Certification Practices Statement
for the
WidePoint Cybersecurity Solutions Corporation
(*formerly Operational Research Consultants, Inc. (ORC)*)
Non-Federal Issuer (NFI)
Public Key Infrastructure (PKI)

Version 1.3.11

11 April 2019

11250 Waples Mill Road
South Tower, Suite 210
Fairfax, Virginia 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. Any and 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. The operation of CAs under this CPS will continue to issue certificates with cn=WidePoint NFI until such time as new CAs are stood up that assert cn=WidePoint NFI. Certificates issued that assert cn=WidePoint NFI will continue to be supported until the last valid certificate expires or is revoked.*

Revision History

Document Version	Revision Date	Revision Details
0.1	11 March 2011	Initial version established to support cross-certification with FBCA as an NFI
	2 May 2011	Edits to comply with WidePoint NFI CP.
	5 May 2011	Edits to comply with WidePoint NFI CP.
1.0	10 June 2011	Edits resulting from Triennial Phase 1 audit.
1.1	17 Nov 2011	Updates resulting from operational updates and completion of Triennial Phase 1 audit.
1.2	12 June 2013	Updates corresponding to changes to CP.
1.3	20 March 2014	Review and updates to Section 5.1.2 procedures to include access for authorized Widepoint personnel and contractors; Update to OIDs; Updates resulting from 2013 audit.
1.3.1	15 July 2015	Annual review and update
1.3.2	14 Aug 2015	Formatting update
1.3.3	23 Nov 2015	Edits to Section 3.2.3.2 removing unneeded sub-heading; adding clarifying text.
1.3.4	4 Feb 2016	Add corporate name change from ORC to Widepoint Cybersecurity Solutions Corporation; addition of Cert-on-device capabilities
1.3.5	28 Apr 2016	Add “Notice” to clarify corporate name change and its implication.
1.3.7	21 Jul 2016	Certificate policy description update
1.3.8	29 August 2018	Annual review and update
1.3.10	15 March 2019	Update to address FBCA CP change requests Annual review and update
1.3.11	11 April 2019	Key recovery practices

TABLE OF CONTENTS

1 Introduction

WidePoint, as a Non-Federal Issuer (NFI), has elected to establish a Certificate Authority (CA) designed and maintained in accordance with established guidance for the purpose of issuing digital certificates and identity cards which are "(a) technically interoperable with Federal government systems, and (b) issued in a manner that allows Federal government relying parties to trust the cards." The WidePoint Non-Federal Issuer Public Key Infrastructure, hereafter referred to as The WidePoint NFI PKI, will operate in accordance with the WidePoint Non-Federal Issuer Certificate Policy v1.3 dated XX February 2019, hereafter referred to as the WidePoint NFI CP.

The goal of the WidePoint NFI PKI is to issue Personal Identity Verification Interoperable (PIV-I) identity cards, as well as other human and device certificates that can be "trusted by the Federal government" through cross-certification with the Federal Bridge Certification Authority (FBCA), accepted as a valid physical and logical form of identity within and outside of the Federal government, and provide a commensurate level of assurance to complement the Federal PKI community.

At a minimum, the WidePoint NFI PKI will provide the following security management services:

- Key generation/storage
- Certificate generation, modification, renewal, rekey, and distribution
- Certificate revocation list (CRL) generation and distribution
- Directory management of certificate related items
- Certificate token initialization/programming/management
- System management functions (e.g., security audit, configuration management, archive)

In accordance with the WidePoint NFI CP, Subscribers are required to use FIPS 140 validated cryptographic modules for cryptographic operations and the protection of trusted public keys. Furthermore, the use of WidePoint NFI PKI certificates with devices requires the use of FIPS 140 validated cryptographic modules for cryptographic operations and the protection of trusted public keys.

The WidePoint NFI PKI certificates may be utilized for, but are not limited to, 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 the WidePoint NFI CP or this Certification Practices Statement (CPS) outside of the purview of the WidePoint NFI PKI is specifically prohibited. It is intended that the WidePoint NFI PKI support interoperability with the Federal PKI.

This document is defined as the WidePoint NFI PKI Certificate Practice Statement, hereafter referred to as the WidePoint NFI CPS and is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) request for comments (RFC) 3647, CP and Certification Practices Statement Framework.

The terms and provisions of this WidePoint NFI CPS are to be interpreted under and governed by applicable Federal law and the laws of the Commonwealth of Virginia.

1.1 Overview

This WidePoint NFI CPS is the implementation document for the WidePoint NFI PKI.

The policies in the WidePoint NFI CPS represent policies for Medium, Medium Hardware, PIV-I Hardware, PIV-I Card Authentication, PIV-I Content Signing, Device, and Device Hardware certificates. Operation of the WidePoint NFI PKI is established by cross-certification with the FBCA. Successful cross-certification asserts that the WidePoint NFI PKI operates in accordance with the standards, guidelines, and practices of the Federal PKI Policy Authority (FPKIPA), acting on the authority of the Identity, Credential and Access Management Subcommittee (ICAMSC) of the Federal Chief Information Officer (CIO) Council's Information Security and Identity Management Committee (ISIMC). The WidePoint NFI CPS applies to Subscribers who are human (individuals, business representatives, State and Local Government employees, etc.) or devices (relying parties, organization applications and devices). Subscribers may use these certificates, to secure transactions conducted at an individual, application, machine or device level.

Certificate users include, but are not limited to, Registration Authorities (RAs), Local Registration Authorities (LRAs), Subscribers, and Relying Parties. To assist in providing these services and in meeting the reporting requirements outlined in this document, WidePoint maintains a website, which contains instructions, online forms, a summary of the WidePoint NFI CP and CPS, compliance audit results, and copies of certificates and CRLs. The website incorporates SSL to promote data integrity and to allow users to validate the source of the information. Portions of the website are access controlled and require certificate authentication for access to authorized individuals.

The WidePoint NFI PKI is periodically audited by an independent IT auditor against the WidePoint NFI CP and CPS, and operates primary and secondary secure data centers in conformance with the U.S. General Services Administration (GSA), National Security Agency (NSA), and commercial best practices.

1.1.1 Certificate Policy

The WidePoint NFI PKI operates in accordance with the policies established in the WidePoint NFI CP, v1.2, dated August 20, 2018. Every WidePoint NFI PKI certificate issued contains at least one registered and cross-certified certificate policy object as listed in Section 1.2, Table 1 in the *certificatePolicies* extension of the certificate issued. This certificate policy object identifier may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. The WidePoint NFI PKI certificate policy object identifier corresponds to an equivalent FBCA certificate policy object identifier with a specific level of assurance. This relationship is defined in Section 1.2, Table 2.

1.1.2 Relationship Between the WidePoint NFI CPS and the WidePoint NFI CP

The WidePoint NFI CP states what level of assurance can be placed in a certificate issued by the WidePoint NFI PKI. The WidePoint NFI CPS is the governing document for practices and procedures for instantiating those levels of assurance through certificate policy object identifiers

into X.509 version 3 certificates issued to Subscribers, both human and device. The certificate policy object identifier along with their commensurate assurance levels are defined in the WidePoint NFI CP and may be used to protect information up to and including Sensitive But Unclassified (SBU). The policies and procedures in this CPS are applicable to individuals who manage the certificates, who directly use these certificates, and individuals who are responsible for applications, servers and devices that rely on these certificates.

1.1.3 Relationship between the WidePoint NFI CP and the Federal Bridge Certification Authority (FBCA) CP

The WidePoint NFI PKI 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 the WidePoint NFI CP and those in the FBCA CP. The relationship between the WidePoint NFI CP and the FBCA CP is asserted in the cross-certificate issued by the FBCA to the WidePoint NFI CA in the policyMappings extension and reflected back in the policyMappings extension of the cross certificate issued by the WidePoint NFI CA to the FBCA.

1.1.4 Scope

The WidePoint NFI PKI exists to facilitate trusted electronic business transactions for Subscribers who may be human (individuals, business representatives, State and Local Government employees, etc) or devices (relying parties, organization applications and devices). This WidePoint NFI CPS describes the following:

- Roles, responsibilities, and relationships among the CAs, Registration Authorities (RAs), 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 CP.

- The primary obligations and operational responsibilities of the Program Participants

- The rules and requirements for the issuance, acquisition, management, and use of WidePoint NFI certificates to verify digital signatures

The WidePoint NFI CPS describes the operations of the WidePoint NFI PKI and the services which the WidePoint NFI PKI provides.

1.1.5 Interaction between WidePoint NFI PKI and the Federal Government

The WidePoint NFI CP and WidePoint NFI CPS collectively ensure interoperability between all Authorized WidePoint NFI CAs and the FBCA, including all other entities cross-certified with the FBCA at the same level of assurance and certificate policies asserted by the WidePoint NFI PKI. MOAs with the FPKIPA and other entities ensure interaction and interoperability with authorized Federal Government and non-government CAs.

1.2 Document Name and Identification

Widepoint is registered with the Internet Assigned Numbers Authority (IANA) for the registration of its own, controlled SMI Network Management Private Enterprise Code, aka "object identifier" (OID). This WidePoint OID is reflected in the first seven octets of each certificate policy object identifiers asserted in all WidePoint NFI PKI certificates issued. This registered OID can be found at:

https://www.iana.org/assignments/enterprise-numbers/enterprise-numbers

The registered OID is listed as: 1.3.6.1.4.1.3922 where the decimal notation represents {iso (1) org (3) dod (6) internet (1) private (4) enterprise (1) Operational Research Consultants (3922).

Each WidePoint NFI CA complies with the WidePoint NFI CP and CPS by asserting one of the following certificate policy object identifiers detailed in the table below in every certificate issued from the WidePoint NFI PKI.

Table 1: WidePoint NFI PKI certificate policies

Certificate Policy	Certificate Policy OID
orc	::={1.3.6.1.4.1.3922 }
orc-cybersecurity	::={orc.1 }
orc-pki	::={orc-cybersecurity.1 }
orc-nfissp-certpolicy	::={orc-pki.1 }
id-orc-nfissp-ca	::={orc-nfissp-certpolicy.100}
id-orc-nfissp-medium	::={orc-nfissp-certpolicy.3}
id-orc-nfissp-mediumHardware	::={orc-nfissp-certpolicy.12}
id-orc-nfissp-pivi-hardware	::={orc-nfissp-certpolicy.18}
id-orc-nfissp-cardAuth	::={orc-nfissp-certpolicy.19}
id-orc-nfissp-contentSigning	::={orc-nfissp-certpolicy.20}
id-orc-nfissp-mediumDevice	::={orc-nfissp-certpolicy.37}
id-orc-nfissp-mediumDeviceHardware	::={orc-nfissp-certpolicy.38}

WidePoint NFI PKI certificates issued under the WidePoint NFI CPS reference the WidePoint NFI CP in the certificatePolicy extension field of all certificate with at least one of the listed certificate policy object identifiers identified in the table above. Additionally, each WidePoint NFI CA that issues certificates asserting a PIV-I certificate policies will be cross-certified with the FBCA CA or an Authorized CA that holds a certificate signed by the FBCA CA. The foregoing certificate policy object identifiers may not be used except as specifically authorized by the WidePoint NFI CP. Unless specifically approved by the Federal PKI Policy Authority, WidePoint NFI CAs do not assert the FBCA CP certificate policy object identifiers in any certificates issued, except in the policyMappings extension establishing an equivalency between an FBCA certificate policy and a certificate policy in the WidePoint NFI CP. Only the certificate policy object indentifiers listed in Section 1.2, Table 1 are used within WidePoint NFI PKI certificates with the exception of the policyMappings extension, which may assert other PKI

certificate policy object identifiers for purposes of cross certification of the WidePoint NFI PKI to another PKI.

The WidePoint NFI PKI and this CPS support medium assurance, medium-hardware assurance and pivi-cardAuth assurance levels as defined in Section 1.4.1, Table 3.

The requirements associated with PIV-I Hardware and PIV-I Content Signing are identical to Medium Hardware except where specifically noted in the text and further described in Appendix A.

In addition, the PIV-I Content Signing policy is reserved for certificates used by the WidePoint Card Management System (CMS) to sign the PIV-I card security objects.

These certificate object identifiers for id-orc-nfissp-pivi-hardware and id-orc-nfissp-cardAuth are specifically mapped to the requirement for Personal Identification Verification – Interoperable (PIV-I). The requirements associated with the Medium Hardware certificates are identical to those defined for the Medium Assurance certificates, with the exception of Subscriber cryptographic module requirements.

Table 2: Certificate Type and OID Mapping and User

Certificate Policy type	Full certificate policy object identifier	FBCA Certificate Mapping & Use
id-orc-nfissp-medium ::=	1.3.6.1.4.1.3922.1.1.1.3	Maps to FBCA mediumAssurance. For users with software cryptographic modules. Uses: digital signature, client authentication, encryption. Mutually exclusive of id-orc-nfissp-mediumHardware.
id-orc-nfissp-mediumHardware ::=	1.3.6.1.4.1.3922.1.1.1.12	Maps to FBCA mediumHardware. For users with hardware cryptographic modules (e.g., smart card). Uses: digital signature, client authentication, encryption. Mutually exclusive of id-orc-nfissp-medium.
id-orc-nfissp-pivi-hardware ::=	1.3.6.1.4.1.3922.1.1.1.18	For user authentication (logical and/or physical access after private key activation); digital signature capability; encryption.

Certificate Policy type	Full certificate policy object identifier	FBCA Certificate Mapping & Use
id-orc-nfissp-pivi-cardAuth ::=	1.3.6.1.4.1.3922.1.1.1.19	For card authentication only, no digital signature capability (comparable to PIV card authentication with pivFASC-N name type). Uses: card authentication for physical access-private key can be used without subscriber activation. Note: a certificate asserting this policy OID is referred to as a PIV-interoperable Card Authentication certificate or PIV-I Card Auth.
id-orc-nfissp-pivi-contentSigning ::=	1.3.6.1.4.1.3922.1.1.1.20	For signing by the CMS only. Uses: certificates used by the Card Management System (CMS) to sign objects on the PIV-I Card (e.g., CHUID, Security Object).
id-orc-nfissp-mediumDevice ::=	1.3.6.1.4.1.3922.1.1.1.37	For devices only; requires a human sponsor. Uses: device authentication, encryption.
id-orc-nfissp-mediumDeviceHardware ::=	1.3.6.1.4.1.3922.1.1.1.38	For devices only; requires a human sponsor. Uses: device authentication, encryption.

Certificates issued to WidePoint NFI CAs may contain any or all of these certificate policy identifiers. Certificates issued to users to support digitally signed documents or key management from the WidePoint NFI PKI may contain the id-orc-nfissp-medium, or id-orc-nfissp-mediumHardware or id-orc-nfissp-pivi-hardware.

Certificates issued to devices from the WidePoint NFI PKI must include either or both the id-orc-nfissp-mediumDevice and id-orc-nfissp-mediumDeviceHardware. In this CPS, the term “device” is defined as a non-person entity, i.e., a hardware device or software application. The use of the mediumDevice and mediumDeviceHardware policies are restricted to devices and systems.

End-Entity certificates issued to devices after October 1, 2016 will assert certificate policies mapped to FBCA Medium Device, Medium Device Hardware, or PIV-I Content Signing policies only. All other policies defined in this document will be reserved for human subscribers when used in End-Entity certificates.

Certificates issued to users supporting authentication but not digital signature may contain id-orc-nfissp-pivi-hardware. Certificates issued to users supporting authentication where the private key can be used without user authentication may contain id-orc-nfissp-cardAuth.

