI SSP or Organization Certificate Authorities may assert policy constraints in WidePoint NFI SSP or Organization Certificate Authority certificates. When this extension appears, at least one of requireExplicitPolicy or inhibitPolicyMapping must be present. When present, this extension may be marked critical.

For WidePoint NFI SSP or Organization Subordinate Certificate Authority certificates inhibitPolicyMapping, skip certs must be set to 0. For cross-certificates inhibitPolicyMapping, skip certs must be set appropriately. When requireExplicitPolicy is included, skip certs must be set to 0.

Practice Note: inhibitPolicyMapping, skip certs is usually set to 1 in a cross-certificate issued to a Bridge so it can do another cross-certificate mapping to its CA members. A skip certs value of 2 may be required to allow transitive trust if that Bridge issues a cross-certificate to a CA that also allows mapping, e.g., the Federal Common Policy CA also issues cross-certificates with policy mapping. If transitive trust is not the desired behavior other constraints such as name constraints may be required to control appropriate results.

7.1.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS

Certificates issued by the WidePoint NFI SSP or Organization may contain policy qualifiers identified in [RFC 5280].

7.1.9 PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES EXTENSION

Certificates must contain a non-critical certificate policies extension.

7.1.10 INHIBIT ANY POLICY EXTENSION

The WidePoint NFI SSP or Organization Certificate Authorities may assert InhibitAnyPolicy in WidePoint NFI SSP or Organization Certificate Authority certificates. When present, this extension may be marked critical. Skip certs must be set to 0.

7.2 CRL PROFILE

7.2.1 VERSION NUMBER(S)

WidePoint NFI SSP or Organization Certificate Authorities must issue X.509 version two (2) CRLs.

7.2.2 CRL AND CRL ENTRY EXTENSIONS

Detailed CRL profiles addressing the use of each extension are specified in [FBCA-PROF].

7.3 OCSP PROFILE

All WidePoint NFI SSP or Organization Certificate Status Services must accept and return SHA-1 hashes in the CertID and responderID fields. WidePoint NFI SSP or Organization Certificate Status Services may accept and return additional hash algorithms within the CertID fields. CSSs must not return any response containing a hash algorithm in the CertID that differs from the CertID in the request.

7.3.1 VERSION NUMBER(S)

CSSs must use OCSP version 1.

7.3.2 OCSP EXTENSIONS

Critical OCSP extensions must not be used.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The WidePoint NFI SSP operating under this WidePoint NFI SSP CP 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. The WidePoint NFI SSP and Organizations are subject to annual review by the WidePoint NFI SSP PMA to ensure their policies and operations remain compliant with this WidePoint NFI SSP CP and the WidePoint NFI SSP or Organization CPS.

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 PMA 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 Organizations must 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 or Organization shall perform compliance audits on an annual basis of all WidePoint NFI SSP or Organization systems that constitute their PKI. This audit shall examine operations to validate WidePoint NFI SSP or Organization systems that constitute their PKI are operating in accordance with the security practices and procedures described in this WidePoint NFI SSP CP and the WidePoint NFI SSP or Organization CPS. The WidePoint NFI SSP or Organization 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 or Organization acknowledges the FPKIPA's right to require periodic and aperiodic inspections and compliance audits of the WidePoint NFI SSP or Organization facility to validate that the WidePoint NFI SSP or Organization systems are operating in accordance with the security practices and procedures set forth in this WidePoint NFI SSP CP and the WidePoint NFI SSP or Organization CPS. The WidePoint NFI SSP and FPKIPA will state the reason(s) for any aperiodic compliance audit.

On an annual basis, for each PIV Card Issuer (PCI) configuration used (as defined by the FIPS 201 Evaluation Program), one populated, representative WidePoint NFI SSP or Organization PIV-I card must be submitted to the FIPS 201 Evaluation Program for testing.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The external independent auditor must demonstrate competence in the field of compliance audits. At the time of the audit, the WidePoint NFI SSP or Organization external independent auditor must be thoroughly familiar with the requirements which this WidePoint NFI SSP CP imposes on the issuance and management of their certificates. The external independent auditor must perform such compliance audits as a regular ongoing business activity.

For the WidePoint NFI SSP or Organization, in addition to the previous requirements, the external independent auditor must be a Certified Information System Auditor (CISA), IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The external independent auditor either must be a private firm that is independent from the entity being audited, or it must be sufficiently organizationally separated from that entity to provide an unbiased, independent evaluation. To ensure independence and objectivity, the external independent auditor may not have served the entity in developing or maintaining the WidePoint NFI SSP or Organization Facility or the WidePoint NFI SSP or Organization CPS.

The FPKIPA and the WidePoint NFI SSP may determine whether an external independent auditor meets this requirement.