1.3 PKI Entities

1.3.1 WidePoint PKI Authorities

1.3.1.1 WidePoint PKI Policy Management Authority

The WidePoint PKI Policy Management Authority (PMA) is responsible for organizing and administering this WidePoint NFI CPS; and for the operations and maintenance of all WidePoint NFI PKI components in accordance with this CPS.

This Authority is responsible for maintaining the WidePoint NFI Certificate Policy, and for ensuring that all WidePoint NFI PKI components (e.g., CAs, CSSs, CMSs, RAs) are operated in compliance with the CP.

The PMA is responsible for notifying the FPKIPA of any change to the infrastructure which has the potential to affect the FPKI operational environment at least two (2) weeks prior to implementation; all new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the change will be provided to the FPKIPA within 24 hours following implementation.

1.3.1.2 WidePoint PKI Program Manager

The WidePoint PKI Program Manager is Caroline Godfrey, Chief Security Officer.

1.3.1.3 WidePoint NFI Certification Authority

The WidePoint NFI CA is responsible for all aspects of the issuance and management of WidePoint NFI Certificates, including:

- The application/enrollment process
- The identification verification and authentication process
- The certificate manufacturing process
- Dissemination and activation of certificates
- Publication of certificates
- Renewal, suspension, revocation, and replacement of certificates
- Verification of certificate status upon request
- Generation and destruction of WidePoint NFI CA signing keys
- Ensuring that all aspects of the WidePoint NFI CA services and WidePoint NFI CA operations and infrastructure related to WidePoint NFI PKI Certificates issued under the WidePoint NFI CP and this CPS are performed in accordance with the requirements, representations, and warranties of the WidePoint NFI CP (the only exception being when the Government, pursuant to agreement between GSA, Relying Parties, and the WidePoint NFI PKI provides defined portions of the RA role and function) and this CPS.

1.3.1.4 Certificate Status Server

The WidePoint NFI PKI operates a Certificate Status Server (CSS) using an OCSP responder which provides revocation status and/or certificate validation responses. The CSS is defined as the authoritative source for certificate status information in all certificates issued by the WidePoint NFI PKI. The CSS operates in a manner which:

- Conforms to the stipulations of the WidePoint NFI CP and this CPS.
- Ensures that certificate and revocation information is accepted only from valid WidePoint NFI CAs.
- Provides only valid and appropriate responses.
- Maintains evidence of due diligence being exercised in validating certificate status.

1.3.1.5 Cross-Certification with the FBCA

In accordance with the MOA, the WidePoint NFI CA cross-certifies directly with the FBCA (through the exchange of cross-certificates). The WidePoint NFI PKI may request that the FBCA cross-certify with more than one CA within the PKI so long as that CA and the end-entity certificates issued beneath do not already have a valid path back to the FBCA. No CA or end-entity certificate may have more than one path back to the FBCA.

1.3.1.6 Key Escrow Database

The WidePoint NFI PKI Key Escrow Database (KED) is maintained within the card management system supporting WidePoint's PIV-I program.

1.3.2 Registration Authority

The RA collects and verifies each Subscriber's identity and information for inclusion in the Subscriber's public key certificate.

1.3.3 Key Recovery Agent (KRA)

A KRA is an appointed and trusted individual who, using a two-party control procedure with a second KRA, is authorized to interact with the WidePoint NFI PKI KED in order to extract an escrowed decryption private key. WidePoint KRAs send the recovered key to the Key Recovery Officer (KRO) or directly to the Requestor. WidePoint KRAs have high-level sensitive access to the KED and are considered Trusted Roles (see Section 5.2.1). A Registration Authority (RA) as defined in the WidePoint NFI Certificate Policy may fill the role of KRA; however, because KRAs can recover large number of keys, the number and location of WidePoint KRAs are closely controlled without limiting the ability to recover or operate in accordance with this CPS. WidePoint may allow Subscriber organizations to designate non-WidePoint employees to fulfill the role of KRA with the stipulation that those KRAs may recover keys of subscribers from the KRAs' Organization/Enterprise only.

1.3.4 Card Management System (CMS)

The CMS may issue certificates asserting id-orc-nfissp-pivi-hardware, id-orc-nfissp-pivi-cardAuth and id-orc-nfissp-medium-hardware in accordance with NFI PIV-I policies. In

addition, the WidePoint NFI PKI CMS is not issued any certificates which express id-orc-nfissp-pivi-hardware or id-orc-nfissp-pivi-cardAuth. Trusted users on the WidePoint NFI PKI CMS who can direct it to perform certificate-related actions are considered to be WidePoint NFI PKI RAs, as described in Section **Error! Reference source not found.**, **Error! Reference source no t found.**. A WidePoint NFI CAA, as defined herein, is the only role authorized to administer the WidePoint NFI PKI CMS.

1.3.5 Subscribers

A Subscriber is an End Entity (EE), human or device, whose name appears as the subject in a certificate, and who (PKI Sponsor, in the case of device) asserts that it uses its key and certificate in accordance with this CPS. Subscribers include, but are not limited to the following categories of entities:

- Unaffiliated Individuals (and devices), including citizens of the United States conducting personal business with a government agency at local, state or Federal level
- Employees (and devices) of businesses acting in the capacity of an employee and conducting business with a government agency at local, state or Federal level
- Employees (and devices) of state and local governments conducting business on behalf of their organization

NB: *Where certificates are issued to devices, the EE will have a human PKI Sponsor responsible for carrying out Subscriber duties.*

WidePoint NFI CAs are technically Subscribers to the WidePoint NFI PKI; however, the term Subscriber as used in this CPS refers only to those EEs who request certificates for uses other than signing and issuing certificates. Additionally, the WidePoint NFI PKI CMS and the WidePoint NFI PKI PIVotalID DCEW are Subscribers which collect and manage the data to be placed in certificate tokens responsible for managing smart card token content. The WidePoint NFI PKI CMS is issued a certificate asserting id-orc-nfissp-pivi-contentsigning and a connector certificate which grants privileges of issuing and revoking on the WidePoint NFI CAs. The WidePoint NFI PKI PIVotalID DCEW is only issued a connector certificate.

1.3.6 Affiliated Organizations

Subscriber certificates may be issued in conjunction with an organization that has a relationship with the Subscriber; this is termed affiliation. The organizational affiliation will be indicated in the 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.

For Affiliated certificates, the Subscriber must show Proof of Organizational Affiliation. A photo ID badge issued by the Affiliated Organization which shows the Subscriber's company affiliation is an acceptable means of Proof of Organizational Affiliation. If the Subscriber does not have a badge which demonstrates company affiliation, then the Subscriber will need to submit a letter on the Affiliated Organization's company letterhead, signed by a Duly Authorized Company Representative, stating that the Subscriber is either an employee of that organization or an authorized contractor affiliated with the Affiliated Organization.

The Proof of Organizational Affiliation Letter does not take the place of a second photo ID, which is required at the time of in-person validation. The Subscriber must still submit 2 photo IDs if they are using the Proof of Organizational Affiliation Letter. The Organizational Affiliation letter is retained by the Registration Authority at the time of registration.

1.3.7 Key Recovery Requestors

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

The identity of all Requestors must be authenticated as described in section 3.2.3.6, "Requestor Authentication".

1.3.7.1 Subscriber

The individual named in the certificate associated with the key being recovered. For devices, this is the human sponsor of the device.

1.3.7.2 Internal Third-Party Requestor

An Internal Third-Party Requestor is an individual who is in the Subscriber's supervisory chain or otherwise authorized to obtain the Subscriber's key from the WidePoint NFI PKI. The WidePoint NFI PKI KRS must be implemented in accordance with this CPS with respect to access and the release of sensitive information.

1.3.7.3 External Third-Party Requestor

An External Third-Party Requestor is an individual outside the Subscriber's organization with an authorized court order or other legal instrument to obtain the decryption private key of the Subscriber (e.g., investigator). An external Requestor must submit the key recovery request via an internal Requestor unless the law requires the WidePoint NFI PKI KED to release the Subscriber's private key without approval of the approval of the Issuing organization. Nothing in this document is intended to change the current procedures for obtaining information about individuals in connection with such requests. WidePoint and Subscriber organizations will appoint authorized personnel and implement this CPS so that the existing organization policy regarding release of sensitive information can be met.

1.3.8 Relying Parties

Relying Parties are those persons and entities which accept and rely upon WidePoint NFI PKI certificates for purposes of verifying digital signatures. A Relying Party is an individual or organization which, by using another's certificate can:

- Verify the integrity of a digitally signed message.
- Identify the creator of a message, or establish confidential communications with the holder of the certificate.
- Rely on the validity of the binding of the Subscriber's name to a public key.

Relying Parties, at their risk, may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

1.3.9 Other Participants

1.3.9.1 WidePoint NFI PKI Local Registration Authorities (LRAs)

WidePoint NFI PKI RAs may delegate the identity proofing tasks to Local Registration Authorities (LRAs). WidePoint NFI PKI LRAs can be WidePoint employees on location at a Subscriber's organization or employees of a Subscriber's organization. Upon performing their duties, WidePoint NFI PKI LRAs provide verification to WidePoint NFI PKI RAs via signed email using a WidePoint NFI PKI certificate asserting id-orc-nfissp-mediumHardware or id-orc-nfissp-pivi-hardware. If a WidePoint NFI PKI RA delegates duties to one or more WidePoint NFI PKI LRAs, then the WidePoint NFI PKI RA informs the WidePoint NFI CAAs. WidePoint NFI PKI LRA certificates are not valid for performing administrative tasks on the WidePoint NFI CA or WidePoint NFI PKI RA equipment, including issuing or revoking certificates.

Further description of the various WidePoint NFI PKI LRA roles are described in Section 5.2.

1.3.9.2 PKI Sponsor

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

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

This section contains definitions for three levels of assurance, and guidance for certificate usage in Relying Party applications. 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 which addresses the specific mission and environment. Each Relying Party is responsible for carrying out this risk analysis.

Table 3 provides a brief description of the appropriate uses for certificates at each level of assurance defined in this CPS. These descriptions are intended as guidance and are not binding.

Table 3: Certificate Appropriate User Guidelines

Assurance Level	Appropriate Certificate Uses
Medium	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. This level of assurance includes the following certificate policies: Medium and Medium Device.
PIV-I Card Authentication	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include contactless smart card readers where use of an activation PIN is not practical.
Medium Hardware	This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk. This level of assurance includes the following certificate policies: Medium Hardware, Medium Device Hardware, PIV-I Hardware, and PIV-I Content Signing.

1.4.1.1 Medium Assurance (Software Certificate)

This level is intended for applications handling sensitive medium value information based on the relying party's assessment, which may 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

1.4.1.2 Medium Device Assurance

Medium Device Assurance is used for authentication between computing and communications components (web servers, routers, firewalls, etc.). In such cases, the component must have a human PKI Sponsor.

1.4.1.3 PIV-I Card Authentication Assurance

PIV-I Card Authentication certificates are issued to Subscribers on hardware tokens. This level of assurance is intended for authentication to physical access systems only. The private key is not exportable. Private/secret key operations may be performed using this key with or without explicit user action (e.g., a PIN is not required to be supplied). The PIV-I Card Authentication certificate asserts id-orc-nfissp-cardAuth.

1.4.1.4 Medium Hardware Assurance

Medium Hardware Assurance certificates are issued to Subscribers on hardware tokens.

1.4.1.5 Medium Device Hardware Assurance

In addition to the stipulations for Medium Device Assurance, the private key is generated on the device and cannot be exported from the device.

1.4.1.6 PIV-I Hardware Assurance

PIV-I Hardware Assurance certificates are issued to Subscribers on hardware tokens.

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

1.4.1.7 PIV-I Content Signing Assurance

PIV-I Content Signing certificates are used to sign objects on PIV-I Cards.

1.4.2 Prohibited Certificate Uses

Certificates which assert id-orc-nfissp-cardAuth are only to be used to authenticate the hardware token containing the associated private key and are not to be interpreted as authenticating the presenter or holder of the token.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The WidePoint Policy Authority is responsible for all aspects of this CPS.

1.5.2 Contact Person

Questions regarding this CPS shall be directed to the WidePoint PKI Policy Authority at PKIPolicy@ORC.com.

1.5.3 Persons Determining WidePoint NFI CPS Suitability for the WidePoint NFI CP

The WidePoint PKI PA has determined the suitability of this CPS as part of an evaluation process. Any changes to this CPS made after determination of suitability will be transmitted to the WidePoint PKI PA for approval prior to incorporation.

The WidePoint PKI PA is responsible for ensuring that this CPS conforms to the WidePoint NFI CP and NFI PKI MOAs.

The WidePoint PKI PA approves the WidePoint NFI CPS for each CA which issues certificates under the WidePoint NFI CP.

1.5.4 CPS Approval Procedures

WidePoint NFI CAs issuing certificates under the WidePoint NFI CP are required to meet all facets of the policy. Waivers will not be issued.

The WidePoint PKI PA makes the determination that this CPS complies with the policy. The WidePoint NFI CAAs and WidePoint NFI PKI RAs must meet all requirements of an approved

WidePoint NFI CPS before commencing operations. In some cases, the WidePoint PKI PA may require the additional approval of an authorized organization or agency. The WidePoint PKI PA will make this determination based on the nature of the system function, the type of communications, or the operating environment.

In each case, the determination of suitability will be based on an independent compliance auditor's results and recommendations.

1.6 Definitions and Acronyms

See Section 12, Acronyms and Abbreviations, and Section 13, Glossary.

2 Publication and Repository Responsibilities

2.1 Repositories

The WidePoint NFI PKI operates and maintains repositories to support WidePoint NFI PKI operations. The location of any publication is available to Subscribers and Relying Parties as stipulated in this CPS.

Information in the WidePoint NFI PKI repositories is protected in accordance with the Privacy Act of 1974 as set forth in WidePoint's Privacy Policy and Procedures documents.

The WidePoint NFI PKI Repository is responsible for:

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

The WidePoint NFI PKI posts CA Certificates at the following location, accessible via HTTP:

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

The WidePoint NFI PKI posts the Root Certificate at the following location, accessible via HTTP:

- http://crl-server.orc.com/caCerts/ORCRoot2.p7c

The WidePoint NFI PKI posts CRLs at the following location, accessible via HTTP:

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

The WidePoint NFI PKI posts certificates and CRL information in a repository established by the WidePoint NFI PKI. Only information contained in the certificate(s) is posted in this directory to ensure compliance with the Privacy Act. Access to the directory is available via:

- CA Cert info is available form http://crl-server.orc.com/caCerts/ORCNFI<#>.p7c, and
- http://crl-server.orc.com/caCerts/ORCNFI<#>_SIA.p7c

The WidePoint NFI PKI directory sub-trees identify the organization of the EE.

HTTP access is defined in the CRL Distribution Point field of end entity certificates.

The certificate repository meets the following obligations:

- To list all un-expired certificates for the WidePoint NFI CAs to relying parties
- To contain an accurate and current CRL for the respective WidePoint NFI CAs for use by relying parties
- To be publicly accessible
- To be maintained in accordance with the practices specified in this CPS

- To meet or exceed the requirement of 99% availability for all components within the control of the operating organization

Communication failures as a result of Internet problems external to the operating organization will not count against this availability requirement.

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

2.1.1 Repository Obligations

Repositories are responsible for maintaining a secure system for storing and retrieving one or more of the following:

- Currently valid WidePoint NFI PKI certificates
- A current copy of this CPS and other information relevant to WidePoint NFI PKI certificates
- To contain an accurate and current CRL for the respective WidePoint NFI CAs for use by Relying Parties
- Providing certificates status services for a Relying Party

Each repository implements access controls to prevent unauthorized modification or deletion of information. WidePoint NFI CAs post CA certificates and CRLs in additional replicated repositories for performance enhancements.

Updating the repository is restricted only to authorized individuals. The WidePoint NFI PKI protects any and all repository information not intended for public dissemination or modification.

2.2 Publication of Certification Information

2.2.1 Publication of Certificates and Certificate Status

WidePoint maintains a publicly accessible repository that is available to Subscribers and relying parties that contains:

- Current, complete, and accurate CRLs issued by the WidePoint NFI PKI
- All WidePoint NFI CA certificates issued by the WidePoint NFI PKI
- A copy or link to the current WidePoint NFI CP
- A summary of this approved CPS
- Any additional policy, waiver, or practice information that is supplemental to the WidePoint NFI CP or this CPS

The repository is located at http://www.orc.com/NFI

All information published in the repository is published immediately after such information is available to the Authorized WidePoint NFI CA. The Authorized WidePoint NFI CA will publish certificates immediately upon acceptance of such certificates. At a minimum, the WidePoint NFI PKI repositories contain all CA certificates issued by or to the WidePoint NFI PKI and CRLs issued by the WidePoint NFI PKI.

Authorized WidePoint NFI CA certificates, CRLs, and online certificate status information are available for retrieval 24 hours a day, 7even days a week, with a minimum of 99% availability overall per year and scheduled down-time not to exceed 0.5% annually, excluding network outages.

2.2.2 Publication of WidePoint NFI CA Information

The WidePoint NFI CP is publicly available on the WidePoint NFI PKI website (see http://www.orc.com/NFI). The WidePoint NFI CPS for the WidePoint NFI CA will not be published; a redacted version of this CPS will be publicly available from the WidePoint NFI PKI website (see http://www.orc.com/NFI/). Additional information related to Authorized WidePoint NFI CAs is also available at this location.

2.2.3 Interoperability

Certificates and CRLs issued under this CPS are published in compliance with the WidePoint NFI CP, the WidePoint NFI CPS and the FBCA CP. The WidePoint NFI PKI ensures that all Authorized WidePoint NFI CAs are interoperable with each other, and with the FBCA repository.

2.3 Frequency of Publication

The summary of this CPS and any subsequent changes will be made publicly available within thirty (30) days of approval at the following location:

http://www.orc.com/NFI

2.4 Access Controls on Repositories

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

Access to WidePoint NFI PKI certificates and WidePoint NFI PKI certificate status information is in accordance with provisions of the WidePoint NFI PKI MOA. Access controls include:

- Access to WidePoint NFI PKI Electronic Resources is controlled by job requirements and authentication, as stipulated in this CPS.
- The WidePoint NFI PKI employees are only able to access those resources that they require to accomplish the tasks they are assigned, as stipulated in this CPS (access rights are assigned by resource [server, computer, share, volume, printer, etc.]).
- User authentication is via certificate authentication (or UserID and password when appropriate) and data encryption is used, as stipulated in this CPS.

- The WidePoint NFI PKI employees are assigned access rights before accessing any electronic resources.
- The WidePoint NFI PKI Corporate Security Auditor determines and periodically reviews user access rights.

These policies are elaborated upon in the WidePoint Systems Security Plan (SSP).

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

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

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

Table 4 below summarizes the naming requirements that apply to each applicable level of assurance.

Table 4: Certificate Naming Requirements by Assurance Level

Assurance Level	Naming Requirement
Medium (all policies)	Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical

Assurance Level	Naming Requirement
PIV-I Card Authentication	Non-Null Subject Name, and Subject Alternative Name For PIV-I Card Authentication Subscriber certificates, use of the Subscriber common name is prohibited. PIV-I Card Authentication certificates must indicate whether or not the Subscriber is associated with an Affiliated Organization by taking one of the following forms: • For certificates with an Affiliated Organization: serialNumber=UUID, ou=Affiliated Organization Name,{Base DN} • For certificates with no Affiliated Organization: serialNumber=UUID, ou=Unaffiliated, ou=Entity CA's Name,{Base DN} The UUID is encoded within the serialNumber attribute using the UUID string representation defined in Section 3 of RFC 4122 (e.g., "f81d4fae-7dec-11d0-a765-00a0c91e6bf6").

Certificates asserting id-orc-nfissp-medium, id-orc-nfissp-mediumHardware, or id-orc-nfissp-pivi-hardware indicate whether or not the 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=Entity CA's Name,{Base DN}

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

For certificates with an Affiliated Organization:

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

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

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

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

For PIV-I Card Authentication Subscriber certificates, use of the Subscriber common name is prohibited.

PIV-I Card Authentication certificates indicate whether or not the Subscriber is associated with an Affiliated Organization by taking one of the following forms:

For certificates with an Affiliated Organization:

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

For certificates with no Affiliated Organization:

- serialNumber=UUID, ou=Unaffiliated, ou=Entity CA's 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").

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

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

3.1.2 Need for Names to be Meaningful

Names used in the certificates issued by an Authorized WidePoint NFI CA identify the person or device to which they are assigned in a meaningful way, as provided in the table below.

Certificate Description	Name Meanings
Authorized WidePoint NFI CA Digital Signature Certificates	Authorized WidePoint NFI CAs implement the name constraint extension of the X.509 version 3, certificate profile in issuing CA certificates.
End Entity Digital Signature and Encryption Certificates	The authenticated common name should be the combination of first name, middle name and/or initial, and surname and reflect the legal name of the organization and/or unit.
Device Certificates	The common name may be the authenticated registered domain name of the Application server or a unique device identification naming convention such as FQDN, IP address, MAC address, device id, etc. depending on device type.
Validation Signing Certificates	The authenticated common name should be the combination of the name of the device and reflect the legal name of the organization and/or unit.

Certificate Description	Name Meanings
FBCA Cross-Certificates	Authorized WidePoint NFI CAs implement the name constraint extension of the X.509 version 3 certificate profile in issuing cross certificates.

Common Names are meaningful as individual names, as actual server Uniform Resource Locators (URLs) or Internet Protocol (IP) addresses, or as code-signing organizational names. Names identify the person or device to which they are assigned. The WidePoint NFI PKI ensures that an affiliation exists between the Subscriber and any organization that is identified by any component of any name in its certificate.

The common name used represents the Subscriber in a way that is easily understandable for humans. For people, this is typically a legal name. In the case of all Digital Signature and Encryption Certificates:

CN = Nickname Smith; or

CN = John J Smith; or

CN = John Jay Smith; or

CN = Smith.John.Jay

For equipment, this may be a model name and serial number, or an application process (e.g., Organization X Mail List or Organization Y Multifunction Interpreter).

The WidePoint NFI CAs asserting this policy only sign certificates with subject names from within a name-space approved by the GSA NFI Program Manager.

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

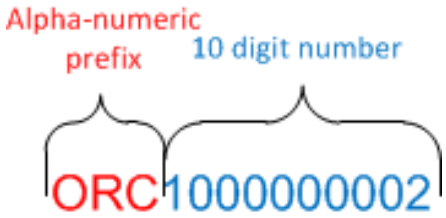


Figure 1: Example of WidePoint Unique Identifier String for Subscriber

The 10-digit number is assigned sequentially by the WidePoint NFI PKI whenever a new Subscriber receives certificates from the WidePoint NFI PKI. Subscribers with existing certificates from the WidePoint NFI PKI who have not changed name or organizational affiliation will be assigned the same 10-digit number from their previous certificates issued by the WidePoint NFI PKI, in accordance with Section 3.2.3.1 and 3.2.3.2. Subscribers with existing certificates from the WidePoint NFI whom have changed name or organizational affiliation will be assigned the next available sequential 10-digit number. The next available

sequential 10-digit number is determined by a query against the WidePoint NFI PKI certificate repository for all certificates issued to date. The alpha-numeric prefix of the Unique Identification String is assigned by the WidePoint NFI PKI.

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

.ID (for Signature Certificates)

.encrypt (for Encryption Certificates)

.Auth (for Authentication Certificates)

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

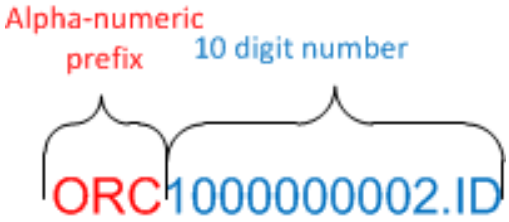


Figure 2: WidePoint Unique Identification String with Certificate Type Appended

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

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

3.1.3 Anonymity or Pseudonymity of Subscribers

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

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting name forms are contained in the applicable certificate profile (see section 7.1.4, Name Forms). The WidePoint NFI PKI PIV-I certificate profiles are established by the WidePoint NFI PKI PA and conform to the FPKI-PROF.

Rules for interpreting the PIV-I certificates UUID name are specified in RFC 4122.

3.1.5 Uniqueness of Names

The WidePoint NFI PKI complies with uniqueness of names; including X.500 DNs. The WidePoint NFI PKI enforces name uniqueness, as described in section 3.1.1, Types of Names, and section 3.1.2, Need for Names to be Meaningful.

The WidePoint NFI PKI ensures the following for Subscriber names:

- The name contains the Subscriber identity and organization affiliation (if applicable) that is meaningful to humans

The naming convention is described in this CPS (see Section 3.1.1, Types of Names).

The WidePoint NFI PKI complies with the WidePoint NFI PKI PA for the naming convention as described in Section 1.3.1.3, WidePoint NFI Certification A.

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

3.1.6 Recognition, Authentication, and Role of Trademarks

A corporate entity is not guaranteed that its Common Name will contain a trademark if requested. The WidePoint NFI PKI will not issue that name to the rightful owner if it has already issued one sufficient for identification.

The use of trademarks in a name form or as any part of a name form is discouraged. Trademarks will not be used as a name form or as a part of the name form for certificates issued to government employees unless U.S. Government personnel hold them or devices have a legitimate right to their use. The holder of the trademark will only use trademarks in certificates issued to contractors, contractor-owned servers, foreign nationals, or organizations with specific permission.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

In cases where the Subscriber generates key pairs, the Subscriber is required to prove, to a WidePoint NFI CA, possession of the private key that corresponds to the public key in the certificate request. Subscribers are required to use a FIPS 140-2 validated cryptographic module for generation of keys. In the case of certificate requests for id-orc-nfissp-medium certificates, the WidePoint NFI CA(s) performs a browser check prior to registration to ensure compliance against a list of FIPS 140-2 Level 1 browsers and upon submitting a registration request. WidePoint NFI CAs only allow compliant key pair generation. In the case of certificate requests for id-nfissp-pivi-cardAuth certificates, key pair generation must be accomplished with a Level 2-compliant token in the presence of a WidePoint NFI PKI RA or LRA, or other specifically assigned authority.

For id-orc-nfissp-medium (except as noted in the following paragraph), the public key generated by the browser's associated Cryptographic Service Provider (CSP) and the challenge string supplied by the WidePoint NFI CA are DER (Distinguished Encoding Rules) encoded together, and the resulting PublicKeyAndChallenge value is then digitally signed with the private key to produce a SignedPublicKeyAndChallenge value. This signed value is then base 64 encoded and sent to the WidePoint NFI CA as part of the certificate request; the WidePoint NFI CA verifies the signature using the included public key, thus proving possession by the browser's CSP of the private key corresponding to that public key.

For id-orc-nfissp-mediumHardware, the key pair is generated by the CSP associated with the cryptographic device (validated at FIPS 140-2 Level 2 or above).

For id-orc-nfissp-pivi-hardware or id-orc-nfissp-pivi-cardAuth, the key pair is generated by the CSP associated with the cryptographic device (validated at FIPS 201-2).

For id-orc-nfissp-pivi-contentSigning, id-orc-nfissp-mediumDevice and id-orc-nfissp-mediumDeviceHardware certificates, the Subscriber generates a key pair (private/public) using the device's associated Cryptographic Service Provider (CSP) and creates a signed PKCS10 object. For id-orc-nfissp-mediumDevice, the key pair is generated in a software CSP, at a minimum. For id-orc-nfissp-mediumDeviceHardware and id-orc-nfissp-pivi-contentSigning, the key pair is generated in a hardware CSP. For id-orc-nfissp-pivi-contentSigning, id-orc-nfissp-mediumDevice, and id-orc-nfissp-mediumDeviceHardware, the PKI Sponsor submits the PKCS10 object to the WidePoint NFI CA for certificate processing.

In all cases, WidePoint NFI PKI RAs may request additional information or verification from a WidePoint NFI PKI RA or LRA if deemed necessary by the RA to confirm the requestor's identity.

3.2.2 Authentication of Sponsoring Organization Identity

In addition to verifying the applicant's authorization to represent the Sponsoring Organization, the WidePoint NFI PKI verifies the Sponsoring Organization's current operating status and that said organization conducts business at the address listed in the certificate application. The WidePoint NFI PKI requests validation of information concerning the Sponsoring Organization, such as legal company name, type of entity, year of formation, names of directors and officers, address (number and street, city, ZIP code), and telephone number. For the website application process, all applicants are notified that the process is secure. The WidePoint NFI PKI will verify the operating status of the organization through publicly available database/websites, such as the Central Contractor Registry (CCR), Dunn and Bradstreet, and corporate and government websites.

Users will provide proof of their relationship to the company/organization for which they work. This proof can be accomplished by:

- Applicant requesting a certificate accompanied by a U.S. Government sponsor
- Applicant presenting a government-issued photo ID badge including the applicant's company affiliation
- Applicant providing a signed letter on company or agency letterhead from an authorized organization official attesting to the relationship (this is the only method approved for server certificate requests and code signing certificate requests)
- Applicant presenting an un-expired photo ID badge issued by the organization
- Citation of authorization letter on file with WidePoint

For key recovery, in addition to the authentication of a third-party requestor as described below, WidePoint will also authenticate the sponsoring organization of said requestor as described above.

3.2.3 Authentication of Individual Identity

The WidePoint NFI PKI allows a certificate to be issued only to a single entity. Certificates are not issued that contain a public key whose associated private key is shared.

Verification of an applicant's identity will be performed prior to certificate issuance. All applicants for id-orc-nfissp-medium, id-orc-nfissp-mediumHardware, id-orc-nfissp-pivi-contentSigning, id-orc-nfissp-mediumDevice, and id-orc-nfissp-mediumDeviceHardware assurance certificates are required to appear in person (except as noted below) before an RA, LRA, or Trusted Agent (Notary Public) for identity authentication. Table 5 below lists the acceptable and applicable roles authorized to perform identity verification for WidePoint NFI human Subscribers.

Table 5: Roles Authorized to Perform Identify Verification

Certificate Type	RA	LRA or TA	CMS Issuer	CMS Registrar	DCEW Issuer
id-orc-nfissp-medium	Yes	Yes	N/A	N/A	Yes
id-orc-nfissp-mediumhardware	Yes	No	N/A	N/A	Yes
id-orc-nfissp-pivi-hardware	N/A	N/A	Yes	Yes	N/A
id-orc-nfissp-pivi-cardAuth	N/A	N/A	Yes	Yes	N/A
id-orc-nfissp-pivi-contentSigning	Yes	No	N/A	N/A	N/A
id-orc-nfissp-mediumDevice	Yes	Yes	N/A	N/A	N/A
id-orc-nfissp-mediumDeviceHardware	Yes	No	N/A	N/A	N/A

Applicants for id-orc-nfissp-medium, id-orc-nfissp-mediumHardware, id-orc-nfissp-pivi-contentSigning, id-orc-nfissp-mediumDevice, and id-orc-nfissp-mediumDeviceHardware assurance certificates are required to present one Federal Government-issued Picture ID, one REAL ID Act- compliant picture ID, or two Non-Federal Government IDs, one of which shall be a photo ID (e.g., Non-REAL ID Act-compliant Driver's License). Any credentials presented must be unexpired.