8.4 TOPICS COVERED BY ASSESSMENT

The purpose of an external independent audit of the WidePoint NFI SSP or Organization must be to verify that it is operating in accordance with the WidePoint NFI SSP or Organization CPS that meets the requirements of this WidePoint NFI SSP CP, as well as any MOAs between the WidePoint NFI SSP or Organization and any other Organization as defined in terms of this WidePoint NFI SSP CP. Components other than WidePoint NFI SSP or Organization Certificate Authorities may be audited fully or by using a representative sample.

If the auditor uses statistical sampling, all PKI components, PKI component managers and operators must be considered in the sample. The samples must vary on an annual basis.

A full compliance audit for the PKI covers all aspects within the scope identified above.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

When the external independent auditor finds a discrepancy between a WidePoint NFI SSP or Organization system's operation and the stipulations of this WidePoint NFI SSP CP or the WidePoint NFI SSP or Organization CPS, the following actions must be performed:

- The external independent auditor must document the discrepancy;
- The external independent auditor must notify the responsible party promptly;
- The WidePoint NFI SSP PMA must determine what further notifications or actions are necessary to meet the requirements of this WidePoint NFI SSP CP, the WidePoint NFI SSP or Organization CPS, and any relevant MOA provisions between the FPKIPA and the WidePoint NFI SSP PMA. The WidePoint NFI SSP PMA must proceed to make such notifications and take such actions without delay.

8.6 COMMUNICATIONS OF RESULTS

On an annual basis, the WidePoint NFI SSP PMA must submit an annual review package to the FPKIPA. This package must be prepared in accordance with the FPKI Annual Review Requirements document and includes an assertion from the WidePoint NFI SSP PMA that all WidePoint NFI SSP and Organization components have been audited - including any components that may be separately managed and operated. The package must identify the versions of the WidePoint NFI SSP CP and WidePoint NFI SSP or Organization CPS used in the assessment. Additionally, where necessary, the results must be communicated as set forth in Section 8.5 above.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

The WidePoint NFI SSP PMA reserves the right to charge a fee to each Organization and Applicant that wishes to receive certificates from the WidePoint NFI SSP. Fees are published in WidePoint's GSA Schedule #47QTCA19D009F.

9.1.1 CERTIFICATE ISSUANCE OR RENEWAL FEES

The WidePoint NFI SSP or Organization must make this determination and clearly state the expectations in the WidePoint NFI SSP or Organization CPS.

9.1.2 CERTIFICATE ACCESS FEES

Section 2 of this WidePoint NFI SSP CP requires that WidePoint NFI SSP or Organization certificates be publicly available. The WidePoint NFI SSP or Organization must make this determination for access to WidePoint NFI SSP or Organization Subscriber certificates in the WidePoint NFI SSP or Organization CPS.

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEES

The WidePoint NFI SSP or Organization must not charge additional fees for revoking certificates or access to CRLs and OCSP status information.

9.1.4 FEES FOR OTHER SERVICES

The WidePoint NFI SSP or Organization must make this determination in the WidePoint NFI SSP or Organization CPS.

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 CP and the WidePoint NFI SSP CPS 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 CP, the WidePoint NFI SSP CPS 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 CP, the WidePoint

NFI SSP CPS 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 CP and the WidePoint NFI SSP CPS shall be referenced in all WidePoint NFI SSP Subscriber agreements.

9.2 FINANCIAL RESPONSIBILITY

This WidePoint NFI SSP CP 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

WidePoint NFI SSP or Organization information identified in Section 2 not requiring protection must be made publicly available. Public access to organizational information must be determined by the respective organization. WidePoint NFI SSP access to Organization information will be addressed in the contract with that Organization.

9.3.1 SCOPE OF BUSINESS CONFIDENTIAL INFORMATION

The WidePoint NFI SSP or Organization must make this determination in the WidePoint NFI SSP or Organization CPS.

9.3.2 Information Not Within the Scope of Business Confidential Information

The WidePoint NFI SSP or Organization must make this determination in the WidePoint NFI SSP or Organization CPS.

9.3.3 Responsibility to Protect Business Confidential Information

Confidential business information provided by the Organization to the WidePoint NFI SSP is protected in accordance with the terms of the agreements entered into between the WidePoint NFI SSP and the Organization. Confidential business information provided by the FPKI to the WidePoint NFI SSP is protected in accordance with the terms of the MOA entered into between the WidePoint NFI SSP and the FPKI.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The WidePoint NFI SSP or Organization must make this determination in the WidePoint NFI SSP or Organization CPS.

9.4.2 Information Treated as Private

For WidePoint NFI SSP and Organization, collection of PII must be limited to the minimum necessary to validate the identity of the WidePoint NFI SSP and Organization Subscriber. This may include attributes that corelate identity evidence to authoritative sources. The WidePoint NFI SSP and Organization Registration Authority must provide explicit notice to the subscriber regarding the purpose for collecting and maintaining a record of the PII necessary for identity proofing and the consequences for not providing the information. PII collected for identity proofing purposes must not be used for any other purpose.