The WidePoint NFI PKI RA or LRA will archive a copy of all information used in the verification process for id-orc-nfissp-medium, id-orc-nfissp-mediumHardware, id-orc-nfissp-pivi-contentSigning, id-orc-nfissp-mediumDevice, and id-orc-nfissp-mediumDeviceHardware assurance certificates.

For id-orc-nfissp-medium, id-orc-nfissp-mediumHardware, id-orc-nfissp-pivi-contentSigning, id-orc-nfissp-mediumDevice, and id-orc-nfissp-mediumDeviceHardware assurance certificates, when in-person identity-proofing is performed, the WidePoint NFI PKI RA or LRA will submit a digitally signed email message to a WidePoint NFI PKI RA, including the public key, attesting that the identity of the individual has been authenticated.

For id-orc-nfissp-medium, id-orc-nfissp-mediumHardware, id-orc-nfissp-pivi-contentSigning, id-orc-nfissp-mediumDevice, and id-orc-nfissp-mediumDeviceHardware assurance certificates, the WidePoint NFI PKI records the following information:

- The identity of the person performing the validation process
- Applicant's name as it appears in the certificate Common Name field
- A signed declaration by the identity-verifying agent that they verified the identity of the applicant
- Method of application (i.e., online, in-person)
- The method used to authenticate the applicant's identity, including identification type and unique number or alphanumeric identifier on the ID
- The date of verification
- A handwritten signature by the applicant in the presence of the person performing the identity verification

For each data element accepted for proofing, including electronic forms, the WidePoint NFI PKI records the following:

- Name of document presented for identity proofing
- The WidePoint NFI PKI RA
- Date of issuance
- Date of expiration
- All fields verified
- Source of verification (i.e., which databases used for cross-checks)
- Method of verification (i.e., online, in-person)
- Date/time of verification
- All associated error messages and codes
- Date/time of process completion

Alternately, certificate requests may be validated and authenticated on the basis of electronically authenticated Subscriber requests using a current, valid PKI signature certificate issued by a WidePoint NFI CA and associated private key. The following restrictions apply:

- The assurance level of the new certificate will be the same or lower than the certificate used as the authentication credential.
- The DN of the new certificate will be identical to the DN of the certificate used as the authentication credential.
- Information in the new certificate that could be used for authorization will be identical to that of the certificate used as the authentication credential.

- The expiration date of the new certificate will be no later than the next required in-person authentication date associated with the certificate used as the authentication credential.
- The validity period of the new certificate will not be greater than the maximum validity period requirements of the WidePoint NFI CP for that particular type of certificate.
- The in-person authentication date associated with the new certificate will be no later than the in-person authentication date associated with the certificate used for authentication.

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

Minors and others not competent to perform face-to-face registration alone are not supported under the CPS.

3.2.3.1 Authentication of Human Subscribers

3.2.3.1.1 Authentication for Digital Signature and Encryption Certificates

All procedures are described in the previous section.

3.2.3.1.2 Authentication for PIV-I Hardware and PIV-I Card Authentication Certificates

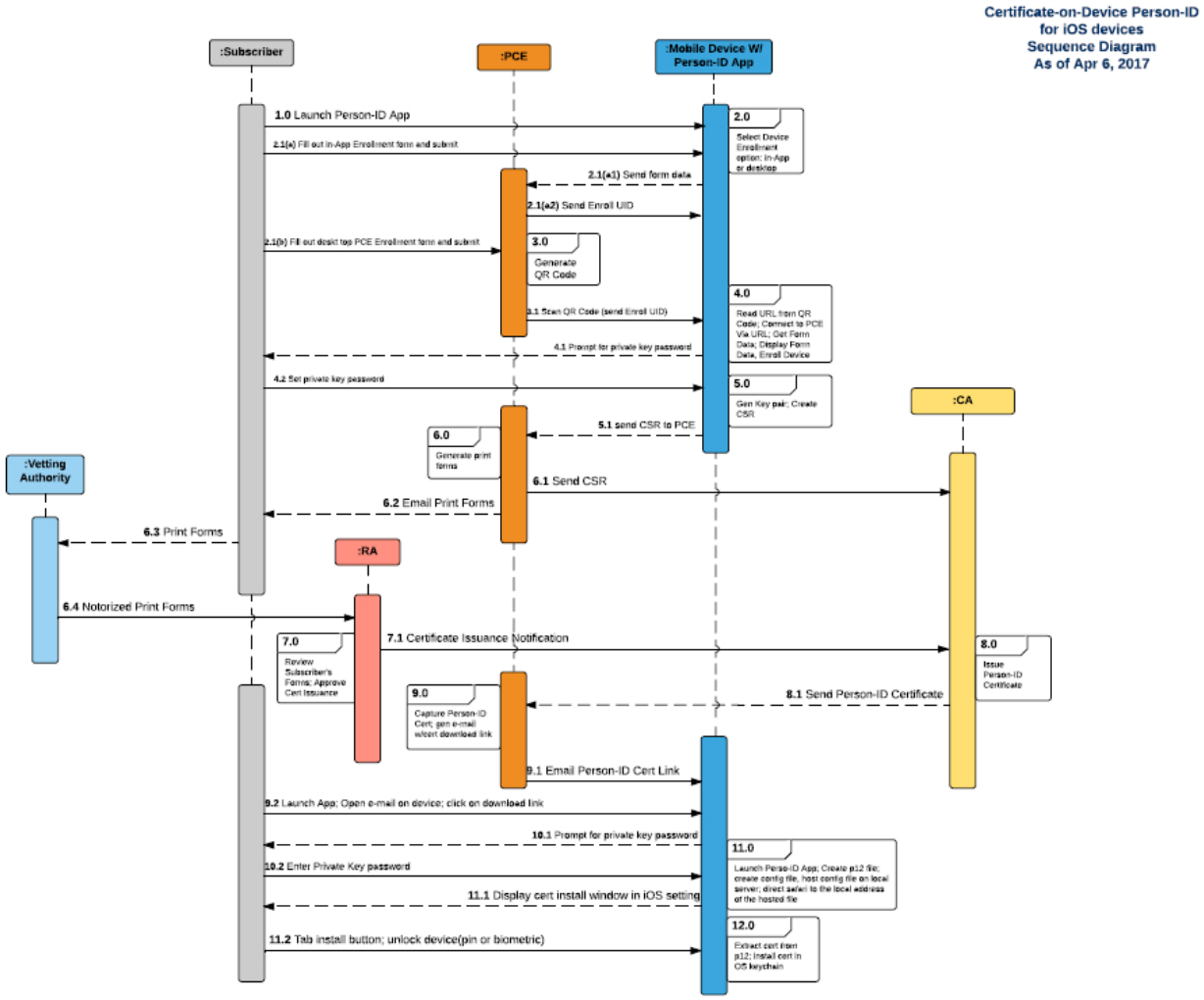
Applicants for id-orc-nfissp-pivi-hardware and id-orc-nfissp-pivi-cardAuth credentials are required to present two identity source documents in original form. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, Employment Eligibility Verification. At least one document shall be a valid State or Federal Government-issued picture identification (ID). For id-orc-nfissp-pivi-hardware and id-orc-nfissp-pivi-cardAuth, the use of an in-person antecedent is not applicable.

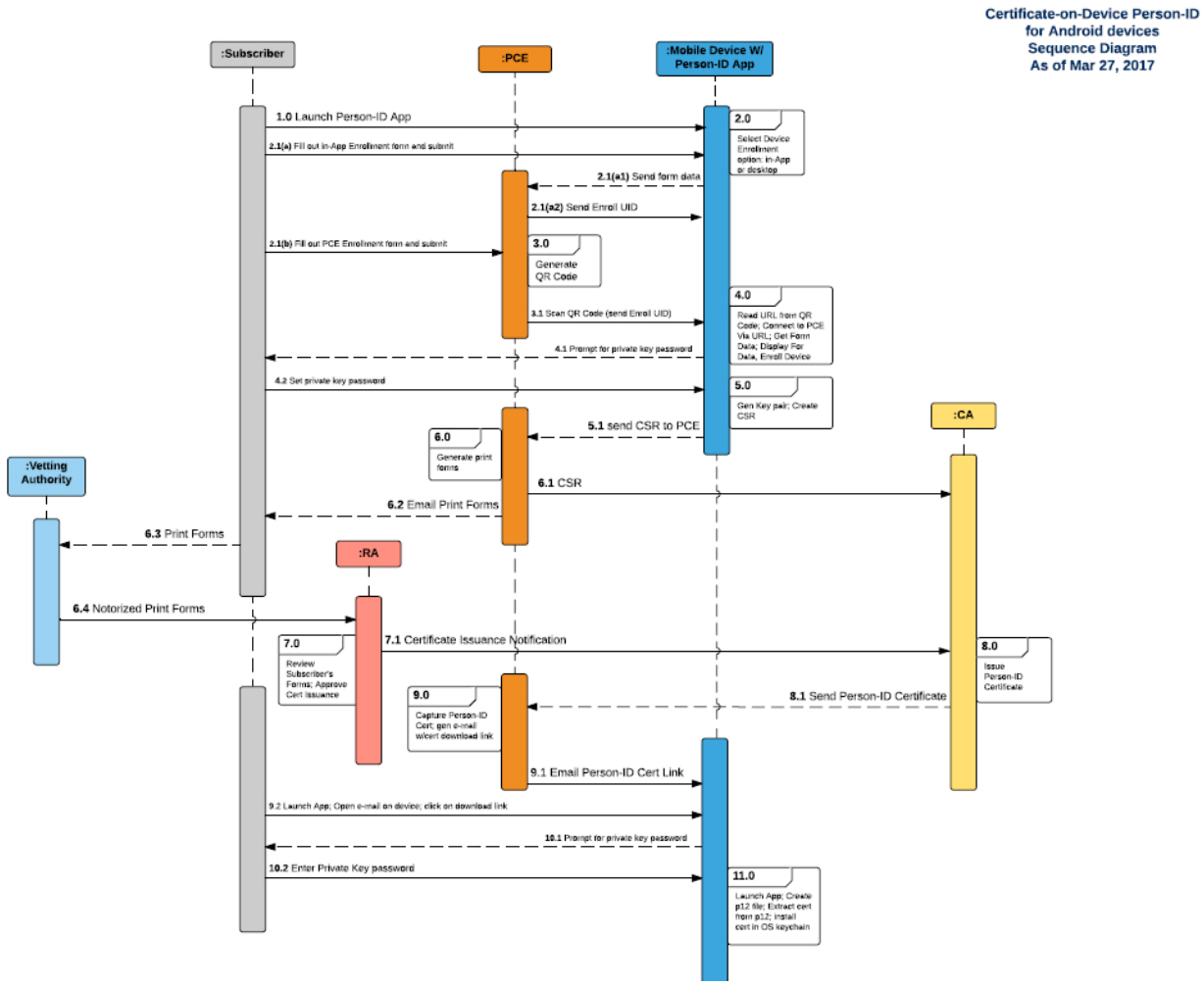
For certificates asserting id-orc-nfissp-pivi-hardware and id-orc-nfissp-pivi-cardAuth, an electronic facial image will be captured along with two fingerprints at the time of Subscriber's appearance before a WidePoint NFI PKI CMS Registrar. The electronic facial image will be used for printing facial image on the card, as well as for performing visual authentication during card usage for physical access. The WidePoint NFI PKI PIV-I credential will contain an electronic representation (as specified in NIST Special Publication 800-73, Interfaces for Personal Identity Verification [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. If a new card is being issued to an existing Subscriber the existing biometrics must be verified. Fingerprints will be stored on the card for biometric authentication during card usage. Appendix A provides additional biometric formatting information. For WidePoint NFI PKI PIV-I identity proofing, registration, and issuance process, the WidePoint NFI PKI follows the principle of separation of duties to ensure that no single individual has the capability to issue a WidePoint NFI PKI PIV-I credential without the cooperation of another authorized person, as detailed in Section 5.2.4.

3.2.3.1.3 Authentication for Certificate-on-Device Person ID Certificates

For requests made through the WidePoint NFI PKI PIVotalID DCEW, the WidePoint NFI PKI PIVotalID DCEW Issuer, as defined in Section 5.2, performs a verification of the identification documents presented and recorded during the registration process, see diagram in Section 4.1.2.2. The WidePoint NFI PKI PIVotalID DCEW Issuer performs a verification of the credential (asserting a FBCA compliant PIV, PIV-I, mediumHardware or medium certificate

policy) electronic authentication presented and recorded in the WidePoint NFI PKI PIVotalID DCEW during the registration process. The credential presented at the time of registration must still be valid at the time of issuance.





3.2.3.2 Authentication of Human Subscribers for Role-based Certificates

The WidePoint NFI PKI does not support role-based certificates.

3.2.3.3 Authentication of Human Subscribers for Group Certificates

The WidePoint NFI PKI does not support Group certificates.

3.2.3.4 Authentication of Devices

Some computing and communications components (e.g. web servers, routers, firewalls, mobile devices, etc.) may be named as certificate subjects. In such cases, the component must have a huma WidePoint NFI PKI Sponsor as described in Section 3.2.3. The WidePoint NFI PKI Sponsor is responsible for providing to a WidePoint NFI PKI RA, through an application form, correct information regarding:

- Equipment identification
- Equipment public keys
- Equipment authorizations and attributes (if any are to be included in the certificate)

- Contact information to enable the WidePoint NFI PKI to communicate with the PKI sponsor when required

A WidePoint NFI PKI RA authenticates the validity of any authorizations to be asserted in the certificate, and verifies source and integrity of the data collected to an assurance level commensurate with the certificate level being requested. Authentication and integrity checking is accomplished by the following method:

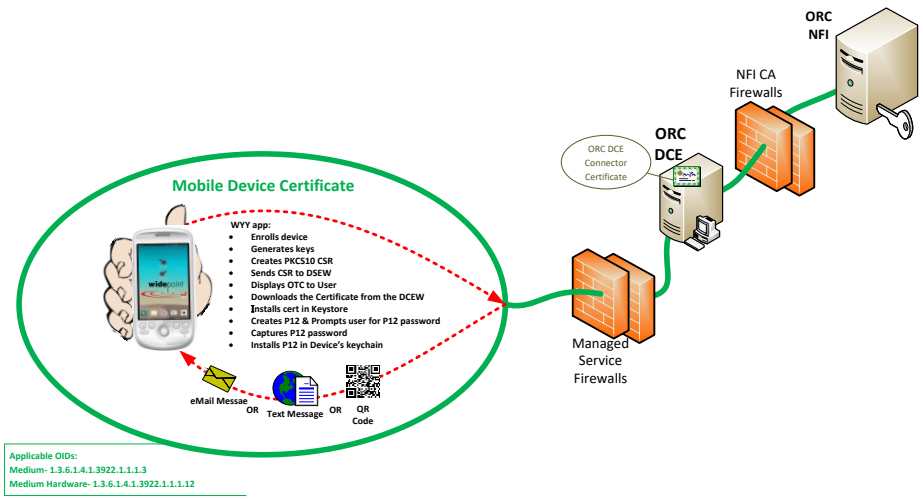
- Verification of digitally signed messages sent from PKI sponsors (using certificates of equivalent or greater assurance than that being requested);

- In person registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of Section 3.2.3.1; or

- In the case of mobile devices, through the WidePoint NFI PKI PIVotalID DCEW.

The enrollment subsystem for mobile devices is a secure application that performs the following functions for enrollment of mobile devices to the WidePoint NFI CA:

- Validates the device owner's certificate
- Parses the certificate
- Prepares and presents a DCEW Enrollment Form
- Captures, verifies and posts the Subscriber's information (Full Name, Subscriber Name, Issuer DN, and Contact number)
- Captures and posts Device information (Device Name, Device Type, Device ID, Phone number, Device OS)
- Generates and sends Enrollment Link to the user
- Receives CSR from the WYY mobile application
- Generates a One-Time-Code (OTC)
- The WidePoint NFI PKI repository securely stores the Subscriber and Device data elements.



3.2.3.5 KRA Authentication

WidePoint KRAs are assigned by a WidePoint CAA, and are issued medium hardware assurance level certificates or higher, generated on cryptographic hardware tokens which have been certified at FIPS 140-1/2 Level 2, as listed on the website of the National Institute of Standards and Technology (NIST). The identity-proofing of a WidePoint KRA is accomplished in person with a WidePoint RA, in accordance with the WidePoint CPS. The medium hardware assurance level certificate is used to access the KED, sign correspondence to the KRO and Requestor, and accept encrypted email from a KRO or Requestor.

The WidePoint NFI PKI KED is configured to establish client-authenticated SSL sessions. The WidePoint NFI PKI KED is configured (by a CAA) to recognize KRAs as legitimate Web users via certificate authentication. KRAs with a WidePoint CA-issued medium hardware assurance certificate, recognized by the KED as a KRA, are required to initiate an SSL session with the WidePoint NFI PKI KED to begin the recovery process. When that is successfully accomplished, two KRAs must authenticate to the KED over the SSL session. Upon successful authentication of the two KRAs, the KED can be used by the KRAs to effect key recovery.

3.2.3.6 Requestor Authentication

This section addresses the requirements for authentication of a third-party Requestor, i.e., a Requestor other than the Subscriber itself. The requirements for authentication, when the Requestor is the Subscriber, are addressed in Section 3.2.3.2.

WidePoint ensures that a Requestor establishes his or her identity to a KRA (or a KRO, as an intermediary for the KRA). In cases where an electronic request is made a KRA or KRO will verify the digital signature on the request and ensure that the request is signed using a certificate at least to the specified assurance level of the key being recovered, prior to initiating the key recovery request. In all cases where a digitally-signed electronic request is made (directly to a KRA, or via a KRO), a KRA must authenticate the identity of the Requestor (and the KRO) by validating their digital signatures.

In cases where digital authentication is not possible, a KRA or KRO will perform in person identity authentication, as specified in Section 3.1. If performed by a KRO, the KRO will provide that information to the KRA, along with a recovery request for the Requestor, via digitally signed email. The KRA receiving the KRO email must authenticate the identity of the KRO by validating the digital signature of the KRO.

In all cases KRAs may request additional information or verification from a KRO if deemed necessary by the KRA to confirm the Requestor's identity.

WidePoint NFI PKI KROs or KRAs will verify the identity of the Requestor prior to initiating the key recovery request.

3.2.4 Non-verified Subscriber Information

The WidePoint NFI PKI does not include information in certificates that has not been verified.

3.2.5 Validation of Authority

Before issuing certificates that assert organizational authority, the WidePoint NFI PKI validates the individual's authority to act in the name of the organization. This validation is performed by having the applicant complete and submit an "Proof of Organizational Affiliation" letter, made

available to applicants on the WidePoint NFI PKI website. The WidePoint NFI PKI uses Proof of Organizational Affiliation letters for applicants attempting to obtain Component/Server certificates. A specific Proof of Organizational Affiliation letter is provided for each particular type of certificate request.

The WidePoint NFI PKI additionally requires a Proof of Organizational Affiliation for certificate requests from individuals who either do not possess a company-issued photo ID badge or organizations which do not issue company photo ID badges, signed by a Duly Authorized Company Representative, stating that they are an employee of that organization.

3.2.5.1 Requestor Authorization Validation

The WidePoint NFI PKI KRA or the KRO, as an intermediary for the WidePoint NFI PKI KRA, will validate the authorization of the Requestor in consultation with Issuing Organization management and/or legal counsel, as appropriate.

3.2.5.2 Subscriber Authorization Validation

Current Subscribers are authorized to request recovery of their own escrowed key material.

3.2.5.3 KRA Authorization Validation

The WidePoint NFI PKI KED will verify that the KRA has the appropriate privileges to obtain keys for the identified subscriber's organization.

3.2.6 Criteria for Interoperation

The FPKIPA determines the interoperability criteria for CAs operating under the FBCA policy. MOA(s) with the FPKIPA and other entities ensure interaction and interoperability with Authorized WidePoint NFI CAs, authorized State and Local Government agencies, and non-government CAs. At no point will CA or end-entity certificates issued under the NFI CP have more than one path back to the FBCA.

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

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

WidePoint NFI PKI Certificate re-keying (signing and encryption) is accomplished through the limitation on certificate renewal. The minimum requirement for all WidePoint NFI PKI certificate re-keying, with the exception of WidePoint NFI CA certificates, is once every 9 years from the time of initial registration (i.e., after two 3-year renewals). WidePoint NFI PKI Subscribers must identify themselves for the purpose of re-keying through use of their current signature key, except that identity will be established through the initial registration process described in Section 3.2. Table 6 provides the routine re-key identify requirements.

Table 6: Routine Re-key Identity Requirements

Assurance Level	Routine Re-key Identity Requirements for Subscriber Signature, Authentication and Encryption Certificates
Medium (all policies)	Identity will be established through use of the current signature key certificate, except that identity will be established through the initial registration process at least once every nine years from the time of initial issuance. For id-orc-nfissp-mediumDevice and id-orc-nfissp-mediumDeviceHardware certificates, Identity will be established through use of the current signature key certificate or using means commensurate with the strength of the certificate being requested, except that identity will be established through initial registration process at least once every nine years from the time of initial registration
PIV-I Card Authentication	Identity may be established through use of the current signature key certificate, except that identity will be established through initial registration process at least once every nine years from the time of initial registration.

Subscribers' signature private keys and certificates have a maximum lifetime of 3 years. Subscriber encryption certificates have a maximum lifetime of 3 years; use of Subscriber decryption private keys is unrestricted.

The WidePoint NFI PKI accepts certificate renewal requests from their Subscribers within 90 days from the scheduled end of the operational period (expiration date) of the WidePoint NFI PKI certificate, provided the WidePoint NFI PKI certificate is not revoked, suspended, or expired. WidePoint NFI PKI Certificates are renewed in 3-year increments; no more than 3 times before certificate re-key is required.

To renew a certificate, as described in the WidePoint NFI CP, the Subscriber obtains a new certificate based on an existing key pair. The WidePoint NFI PKI authenticates the Subscriber's renewal request using the Subscriber's current certificate for authentication in the renewal process. The authentication in the renewal process examines the expiration date of the current certificate and will only allow renewal if within 90 days of expiration but currently valid. In the event that subject information has changed (and/or the key pair is required to be changed for any reason), the WidePoint NFI PKI requires the Subscriber to request a new WidePoint NFI PKI certificate. The old certificate (as a result of an update action) may or may not be revoked, but is not further re-keyed, renewed, or updated. A certificate that is not renewed by the end of the operation period reflects an expired status.

Server Subscribers (PKI Sponsors) are required to revalidate their identity and any equipment authorizations and/or attributes (if any are to be included in the certificate).

The Subscriber is required to present a currently valid certificate to request a new certificate.

WidePoint NFI PKI certificates asserting id-orc-nfissp-medium may be renewed or updated on the basis of electronically authenticated Subscriber requests two times. Every 9 years, in-person authentication is required.

WidePoint NFI PKI certificates asserting id-orc-nfissp-mediumHardware may be renewed or updated on the basis of electronically authenticated Subscriber requests only one time. Every 6 years, in-person authentication is required.

During the renewal process, the user must present his or her current WidePoint NFI PKI identity certificate during an SSL client authentication to the WidePoint NFI CA. The WidePoint NFI CA validates the authenticity of the certificate being presented by verifying that the certificate was issued by the WidePoint NFI CA in question and mapping the subject name in the certificate to its corresponding certificate in the database. This process verifies that the Subscriber is eligible for renewal on the basis of the Subscriber's existing certificate, as stipulated above. If the Subscriber is not eligible for renewal on the basis of the Subscriber's existing certificate, WidePoint NFI PKI redirects the Subscriber to the in-person registration process. The forms to accomplish this process are controlled by access control lists on a secure web server that binds to the corresponding users with certificates in the repository. Access control to the renewal forms is based on comparing the certificate with the Distinguished Name of the Subscriber (based on an X.509 certificate-based authentication) against the certificate with DN in the directory.

In cases where a Subscriber's organization (including WidePoint NFI PKI Sponsors) has required authorizations to be included in a WidePoint NFI PKI certificate, the person responsible for that organization's WidePoint NFI PKI agreement must notify a WidePoint NFI PKI RA of the withdrawal of authorizations, via digitally signed email using a medium assurance hardware certificate. The RA verifies the signature of the Subscriber's organization.

3.3.2 Identification and Authentication for Re-key after Revocation

After a certificate has been revoked or expired, the applicant is required to go through the initial registration process as described in Section 3.2.

3.4 Identification and Authentication for Revocation Request

Certificate revocation requests may be made using the same practices as certificate issuance requests. In addition, certificate revocation requests may be made electronically using email digitally signed by a certificate of equal or greater level of assurance than that of the certificate for which the request is made. In either case, the request must include the reason for revocation. See Section 4.9 for details on certificate revocation procedures.

A Subscriber may request revocation of a certificate regardless of whether or not it has been compromised. The WidePoint NFI PKI may revoke a Subscriber's certificate for cause. The WidePoint NFI PKI RA collects signed documentation stating the reason and circumstances for the revocation. If a WidePoint NFI PKI RA performs this on behalf of a Subscriber, a formal, signed message format known to the WidePoint RA is employed.

In accordance with the WidePoint NFI PKI MOA, a WidePoint NFI PKI certificate revocation request that is submitted electronically may be authenticated on the basis of a digital signature using the WidePoint NFI PKI certificate's associated key pair. The identity of the person submitting a revocation request in any other manner is authenticated in accordance with Section

4.9 of this CPS. Revocation requests authenticated on the basis of the WidePoint NFI PKI certificate's associated key pair are always accepted as valid. WidePoint NFI PKI RAs verify the authentication mechanism and balance the need to prevent unauthorized revocation requests against the need to quickly revoke certificates. In the case of certificates asserting WidePoint NFI PKI certificates, WidePoint will only accept revocation requests from the Subscriber, or WidePoint NFI PKI RAs, or persons authorized by each sponsoring organization or the WidePoint NFI PKI to make revocation requests.

4 Certificate Life-Cycle Operational Requirements

The WidePoint NFI PKI is comprised of components that include Certificate Authorities, Card Management Systems (CMS), RA Workstations, Card Management Workstations, and PIVotalID DCEW, <REDACTED>

In all cases, WidePoint NFI PKI CMS and RA Workstations are maintained with all controls and procedures for the WidePoint NFI PKI RA workstation as described throughout this CPS.

4.1 Certificate Application

The WidePoint NFI PKI offers certificates that may assert any of the policy OIDs listed in Section 1.2. The WidePoint NFI CAs are configured with certificate profiles for each of the types listed in Section 1.2. The profiles are configured with the appropriate extensions and values for each certificate type as specified in Section 7. Certificate policies are encoded in the certificate profile of the WidePoint NFI CAs and cannot be overwritten by any certificate policy asserted in the certificate request. Certificate requests are submitted against a particular profile on the WidePoint NFI CAs and cannot be transferred to a different profile.

The WidePoint NFI PKI is authorized to issue a certificate for another Certification Authority or a subordinate WidePoint NFI PKI Certification Authority.

<REDACTED>.

4.1.1 Who Can Submit a Certificate Application

The WidePoint NFI PKI only accepts certificate applications from Subscribers, either for themselves or as the designated certificate holder for a component or device. For id-orc-nfissp-medium, id-orc-nfissp-mediumhardware, id-orc-nfissp-pivi-contentSigning, id-orc-nfissp-mediumDevice, id-orc-nfissp-mediumDeviceHardware, WidePoint NFI PKI does not allow for certificate requests to be made by a WidePoint NFI PKI RA on behalf of a Subscriber.

The following parties provided in Table 7 may initiate the WidePoint NFI PKI Certificate application process:

Table 7: Authorized Certificate Application Initiators

Potential Subscriber	Authorized Initiator
Individuals	Persons associated with a business or organization Persons with no business affiliation
Devices	PKI sponsor responsible for the component receiving the certificate
State/Local Government Employee	Sponsoring Organization; or potential Subscriber

A Subscriber may request recovery of their own escrowed encryption key. Authorization of this request would be validated as documented in section 3.2.5.2, "Subscriber Authorization Validation".

Internal third-party requestors, as described in section 1.3.7.2, "Internal Third-Party Requestor", may request recovery of a Subscriber's escrowed encryption key. Authorization of this request would be validated as documented in section 3.2.5.1, "Requestor Authorization Validation".

External third-party requestors, as described in section 1.3.7.3, "External Third-Party Requestor", may request recovery of a Subscriber's escrowed encryption key. Authorization of this request would be validated as documented in section 3.2.5.1, "Requestor Authorization Validation".

The identity of all Requestors must be authenticated as described in section 3.2.3.6, "Requestor Authentication".

4.1.2 Enrollment Process and Responsibilities

The WidePoint NFI PKI provides either a Federal Information Processing Standards (FIPS) 140-2 level 3 Secure Socket Layer (SSL) connection to the certification authority or a FIPS 201-approved Card Management System (CMS) via a FIPS 140-2 level 1 or 2 client connection during enrollment. These processes are detailed in this section.

4.1.2.1 Enrollment Process and Responsibilities via WidePoint NFI PKI RA Workstation

- id-orc-nfissp-medium
- id-orc-nfissp-mediumHardware
- id-orc-nfissp-pivi-contentSigning
- id-orc-nfissp-mediumDevice
- id-orc-nfissp-mediumDeviceHardware

WidePoint NFI PKI RAs, LRAs, or Trusted Agents (as defined in section 1.3, "PKI Entities") perform identity verification (as discussed in section 3.2, "Initial Identity Validation") of Subscribers requesting certificates which assert id-orc-nfissp-medium, id-orc-nfissp-mediumDevice, or id-orc-nfissp-pivi-contentSigning. Subscribers requesting certificates asserting id-orc-nfissp-medium, id-orc-nfissp-pivi-contentSigning, id-orc-nfissp-mediumDevice may generate their certificate requests prior to appearing before a WidePoint NFI PKI RA, LRA, or Trusted Agent to have their identity verified.

For WidePoint NFI PKI certificates that assert id-orc-nfissp-mediumHardware or id-orc-nfissp-mediumDeviceHardware, only WidePoint NFI PKI RAs or LRAs are permitted to perform identity verification. Subscribers requesting certificates asserting id-orc-nfissp-mediumHardware must generate their certificate requests in the presence of a WidePoint NFI PKI RA or LRA.