9.4.3 Information Not Deemed Private

Information included in certificates is not subject to protections outlined in Section 9.4.2 of this WidePoint NFI SSP CP but may not be sold to a third party.

9.4.4 Responsibility to Protect Private Information

Sensitive information must be stored securely and may be released only in accordance with other stipulations in Section 9.4 of this WidePoint NFI SSP CP.

All information collected as part of the identity proofing process must be protected to ensure confidentiality and integrity. In the event the Entity terminates PKI activities, it must be responsible for disposing of or destroying sensitive information, including PII, in a secure manner, and maintaining its protection from unauthorized access until destruction.

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

The WidePoint NFI SSP does not disclose private information to any third party unless authorized by this WidePoint NFI SSP Policy, required by law, government rule or regulation, or order of a court of competent jurisdiction.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

The WidePoint NFI SSP or Organization must not knowingly violate intellectual property rights held by others.

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.

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

With respect to WidePoint 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 a WidePoint 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.

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.

9.6.4 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.

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 certificates 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 validating 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 revocation of any or all WidePoint NFI SSP certificates issued to the organization.

9.6.5.6 Third-Party Requestor Representations and Warranties

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

- The Third-Party Requestor must protect Subscribers' recovered key(s) from compromise. The Third-Party Requestor must use a combination of computer security, cryptographic, network security, physical security, personnel security, and procedural security controls to protect their keys and recovered WidePoint NFI SSP or Organization Subscribers' keys.
- The Third-Party Requestor must destroy or surrender WidePoint NFI SSP or Organization Subscribers' keys when no longer required (i.e., when the data has been recovered).
- The Third-Party Requestor must request and use the WidePoint NFI SSP or Organization Subscriber's escrowed key(s) only to recover WidePoint NFI SSP or Organization Subscriber's data they are authorized to access.
- The Third-Party Requestor must accurately represent themselves to all entities during any key recovery service.
- When the request is made, the Third-Party Requestor must provide accurate identification and authentication information at least to the same level required for issuing new PKI certificates at the level of the key being requested (e.g., the Third-Party Requestor sends a digitally signed request using the credential issued by the WidePoint NFI SSP or Organization at the same or higher assurance level as the key being recovered).
- The Third-Party Requestor must protect information concerning each key recovery operation.
- Upon receipt of the recovered key(s), the Third-Party Requestor must sign an acknowledgement of agreement to follow the law and the WidePoint NFI SSP or Organization Subscriber's organization policies relating to protection and release of the recovered key. Such agreement should include the following attestations attestation:
    - Third Party Requestor has been accurately represented their identity to all key recovery entities,
    - Third Party Requestor has truthfully described the reason(s) for the key recover request,
    - Third Party Requestor has a legitimate and official need to obtain the requested key(s),
    - Third Party Requestor has received the recovered key(s),
    - Third Party Requestor will use the recovered key only for the stated purpose(s),
    - Third Party Requestor will protect the recovered key form unauthorized access. When no longer required, the Third Party Requestor shall either destroy the key(s) and inform the organization of destruction per agency requirements or return any recovered key(s) stored on hardware to the organization.
    - Third Party Requestor is bound by applicable laws and regulations concerning the protection of the recovered key(s) and any data recovered using the key(s).

9.7 DISCLAIMERS OF WARRANTIES

The WidePoint NFI SSP or Organization may not disclaim any responsibilities described in this WidePoint NFI SSP CP.

9.8 LIMITATIONS OF LIABILITY

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

9.9 INDEMNITIES

Agents of the WidePoint NFI SSP (e.g., WidePoint NFI SSP Registration Authorities, WidePoint NFI SSP Issuer, WidePoint NFI SSP Registrar, WidePoint NFI SSP 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 CP will remain in effect until an updated WidePoint NFI SSP CP supplants this CP, or the WidePoint NFI SSP is terminated.

9.10.2 TERMINATION

Termination of this WidePoint NFI SSP CP is at the discretion of the WidePoint NFI SSP PMA.

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

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

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

For the WidePoint NFI SSP or Organization, any planned change to the infrastructure that has the potential to affect the FPKI operational environment must be communicated to the FPKIPA at least two weeks prior to implementation. All new artifacts (WidePoint NFI SSP or Organization Certificate Authority certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the change must be provided to the FPKIPA within 24 hours following implementation.

9.12 AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENT

The WidePoint NFI SSP will notify the FPKIPA of any changes to this WidePoint NFI SSP CP. 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 NFI SSP will notify WidePoint NFI SSP or Organization Subscribers of any changes to subscriber obligations via posting to the WidePoint NFI SSP website. The WidePoint NFI SSP or Organization will post a summary of this WidePoint NFI SSP CP on its web site. WidePoint NFI SSP or Organization Subscriber obligation changes will be published within 7 days.