During the enrollment process, the Subscriber must attest to the Subscriber Obligations as detailed in section 9.6.3, Subscriber Representations and Warranties. Upon acceptance by the Subscriber of the Subscriber Obligations, the Subscriber will submit their user-specific information in accordance with Section 3.1.1. This information will include:

- Validity Period Requested (Max 3 years)

- First Name
- Middle Name or Initial
- Last Name
- Company Name
- Email address
- Contact Phone Information

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

<REDACTED>

When applicable, as in the case of all identity and encryption certificates that will be issued to LRAs, the Subscriber's organization will provide a point of contact for verification of any roles or authorizations to be included in the Subscriber's certificates (affiliation) via signed letterhead or digitally-signed email. <REDACTED>.

4.1.2.2 Enrollment Process and Responsibilities via WidePoint NFI PKI CMS

The WidePoint NFI PKI CMS is used to manage the enrollment process for only the following certificate types:

- id-orc-nfissp-mediumHardware
- id-orc-nfissp-pivi-hardware
- id-orc-nfissp-pivi-cardAuth

Subscribers asserting an Organizational Affiliation must be authorized by a WidePoint NFI PKI Point of Contact for that Organization, as defined in Section 1.3.5.4. Subscribers asserting no Organization Affiliation will assert an Organization Unit value of Unaffiliated in their Distinguished Name.

All Subscribers requesting certificates that assert id-orc-nfissp-pivi-hardware or id-orc-nfissp-pivi-cardAuth are required to appear in-person before a WidePoint NFI PKI CMS Registrar as shown below, in accordance with Section 3.2.3.1 to complete the enrollment process.

<REDACTED>

4.1.2.3 Enrollment Process and Responsibilities via WidePoint NFI PKI PIVotalID DCEW

The WidePoint NFI PKI PIVotalID DCEW is used to manage the enrollment process for only the following certificate types:

- id-orc-nfissp-medium
- id-orc-nfissp-mediumHardware
- id-orc-nfissp-mediumDevice
- id-orc-nfissp-mediumDeviceHardware

For a certificate asserting id-orc-nfissp-medium or id-orc-nfissp-mediumHardware which is to be issued on a mobile device (but not a device certificate), an Applicant enrolls at the PIVotalID DCEW portal. During the enrollment process, the Subscriber must attest to the Subscriber Obligations as detailed in section 9.6.3, Subscriber Representations and Warranties. The Applicant enters his/her information into the site along with information for the device which will receive the certificate. The enrollment portal sends a link (via QR code, e-mail, or text as selected by the Applicant at the portal) to the device which the Applicant uses to generate a CSR. The key generation process is initiated on the mobile device. The CSR is submitted to the enrollment portal. The enrollment portal forwards the CSR to a WidePoint NFI CA. (See section 3.2.1, "Method to Prove Possession of Private Key" for relevant proof of possession discussion.) The CA delivers (via the PIVotalID DCEW) the certificate application form to the Applicant to be printed, completed, and presented to an RA or LRA (or Trusted Agent, in the case of id-orc-nfissp-medium) for identity verification as discussed in section 0, "For key recovery, in addition to the authentication of a third-party requestor as described below, WidePoint will also authenticate the sponsoring organization of said requestor as described above.

Authentication of Individual Identity".

For a certificate asserting id-orc-nfissp-mediumDevice or id-orc-nfissp-mediumDeviceHardware which is to be issued on a mobile device, an Applicant enrolls at the PIVotalID DCEW.

During the enrollment process, the Subscriber must attest to the Subscriber Obligations as detailed in section 9.6.3, Subscriber Representations and Warranties. The Applicant enters his/her information into the site along with information for the device which will receive the certificate. The WidePoint NFI PKI PIVotalID DCEW sends a link (via QR code, e-mail, or text as selected by the Applicant at the portal) to the device which the Applicant uses to generate a CSR. The key generation process is initiated on the mobile device. The CSR is submitted to the WidePoint NFI PKI PIVotalID DCEW. The enrollment portal forwards the CSR to a WidePoint NFI CA. (See section 3.2.1, "Method to Prove Possession of Private Key" for relevant proof of possession discussion.) The WidePoint NFI PKI PIVotalID DCEW application validates the credential and displays a Mobile Certificate Request form that includes the subscriber and the device information.

4.1.3 Key Escrow Process and Responsibilities

The Subscriber private keys (i.e., decryption private keys) associated with a key management certificate is securely escrowed by the WidePoint NFI PKI KED. The WidePoint NFI PKI KED is a function of the WidePoint NFI PKI Card Management System (CMS), and employs the use of a Hardware Secure Module (HSM) to secure Subscriber private keys during transit and storage using cryptography equal to or greater than the key being escrowed. The WidePoint NFI PKI CA only provides escrow for key management certificates issued through the WidePoint NFI PKI CMS. The Subscriber's private key for the key management certificate is generated in the HSM and stored encrypted and protected by the Key Encryption Key (KEK) {which is a 24-byte AES key} in the WidePoint NFI PKI KED database, prior to the key being injected onto the PIV-I card. When the WidePoint NFI PKI KED has stored the key management key, the WidePoint NFI PKI CMS, acting in conjunction with the WidePoint NFI PKI CA, establishes a secure channel session using Secure Channel Protocol (SCP-03) with the Subscriber's PIV-I card to inject the key management key and certificate into the appropriate container on the

Subscriber's PIV-I card. This secure channel is secured with AES keys; additionally, key data is encrypted with an AES data encryption key. The Subscriber's encryption keys are protected by the KEK. All cryptographic operations occur in the HSM.

4.1.4 Key Recovery Process and Responsibilities

Requestors must submit a key recovery request to a designated WidePoint NFI PKI KRA or KRO. The Requestor will digitally sign the request using a WidePoint-issued signature certificate of assurance level equal to or greater than that of the escrowed key. Written requests signed by hand, and notarized or witnessed by a WidePoint NFI PKI KRA or KRO may be accepted on a case-by-case basis.

4.1.4.1 Key Recovery through KRA

WidePoint NFI PKI KRAs are authorized to recover key(s) escrowed in the WidePoint NFI PKI KED only in response to a properly authenticated and authorized key recovery request. Recovery requires the actions of at least two WidePoint NFI PKI KRAs. Escrowed keys are protected using two-person control procedures during recovery and delivery to the authenticated and authorized Requestor, and during operation and maintenance of the WidePoint NFI PKI KED.

WidePoint NFI PKI KRA #1 authenticates to the CMS to request key recovery within the CMS. WidePoint NFI PKI KRA #2 authenticates to the CMS to approve request key recovery within the CMS. KRA #1 recovers the key to a password-protected PKCS #12 format file which is possessed by KRA #2 (who does not know the password).

For delivery, the PKCS #12 file is delivered via encrypted email from WidePoint NFI PKI KRA #1 to the Requestor (or to a KRO in the case where the Requestor cannot receive encrypted email) and the password is delivered by WidePoint NFI PKI KRA #2 via encrypted email to the Requestor (or by separate channel[1] securely to the Requestor). If the KRO receives the PKCS #12, the KRO will deliver the key to the Subscriber or authorized third party only after verifying their identification.

4.1.4.2 Automated Self-Recovery

Not Applicable. Automated self-recovery is not supported.

4.1.4.3 Key History Recovery to Hardware Token

The WidePoint NFI PKI CMS, when issuing a new PIV Card to a Subscriber, will recover previous key management keys stored in escrow for that user and inject them into the archive key management slots designated of the FIPS 201 Card for the Subscriber using the same protocols and protections as defined in Section 4.1.2.

[1] This will be accomplished via in-person delivery or tracked delivery such as USPS certified mail, FedEx, UPS, etc.

4.2 Certificate Application Processing

Information in certificate applications is verified as being accurate before certificates are issued. This section describes WidePoint NFI PKI procedures to verify information in certificate applications.

4.2.1 Performing Identification and Authentication Functions

Verification of an applicant's identity is performed prior to certificate issuance as discussed in Sections 3.2.2, "Authentication of Sponsoring Organization Identity" and 0, "For key recovery, in addition to the authentication of a third-party requestor as described below, WidePoint will also authenticate the sponsoring organization of said requestor as described above.

Authentication of Individual Identity."

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

4.2.2 Approval or Rejection of Certificate Applications

The Subscriber identification and authentication process has been completed successfully when the process(es) described in Section 3.2 have occurred and the requested name and Organization have been verified by examination of documentation.

If verification is not successful or the application is otherwise rejected, the WidePoint NFI PKI notifies the applicant of the verification failure or rejection at the time of in-person verification, or via email notification, or by way of an out-of-band notification process linked to the certificate applicant's physical postal address. This notification includes the steps required by the applicant to resume processing of the certificate request.

4.2.3 Time to Process Certificate Applications

The entire process from applicant appearing before one of the required identity verifiers to certificate issuance will take no more than 30 days. WidePoint NFI PKI RAs will not process certificate requests for issuance if the date of the Identity Verification process is more than 30 days old.

4.3 Certificate Issuance

Upon successful completion of the Subscriber identification and authentication process in accordance with this CPS and the WidePoint NFI CP, the WidePoint NFI PKI creates the requested NFI Certificate(s), notifies the applicant thereof, and makes the WidePoint NFI PKI Certificate(s) available to the applicant. If the applicant provided an email address, the WidePoint NFI PKI sends the notification message via email. If no email address was provided, the WidePoint NFI PKI sends the notification to the U.S. postal address provided.

4.3.1 CA Actions During Certificate Issuance

Upon successful completion of the Subscriber identification and authentication process, the WidePoint NFI PKI creates the requested WidePoint NFI PKI Certificate, notifies the applicant thereof, and makes the WidePoint NFI PKI Certificate available to the applicant.

<REDACTED>

At the time of issuance, the RA performs the following steps:

1. Determines the proposed Subscriber DN.
2. Verifies uniqueness of Subscriber DN against the Subscriber base (this includes a search of current and prior CAs to avoid duplications/ collisions).
3. Verifies the DN string integrity and uniformity within a specific organization, where applicable.
4. Matches the request ID number provided in the request.
5. Reviews certificate body content against LRA approval email.
6. Issues certificate, ensuring proper publication to the repository.
7. Sends certificate issuance notification (CIN) email to Subscriber's email address provided during the request <REDACTED>

At the completion of certificate issuance activity, the WidePoint NFI PKI RA logs off of the WidePoint NFI PKI RA workstation and removes his/her WidePoint NFI PKI RA Medium Hardware token.

<REDACTED>

The WidePoint NFI PKI Issuer will compare the identity documentation provided by the Subscriber against the identity documentation presented and recorded during the WidePoint NFI PKI Registrar process. Upon successful verification of the identity documentation, the WidePoint NFI PKI Issuer will print the Subscriber's WidePoint NFI PKI PIV-I credential in accordance with Section 13, Appendix A. After the card has been successfully printed, the Subscriber will authenticate with one of the fingerprints captured during the registration process and create a numeric PIN as specified in Section 6.4.1. Upon successful fingerprint match and setting of PIN, Subscriber's card begins the activation process.

<REDACTED>Upon successful completion of the WidePoint NFI PKI PIV-I Card Activation, the Subscriber must attest to the Subscriber Obligations.

For a certificate asserting id-orc-nfissp-medium or id-orc-nfissp-mediumHardware which is to be issued on a mobile device (but not a device certificate), a WidePoint NFI PKI LRA reviews the notarized forms if identity verification was performed by a Trusted Agent (otherwise, the WidePoint NFI PKI LRA would perform identity verification). If appropriate, the WidePoint NFI PKI LRA communicates her approval to a WidePoint NFI PKI RA via digitally-signed e-mail. The RA reviews the WidePoint NFI PKI LRA's communication and, if appropriate, accesses a WidePoint NFI CA in order to issue the certificate.

In the case of certificates asserting id-orc-nfissp-mediumDevice, and id-orc-nfissp-mediumDeviceHardware issued via the WidePoint NFI PKI PIVotalID DCEW the WidePoint NFI CA receives a CSR from the portal through the DCEW server. <REDACTED>

4.3.2 Notification to Subscriber by the WidePoint NFI CA of Issuance of Certificate

For id-orc-nfissp-medium, id-orc-nfissp-mediumhardware, id-orc-nfissp-pivi-contentSigning, id-orc-nfissp-mediumDevice, and id-orc-nfissp-mediumDeviceHardware, if the applicant provided an email address, the WidePoint NFI PKI sends the notification message via email. If no email address was provided, the WidePoint NFI PKI sends the notification to the U.S. postal address provided. The notification informs the applicant of the creation of a certificate, states a URL for use by the applicant for retrieving the certificate, contains a unique serial number, and informs the Subscriber if the private key has been escrowed. The notification also obligates the Subscriber to:

- Accurately represent themselves in all communications with the WidePoint NFI PKI.
- Protect the private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements, and local procedures.
- Notify the WidePoint NFI PKI, in a timely manner, of the suspicion that his or her private key(s) is compromised or lost. Such notification is through mechanisms consistent with this CPS.
- Abide by all the terms, conditions, and restrictions levied upon the use of his or her private key(s) and certificate(s).

For id-orc-nfissp-pivi-hardware and id-orc-nfissp-pivi-cardAuth, issuance occurs in the presence of the Applicant at the time of in-person activation. Thus, notification occurs during issuance.

For a certificate asserting id-orc-nfissp-medium or id-orc-nfissp-mediumHardware which is to be issued on a mobile device (but not a device certificate), a WidePoint NFI CA sends notification of the issuance to the Applicant via the PIVotalID DCEW. This notification includes a link to retrieve the certificate. When retrieved, the certificate is placed in the keystore of the device.

4.4 Certificate Acceptance

A condition to issuing a WidePoint NFI PKI Certificate is that the Subscriber will indicate acceptance or rejection of the WidePoint NFI PKI Certificate to WidePoint and acknowledge the Subscriber obligations. By accepting the WidePoint NFI PKI Certificate, the Subscriber is warranting that all information and representations made by the Subscriber that are included in the WidePoint NFI PKI Certificate are true.

4.4.1 Conduct Constituting Certificate Acceptance

Subscriber signature (wet or digital) on certificate application and lack of objection to published certificate constitutes certificate acceptance. The Subscriber signature is collected before the WidePoint NFI CA allows a Subscriber to make effective use of its private key.

For id-orc-nfissp-pivi-hardware, and id-orc-nfissp-pivi-cardAuth, during card activation, the Subscriber explicitly agrees to Subscriber Obligations and accepts delivery of the card and certificates hosted on the card.

4.4.2 Publication of the Certificate by the WidePoint NFI CA

The WidePoint NFI CA and Subscriber digital signature and encryption certificates are published to the appropriate repositories. The WidePoint NFI CA maintains a publicly accessible repository that is available to Subscribers and relying parties that contains:

- A listing of all current signature and encryption certificates signed by the WidePoint NFI CA
- A current and accurate CRL for all Certificate Authorities of the WidePoint NFI CA
- A copy or link to the current WidePoint NFI CP
- An abridged version of this approved CPS, which will include, at a minimum, the sections itemized below and all obligations and requirements levied on entities external to the WidePoint NFI CA
- Section 1.5.2, WidePoint NFI CA Contact Information
- Section 3.2, Initial Identity Validation
- Section 4.9, Certificate Revocation and Suspension
- Section 1.5, Certificate Policy Administration
- Any additional policy, waiver, or practice information that is supplemental to the WidePoint NFI CP or this CPS

The repository information is located at: https://www.orc.com/NFI .