9.12.2 NOTIFICATION MECHANISM AND PERIOD

The WidePoint NFI SSP or Organization will publish information (including this WidePoint NFI SSP CP with sensitive data redacted) on the WidePoint NFI SSP or Organization web site.

9.12.3 CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED

A certificate policy object identifier will hanged if the FPKIPA determines that a change in the CP reduces the level of assurance provided.

9.13 DISPUTE RESOLUTION PROVISIONS

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

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 CP with respect to the Federal Bridge Certificate Policy and the Memorandum of Understanding between the FPKIPA and the WidePoint NFI SSP.

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

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

The WidePoint NFI SSP and Organization are required to comply with applicable law.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 ENTIRE AGREEMENT

This WidePoint NFI SSP CP 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 CP.

9.16.2 ASSIGNMENT

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

9.16.3 SEVERABILITY

Should it be determined that one section of this WidePoint NFI SSP CP 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 CP. 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 CP 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 CP 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 CP 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 CP, 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 CP 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.
- 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 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] <#>[1], 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
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

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

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

[2] 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 Bridge Certificate Policy CA G#, OU=FPKI, O=U.S. Government,C=US or cn=WIDEPOINT NFI ROOT [UNIQUE NAME] <#>[3], 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] <#>[4], 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[5]	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

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

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

[5] 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[6]	c=no; octet string
subject key identifier[7]	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/

[6] 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.

[7] 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[8]	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};

[8] 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[9]	c=no; octet string
subject key identifier[10]	c=no; octet string

[9] 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.

[10] 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[11]	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}[12]

[11] 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).

[12] 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[13]	c=no; octet string
subject key identifier[14]	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.

[13] 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.

[14] 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[15]	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}[16]

[15] 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).

[16] 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[17]	c=no; octet string
subject key identifier[18]	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.

[17] 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.

[18] 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[19]	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}[20]

[19] 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).

[20] 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[21]	c=no; octet string
subject key identifier[22]	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.

[21] 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.

[22] 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[23]	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}[24]

[23] 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).

[24] 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[25]	c=no; octet string
subject key identifier[26]	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

[25] 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.

[26] 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[27]	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}[28]

[27] 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).

[28] 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[29]	c=no; octet string
subject key identifier[30]	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.

[29] 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.

[30] 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[31]	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.

[31] 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}[32]	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>

[32] 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[33], thisUpdate, nextUpdate[34],
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

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

[34] 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.

1. 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.
2. 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.
3. 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.
4. 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.

5. 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 22, 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	An individual who represents a device or group in all certificate life-cycle activities. A PKI Sponsor asserts that the certificate and associated private key are being used in accordance with the subscriber and certificate specific obligations in this CP.
privacy	State in which data and system access is restricted to the intended user community and target recipient(s).
Public Key Infrastructure (PKI)	Framework established to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	Entity responsible for identification and authentication of certificate subjects that has automated equipment for the communication of Subscriber data to Certification Authorities and does not sign or directly revoke certificates.
re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application.
Relying Party	A person who has received a certificate and a digital signature verifiable with reference to a public key listed in the certificate and is in a position to rely on them. [ABADSG]
Remote Workstation	In the context of FPKI, "remote workstation" refers to a system used to access either the system hosting the CA or the CA itself through a network or networks that are not dedicated to the maintenance and administration of the CA. Note: Reference Sections 5.1, 6.5, 6.6.1, and 6.7 for additional technical controls required of remote workstations. This term does not refer to consoles within the CA's security perimeter or to Registration Authority workstations.
renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
repository	A trustworthy system for storing and retrieving certificates or other information relevant to certificates. [ABADSG]
risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
risk tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
server	A system entity that provides a service in response to requests from clients.
subordinate CA	In a hierarchical PKI, a CA whose certificate signing key is certified by another CA, and whose activities are constrained by that other CA. (see superior CA)
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to such an entity, and (2) holds a private key that corresponds to a public key listed in that certificate. [ABADSG]. Current Subscribers possess valid ECA-issued certificates.
superior CA	In a hierarchical PKI, a CA who has certified the certificate signing key of another CA, and who constrains the activities of that CA. (see subordinate CA)
system equipment configuration	A comprehensive accounting of all system hardware and software types and settings.
technical non-repudiation	The contribution public key mechanisms make to the provision of technical evidence supporting a non-repudiation security service.
threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
trust list	Collection of Trusted Certificates used by Relying Parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of a Certificate Management Authority in providing Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.

Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure, authenticated delivery. The public keys included in Trusted Certificates are used to start certification paths. Also known as a "trust anchor".
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
two person control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements. [NS4009]
update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS140]