4.4.3 Notification of Certificate Issuance by the WidePoint NFI CA to Other Entities

The WidePoint NFI will notify the FPKIPA at least two weeks prior to the issuance of a new CA certificate upon or issuance of new inter-organizational CA cross-certificates. In addition, all new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the CA certificate issuance will be provided to the FPKIPA within 24 hours following issuance.

The method for notification is included in the MOA between the Widepoint NFI PKI and the FBCA. The notification asserts that the new CA cross-certification does not introduce multiple paths to a CA already participating under this Certificate Policy.

4.5 Key Pair and Certificate Usage

The WidePoint NFI PKI certifies keys for use in signing or encrypting, but not both. The use of a specific key is determined by the key usage extension. The key usage extension is included in all certificates and is always marked critical in order to limit the use of a public key certificate for its intended purpose, as stipulated in the X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards.

WidePoint NFI PKI certificates asserting id-orc-nfissp-pivi-hardware include a critical keyusage extension, asserting only the digitalSignature value.

4.5.1 Subscriber Private Key and Certificate Usage

As part of the process of certificate acceptance, Subscribers agree to a set of obligations, defined elsewhere in this CPS, which address key and certificate usage. As stated in the Subscriber agreement, failure to comply with all obligations on usage may result in immediate revocation of all related credentials, as well as appropriate legal actions.

4.5.2 Relying Party Public key and Certificate Usage

This CPS governs the use of, and reliance on WidePoint NFI PKI Certificates.

The WidePoint NFI PKI publicly posts a summary of this CPS on the WidePoint website (http://www.orc.com/NFI) to provide the relying party information regarding the expectation of the WidePoint NFI PKI systems. When accepting a certificate issued under this CPS, a relying party accepts the following obligations:

- To 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
- To ensure that the certificate is being used for an appropriate approved purpose
- To check for certificate revocation prior to reliance
- To use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension)
- To verify the digital signature of the WidePoint NFI CA that issued the certificate being relied upon as stipulated in the WidePoint NFI CP
- To acknowledge all warranty and liability limitations
- To 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
- To abide by all the terms, conditions and restrictions levied upon the use of the issued private key(s) and certificate(s) as stipulated in the WidePoint NFI CP

Data format changes associated with application upgrades may invalidate digital signatures and will be avoided.

Relying parties that do not abide by these obligations assume all risks associated with the certificates upon which they are relying.

4.6 Certificate Renewal

This section applies only to id-orc-nfissp-medium, id-orc-nfissp-mediumhardware, id-orc-nfissp-mediumDevice, and id-orc-nfissp-mediumDeviceHardware.

4.6.1 Circumstance for Certificate Renewal

The WidePoint NFI PKI accepts WidePoint NFI PKI Certificate renewal requests within 90 days from the scheduled end of the operational period (expiration date) of the WidePoint NFI PKI Certificate, provided the WidePoint NFI PKI Certificate is not revoked, suspended, or expired. <REDACTED>

Subscribers are notified via automated email, 30 days prior to expiration and again 15 days prior to expiration, that their Subscriber certificates about to expire.

4.6.2 Who May Request Renewal

The WidePoint NFI PKI accepts WidePoint NFI PKI Certificate renewal requests from their Subscribers.

4.6.3 Processing Certificate Renewal Requests

To renew a certificate, as described in the WidePoint NFI CP, the Subscriber obtains a new certificate based on an existing key pair. The WidePoint NFI PKI authenticates the Subscriber's renewal request using the Subscriber's current certificate for authentication in the renewal process. In the event that subject information has changed (and/or the key pair is required to be changed for any reason), the WidePoint NFI PKI requires the Subscriber to request a new WidePoint NFI PKI Certificate. The old certificate (as a result of an update action) may or may not be revoked, but is not further re-keyed, renewed, or updated. A certificate that is not renewed by the end of the operation period reflects an expired status.

Device Subscribers (PKI Sponsors) are required to revalidate their identity and any equipment authorizations and/or attributes (if any are to be included in the certificate). The Subscriber is required to present a currently valid certificate in order to renew a certificate. End-users are required to renew their certificates through a web-based electronic form.

- Certificates asserting id-orc-nfissp-medium or id-orc-nfissp-mediumDevice may be renewed or updated on the basis of electronically authenticated Subscriber requests two times. Every 9 years, in-person authentication is required.
- Certificates asserting id-orc-nfissp-mediumhardware or id-orc-nfissp-mediumDeviceHardware may be renewed or updated on the basis of electronically authenticated Subscriber requests only one time. Every 6 years, in-person authentication is required.

Subscriber certificates issued by a WidePoint NFI CA have a maximum validity period of 3 years. Prior to the expiration of these certificates, identity and encryption certificate Subscribers may request a new certificate, which may be done by electronically submitting their existing certificates.

During the renewal process, the user must present his or her current identity certificate during a TLS client authentication to the WidePoint NFI CA. The WidePoint NFI CA validates the

authenticity of the certificate being presented by verifying that the certificate was issued by the WidePoint NFI CA in question and mapping the subject name in the certificate to its corresponding certificate in the database. This process verifies that the Subscriber is eligible for renewal on the basis of the Subscriber's existing certificate, as stipulated above. If the Subscriber is not eligible for renewal on the basis of the Subscriber's existing certificate, the WidePoint NFI PKI redirects the Subscriber to the in-person registration process. The forms to accomplish this process are controlled by access control lists on a secure web server that binds to the corresponding users with certificates in the repository. Access control to the renewal forms is based on comparing the certificate with the Distinguished Name of the Subscriber (based on an X.509 certificate-based authentication) against the certificate with DN in the directory.

In cases where a Subscriber's organization (including WidePoint NFI PKI Sponsors) has required authorizations to be included in a WidePoint NFI PKI certificate, the person responsible for that organization's WidePoint NFI PKI agreement will notify a WidePoint NFI PKI RA of the withdrawal of authorizations, via digitally signed email using a medium assurance hardware certificate. The WidePoint NFI PKI RA verifies the signature of the Subscriber's organization.

4.6.4 Notification of New Certificate Issuance to Subscriber

Upon successful completion of the Subscriber identification and authentication process in accordance with the GSA - WidePoint NFI PKI MOA, WidePoint creates the requested WidePoint NFI PKI Certificate, notifies the applicant thereof, and makes the WidePoint NFI PKI Certificate available to the applicant. If the applicant provided an email address, the WidePoint NFI PKI sends the notification message via email. If no email address was provided, the WidePoint NFI PKI sends the notification to the U.S. postal address provided.

The notification informs the Applicant of the creation of a certificate, states a URL for use by the applicant for retrieving the certificate, contains a unique serial number, and reaffirms the Subscriber's responsibilities as explained in the application process.

Upon issuance of a WidePoint NFI PKI Certificate, the WidePoint NFI PKI warrants as stated in Section 4.3.1, "CA Actions During Certificate Issuance."

The WidePoint NFI CAs are configured to establish client authenticated TLS sessions and to recognize RAs as legitimate issuers via certificate authentication. WidePoint NFI PKI RAs using WidePoint NFI CA issued medium hardware assurance certificates, and recognized by the CA, are required to initiate the SSL session with the WidePoint NFI CA to begin the issuance process. Upon successful authentication, the RA searches the CA database for the appropriate certificate request.

The WidePoint NFI PKI RA issues certificates upon receipt of the WidePoint NFI PKI RA digitally signed email only after verifying that the applicant's subject DN (provided in the RAs email) matches the subject DN in the WidePoint NFI CA database. The WidePoint NFI PKI RA archives the emails signed by WidePoint NFI PKI LRAs when issued certificates are published and issuance transactions automatically logged.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

For all other WidePoint NFI CAs operating under this WidePoint NFI CPS, failure to object to the renewal of the certificate or its contents constitutes acceptance of the certificate.

The Subscriber is in possession and control of the private key from time of generation or benign transfer. The WidePoint NFI CAs authenticate the Subscriber with a Proof of Possession (POP) test when requesting and retrieving a certificate by requiring the Subscriber to perform a private key operation and verifying that the public key presented by the Subscriber matches the private key. The WidePoint NFI PKI supports multiple enrollment protocols which support POP including: KEYGEN/SPAC, CRMF/CMMF, PKCS #10 and CMC.

<REDACTED>

In all cases, WidePoint NFI PKI RAs may request additional information or verification from a WidePoint NFI PKI RA or LRA if deemed necessary by the WidePoint NFI PKI RA to confirm the requestor's identity.

4.6.6 Publication of the Renewal Certificate by the WidePoint NFI CA

Publication of the renewed WidePoint NFI CA certificate will be in accordance with Section 4.4.2.

4.6.7 Notification of Certificate Issuance by the WidePoint NFI CA to Other Entities

WidePoint NFI CAs will provide notification of cross-certificate issuance to other inter-organizational entities in accordance with the notification processes specified in Section 4.4.3.

4.7 Certificate Re-Key

WidePoint NFI PKI Certificate re-keying (signing and encryption) is accomplished through the limitation on certificate renewal, see Section 3.3, "Identification and Authentication for Re-key ". The minimum requirement for all WidePoint NFI PKI certificate re-keying, with the exception of WidePoint NFI CA certificates, is once every 9 years from the time of initial registration (i.e., after two 3-year renewals). WidePoint NFI PKI Subscribers will identify themselves for the purpose of re-keying through use of their current signature key, except that identity will be established through initial registration process described in Section 3.

After certificate re-key and issuance of new certificate, the old certificate will be revoked and placed on the next CRL. The old certificate will not be further re-keyed, renewed, or modified.

4.7.1 Circumstance for Certificate Re-key

A certificate may be re-keyed when it can no longer be renewed.

A revoked WidePoint NFI PKI certificate will not be re-keyed.

Requirements for WidePoint NFI CA re-key are described in Section 5.6.

4.7.2 Who May Request Certification of a New Public Key

<REDACTED>

Subscribers with a currently valid certificate may request certification of a new public key. For id-orc-nfissp-pivi-hardware and id-orc-nfissp-pivi-cardAuth, a successful biometric 1:1 match of the applicant against the biometrics collected, as stipulated in Section 3.2.3.1 is required. This biometric 1:1 match must be conducted in the presence of a trusted agent of the issuer.

4.7.3 Processing Certificate Re-keying Requests

The re-key process will be in accordance with the certificate issuance process described in Section 4.3, "Certificate Issuance." Identity validation will be in accordance with Section 3.3, "Identification and Authentication for Re-key ."

4.7.4 Notification of New Certificate Issuance to Subscriber

WidePoint NFI CAs will notify Subscribers of new WidePoint NFI PKI certificate issuance in accordance with the notification processes specified in Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Conduct constituting acceptance of a re-keyed certificate will be in accordance with the processes specified in Section 4.4.1.

4.7.6 Publication of the Re-keyed Certificate by the WidePoint NFI CA

Subscriber certificates are published to a repository at the time of issuance, including re-keyed certificates, and remain accessible from the repository following Subscriber acceptance.

4.7.7 Notification of Certificate Issuance by the WidePoint NFI CA to Other Entities

<REDACTED>.

4.8 Certificate Modification

Updating a certificate means creating a new certificate that has the same or a different key, a different serial number, and differs in one or more other fields, from the old certificate. For example, the WidePoint NFI PKI may choose to update a certificate of a Subscriber who gains an authorization. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or updated.

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

4.8.1 Circumstance for Certificate Modification

<REDACTED>

A WidePoint NFI PKI certificate may be modified if some of the information other than the DN, such as the email address or authorizations, has changed.

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

4.8.2 Who May Request Certificate Modification

The Subscriber or WidePoint NFI PKI RA may request the modification of a Subscriber certificate. The WidePoint NFI PKI RA will validate any changes in the Subscriber authorizations reflected in the certificate.

4.8.3 Processing Certificate Modification Requests

The certificate modification process will be in accordance with the certificate issuance process described in Section 4.3, "Certificate Issuance." Identity validation will be in accordance with this CPS. In addition, the WidePoint NFI CA or RA validates any changes in the Subscriber authorizations reflected in the certificate. Proof of all subject information changes must be provided to the WidePoint NFI PKI RA or other designated agent and verified before the modified certificate is issued. Verification may occur via digitally signed email or written verification from the Subscriber that the information has changed.

4.8.4 Notification of New Certificate Issuance to Subscriber

WidePoint NFI CAs will notify Subscribers of new certificate issuance in accordance with the notification processes specified in Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Conduct constituting acceptance of a certificate will be in accordance with the processes specified in Section 4.4.1.

4.8.6 Publication of the Modified Certificate by the WidePoint NFI CA

No stipulation regarding publication of Subscriber certificates, except as noted in Section 4.4.2.

4.8.7 Notification of Certificate Issuance by the WidePoint NFI CA to Other Entities

Notification of certificate issuance is performed in accordance with the Section 4.4.3.

4.9 Certificate Revocation and Suspension

WidePoint NFI CAs will publish CRLs and provide certificate status information via the Online Certificate Status Protocol (OCSP) for all revoked and suspended certificates. To the extent practical, the contents of changes in status will be checked before posting to ensure that all information is correct.

The individual making the request will either digitally sign requests for certificate revocation, or the individual will present the request in person to a WidePoint NFI PKI RA or LRA.

WidePoint NFI PKI code signer certificates, which are not revoked when the PKI Sponsor departs or is no longer with the organization, must be assigned a new WidePoint NFI PKI PKI Sponsor. WidePoint NFI PKI code signing certificates suspected of having been used to sign unapproved code (knowingly or not) may be revoked by a WidePoint NFI PKI RA.

The WidePoint NFI will notify the FPKIPA at least two weeks prior to the revocation of a CA certificate, whenever possible. For emergency revocation, the WidePoint NFI will follow the notification procedures in Section 5.7.

4.9.1 Circumstances for Revocation

A certificate will be revoked when the binding between the subject and the subject's public key defined within a certificate is no longer considered valid. There are three circumstances under which certificates issued by the WidePoint NFI CA will be revoked:

- The first circumstance is when the WidePoint NFI PKI Policy Authority requests a WidePoint NFI PKI-issued certificate be revoked. This will be the normal mechanism for revocation in cases where the WidePoint NFI PKI Policy Authority determines that a WidePoint NFI CA does not meet the policy requirements or certification of the WidePoint NFI CA is no longer in the best interests of WidePoint.

- The second circumstance is when the WidePoint NFI PKI receives an authenticated request from a previously designated official of the WidePoint NFI PKI responsible for the WidePoint NFI CA.

- The third circumstance is when WidePoint NFI PKI Operational personnel determine that an emergency has occurred that may impact the integrity of the certificates issued by the WidePoint NFI CA. Under such circumstances, the following individuals may authorize immediate certificate revocation: WidePoint Chief Security Officer (CSO) or other personnel as designated by the CSO.

The WidePoint NFI PKI Policy Authority will meet as soon as practical to review the emergency revocation.

Whenever any of the circumstances herein occur, the associated certificate will be revoked and placed on the CRL. In addition, if it is determined, subsequent to issuance of new certificates, that a private key used to sign requests for one or more additional certificates may have been compromised at the time the requests for additional certificates were made, all certificates authorized by directly or indirectly chaining back to that compromised key will be revoked. Certificates will remain on the CRL until they expire. They will be removed after they expire, but must at least appear in one CRL.

A Subscriber, or a Sponsoring Organization (where applicable), is responsible for promptly requesting revocation of a WidePoint NFI PKI certificate for the following scenarios:

- When the private key, or the media holding the private key, associated with the WidePoint NFI PKI Certificate is, or is suspected of having been, compromised.

- When the individual named as a Business Representative no longer represents, or is no longer affiliated with, the Sponsoring Organization.

- If the WidePoint NFI PKI learns, or reasonably suspects, that the Subscriber's private key has been compromised or the Subscriber has failed to meet their responsibilities.

- If WidePoint determines that the WidePoint NFI PKI Certificate was not properly issued in accordance with this CPS.

- If the certificate holder requests that the certificate be revoked.

- If the certificate holder can be shown to have violated the Subscriber obligations, including payment of any required fees.

- If the certificate holder is no longer authorized to hold the certificate (e.g., termination of employment, change in responsibilities, etc.).

- If the information in the certificate is no longer accurate so that identifying information needs to be changed (e.g., change of name, privilege attributes asserted in the Subscriber's certificate are reduced, etc.).
- The Subscriber's employer or organization requests revocation.
- The certificate was obtained by fraud or mistake.
- The certificate was not correctly requested, issued or accepted.
- The certificate contains incorrect information, is defective or creates a possibility of incorrect reliance or usage.
- Certificate private key compromise is suspected
- The certificate holder fails to make a payment or other contractual obligations related to the certificate.

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

The WidePoint NFI PKI provides for the revocation of certificates when requested, at any time for any reason.

4.9.2 Who Can Request Revocation

A Subscriber may request revocation of his/her/its WidePoint NFI PKI Certificate at any time for any reason. A Sponsoring Organization may request revocation of an NFI Certificate issued to its Business Representative at any time for any reason.

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

4.9.3 Procedure for Revocation Request

A WidePoint NFI PKI certificate revocation request should be promptly communicated directly to a WidePoint NFI PKI RA or LRA who is authorized to accept such notices on behalf of the WidePoint NFI CA.

If the Subscriber is making the revocation request for their identity certificate, and is in possession of their private identity key associated with the certificate, the Subscriber may notify the WidePoint NFI PKI via digitally-signed email to revoke his or her own certificate at any time. If a Subscriber revokes their private identity key, but continues to hold a key management certificate, then they must either submit a request for a new identity certificate or a request to revoke their key management certificate(s). If the WidePoint NFI PKI does not receive such a request within 30 days, the Subscriber's key management certificate(s) will be administratively revoked.

In the case of a Subscriber's key management certificate or if the Subscriber is no longer in possession of the private key, or an entity other than the Subscriber is making the revocation request, this request may be communicated via an online form, digitally signed email, in person to a WidePoint NFI PKI RA/LRA, or via U.S. postal mail. In the case of a digitally signed email

from the Subscriber, the signature will be generated using the Subscriber's identity certificate. When revoking a Subscriber's key management certificate, the WidePoint NFI PKI RA will verify that the Subscriber's identity certificate dnQualifier is consistent with the dnQualifier of the Subscriber's key management certificate.

All revocation requests are verified prior to certificate revocation. If the Subscriber makes the request and has the private key (as determined by a proof of possession test), then the certificate is revoked immediately.

If the request comes via a digitally signed email message (signed with a certificate at least of the same assurance level as the certificate to be revoked) sent from the WidePoint NFI PKI or an authorized Sponsoring Organization representative, validation of the email signature is considered adequate and the certificate is revoked.

If the request comes from an in person visit, identity credentials are required (at least to the same assurance level as the certificate to be revoked) from the individual making the request and verified prior to revoking the certificate. If the request is made via unsigned email, then the WidePoint NFI PKI contacts the requesting party having confirmed authorization to act upon said party's request when authenticated.

If a LRA is making the request, the reason for the revocation request is documented. The reason may be sent to a WidePoint NFI PKI RA via a digitally signed email message for revocation, who investigates the request, documents the reason for the revocation request, and archives it.

The WidePoint NFI PKI will revoke the certificate by placing its serial number and identifying information on a CRL. The WidePoint NFI PKI will also remove the certificate from any repositories containing that certificate.

When appropriate, the Subscriber is notified of the revocation request, reason for the request, and status of the request. If appropriate, the Subscriber is provided information on obtaining a new certificate and a list of all certificates issued.

If WidePoint is choosing to revoke a certificate because of sufficient evidence of noncompliance with this CPS, a WidePoint NFI PKI RA documents the reason for certificate revocation and, if appropriate, notifies the Subscriber of the revocation.

Subscribers leaving the organizations that sponsored their participation in the WidePoint NFI PKI will surrender to their organization's PKI point of contact (POC) (through any accountable mechanism) all cryptographic hardware tokens that were issued, under the sponsoring organization, prior to leaving the organization. The WidePoint NFI PKI PoC will zero (refer to Section 6.2.7) or destroy the token promptly upon surrender and will protect the token from malicious use from the time of surrender. The procedure(s) used to zero a token will depend on the type of applications and hardware used to access or create the token. If the Subscriber leaves an organization and the hardware tokens cannot be obtained, then all certificates associated with the unretrieved tokens will be immediately revoked. In all cases, whether software or hardware tokens are involved, the organization will promptly notify a WidePoint NFI PKI RA to revoke the certificate and attest to the disposition of the token, via a digitally signed email.

If the Government provided WidePoint NFI PKI LRA functions, or if the WidePoint NFI PKI has delegated revocation functions to subcontractor WidePoint NFI PKI LRAs, all information is transmitted via digitally-signed email between the WidePoint NFI PKI and/or subcontractors and/or government WidePoint NFI PKI LRAs.

4.9.4 Revocation Request Grace Period

Certificates are revoked upon request as soon as the need can be verified. There is no grace period. The Subscriber, or sponsoring organization, must request revocation from the WidePoint NFI PKI as soon as the need for revocation has been determined.

4.9.5 Time Within Which WidePoint NFI CA Must Process the Revocation Request

WidePoint NFI CAs will revoke certificates within 8 business hours of receipt of a proper revocation request. Revocation requests are processed before the next CRL is published, excepting those requests validated within 2 hours of CRL issuance. Revocation requests validated within 2 hours of CRL issuance are processed before the following CRL is published.

4.9.6 Revocation Checking Requirements for Relying Parties

No stipulation.

4.9.7 CRL Issuance Frequency

The WidePoint NFI CAs issue CRLs every 12 hours, at a minimum, with a validity period of 48 hours. New WidePoint NFI PKI CRLs are issued twice per day even if there are no changes or updates to be made. When a revocation request is granted for the reason of key compromise, the revocation information will be posted on the next WidePoint NFI PKI CRL, except that, if the revocation request is made within 2 hours of the next scheduled CRL, the revocation information may be posted on the following WidePoint NFI PKI CRL.

All superseded WidePoint NFI PKI CRLs are removed from the repository upon posting of the latest CRL.

When a WidePoint NFI CA certificate or Subscriber certificate is revoked because of compromise, or suspected compromise, of a private key, a WidePoint NFI PKI CRL is issued immediately as stipulated in Section 4.9.12.

WidePoint NFI PKI CRLs may be obtained from: https://crl-server.orc.com/CRLs/

4.9.8 Maximum Latency for WidePoint NFI PKI CRLs

The WidePoint NFI PKI CRL will be posted upon generation, but within no more than 4 hours after generation. The system is configured to publish to a public repository upon issuance of the WidePoint NFI PKI CRL. In the event of publishing failure, automated monitoring scripts verify the current WidePoint NFI PKI CRL on the WidePoint NFI CA versus our publicly available WidePoint NFI PKI CRLs. If the WidePoint NFI PKI CRL on the WidePoint NFI CA is more recently published than the publicly available WidePoint NFI PKI CRL, the scripts pull the newer WidePoint NFI PKI CRL and replace the publicly available WidePoint NFI PKI CRL with the more recent WidePoint NFI PKI CRL.

4.9.9 On-line Revocation/ Status Checking Availability

The WidePoint NFI PKI validates online and near-real-time the status (Valid, Invalid or Suspended) and signature of the WidePoint NFI PKI Certificate indicated in a WidePoint NFI PKI Certificate Validation Request message. The WidePoint NFI CA returns in the Certificate

Status Response message a signed message. This functionality is integrated with the GSA-approved Certificate Arbitrator Module (CAM) using the OCSP.

The WidePoint NFI PKI WAN OCSP Responder (CSP) is located at: http://NFI2.eva.orc.com.

The WidePoint NFI PKI supports online status checking via OCSP [RFC 6960] for end entity certificates issued under all subject certificate policies defined in this CPS. Status information maintained by the WidePoint NFI PKI OCSP server is updated and available to relying parties within 6 hours.

4.9.10 On-line Revocation Checking Requirements

Each relying party will validate every WidePoint NFI PKI Certificate it receives in connection with a transaction. Any self-signed WidePoint NFI PKI responder used for verifying certificates asserting a policy object identifier from this CPS is required to meet the certificate profile stipulated in the X.509 Certificate and CRL Extensions Profile and ensure that:

- Certificates indicated as being valid have a chain of valid certificates (valid as defined by [X.509]) linking back to a "trusted Root CA."

- Each certificate in the certificate chain used to validate the certificate whose status is being requested is checked for revocation, such that the Relying Party need not check more than one responder to validate a Subscriber certificate.

- Certificate status responses provide authentication and integrity services commensurate with the assurance level of the certificate being verified.

- It is made clear in the certificate status response the attributes (other than certificate subject name (e.g., citizenship, clearance authorizations, etc.)) being authenticated by the responder.

- Accurate and up-to-date WidePoint NFI PKI CRLs, from the WidePoint NFI CAs, are used to provide the revocation status .

- Revocation status responses provide authentication and integrity services commensurate with the assurance level of the certificate being checked.

The WidePoint NFI PKI disclaims any liability for loss due to use of any validation information relied upon by any party that does not comply with this stipulation, in accordance with this CPS.

4.9.11 Other Forms of Revocation Advertisements Available

No other forms have been implemented.

4.9.12 Special Requirements Related To Key Compromise

If a WidePoint NFI PKI certificate is revoked because of suspicion of private key compromise, then the WidePoint NFI PKI issues new WidePoint NFI PKI CRLs with date of compromise and notifies, through website posting, any relying parties which download the WidePoint NFI PKI CRL that a certificate has been revoked because of key compromise, and the date that the suspected compromise occurred.

If the compromised certificate was a WidePoint NFI PKI RA certificate, then the WidePoint NFI PKI RA revalidates any Subscriber certificates validated after the date of the suspected compromise, and revokes any certificates not revalidated.

4.9.13 Circumstances for Suspension

Suspension is not implemented.

4.9.14 Who Can Request Suspension

Suspension is not implemented.

4.9.15 Procedure for Suspension Request

Suspension is not implemented.

4.9.16 Limits on Suspension Period

Suspension is not implemented.

4.10 Certificate Status Services

The WidePoint NFI PKI CSS operating under this CPS uses OCSP and CRLs for the distribution of certificate status information, as detailed in the following subsections.

4.10.1 Operational Characteristics

The WidePoint NFI PKI CSS provides OCSP responses to Subscribers and is responsible for:

- Providing certificate revocation status and/or complete certification path validation (including revocation checking) to the Relying Parties upon request.
- Ensuring that the status and validation responses contain authentication and integrity services commensurate with the assurance level of the certificate being checked.

A WidePoint NFI CAA administers the WidePoint NFI PKI CSS.

4.10.2 Service Availability

WidePoint NFI PKI Certificate Status Servers maintain service availability by striving to operate at 99% up-time annually.

4.10.3 Optional Features

WidePoint NFI PKI Certificate Status Servers do not currently operate any optional features beyond those specified by the CP, if any.

4.11 End of Subscription

See 4.9.3, “Procedure for Revocation Request”.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

<REDACTED>Under no circumstances is a Subscriber signature key allowed to be held in trust by a third party.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

The WidePoint NFI PKI does not support key escrow and recovery using key encapsulation techniques.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

Unauthorized use of WidePoint NFI CA, RA, CMS, DCEW and CSS equipment is forbidden. Physical security controls are implemented that protect the hardware and software from unauthorized use. Cryptographic modules are protected against theft, loss, and unauthorized use through multiple party management.

<REDACTED>.

5.1.1 Site Location and Construction

<REDACTED>.

5.1.2 Physical Access

<REDACTED>.

5.1.2.1 Physical Access for CA Equipment

<REDACTED>.

5.1.2.2 Physical Access for RA Equipment

<REDACTED>.

5.1.2.3 Physical Access for CSS Equipment

<REDACTED>.

5.1.2.4 Physical Access for CMS Equipment

<REDACTED>.

5.1.3 Power and Air Conditioning

<REDACTED>.

5.1.4 Water Exposure

<REDACTED>.

5.1.5 Fire Prevention and Protection

The WidePoint NFI PKI facility complies with all applicable national, state, and local fire regulations for a commercial office building. Fire prevention devices are enabled to eliminate or reduce fire and smoke damage to the WidePoint NFI CA, RA and CSS equipment. Backup materials and documentation are located in fire resistant storage devices to reduce or eliminate damage to such materials.

5.1.6 Media Storage

<REDACTED>.

5.1.7 Waste Disposal

<REDACTED>

5.1.8 Off-Site Backup

5.2 <REDACTED>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 people selected to fill these roles have proven to be diligent and trustworthy as described in the next section. The functions performed in these roles form the basis of trust in the entire PKI. WidePoint NFI PKI uses two approaches to increase the likelihood that these roles can be successfully carried out. The first approach is to ensure that the persons filling the roles are trustworthy and properly trained. The second is to distribute the functions of the role among several people, so that any malicious activity requires collusion.

<REDACTED>.

5.2.2 Number of Persons Required Per Task

<REDACTED>.

5.2.3 Identification and Authentication for Each Role

<REDACTED>.

5.2.4 Separation of Roles

WidePoint NFI PKI implements commercially reasonable practices that ensure that one person acting alone cannot circumvent safeguards, as described in Section 5.2.2. To increase the likelihood that these roles can be successfully carried out, the functions of WidePoint NFI CAA, SA and RA are distributed among more than one person, so that any malicious activity would require collusion.

Under no circumstances will the incumbent of these roles perform their own auditing function. No individual is assigned more than one trusted role.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

<REDACTED>.

5.3.2 Background Check Procedures

WidePoint NFI CAAs, RAs, SAs, and Security Auditors will either hold a US security clearance or go through a thorough background check covering the past 7 years performed by a qualified investigator <REDACTED>.

5.3.3 Training Requirements

<REDACTED>.

5.3.4 Retraining Frequency and Requirements

<REDACTED>.

5.3.5 Job Rotation Frequency and Sequence

<REDACTED>.

5.3.6 Sanctions for Unauthorized Actions

<REDACTED>.

5.3.7 Independent Contractor Requirements

<REDACTED>.

5.3.8 Documentation Supplied to Personnel

<REDACTED>.

5.4 Audit Logging Procedures

<REDACTED>

5.4.1 Types of Events Recorded

<REDACTED>

5.4.2 Frequency of Processing Log

<REDACTED>

5.4.3 Retention of Audit Log

<REDACTED>.

5.4.4 Protection of Audit Log

<REDACTED>.

5.4.5 Audit Log Backup Procedures

<REDACTED>.

5.4.6 Audit Collection System (Internal vs. External)

<REDACTED>.

5.4.7 Notification to Event-Causing Subject

<REDACTED>.

5.4.8 Vulnerability Assessment

<REDACTED>.

5.5 Records Archival

5.5.1 Types of Events Archived

<REDACTED>

5.5.2 Retention Period for Archive

<REDACTED>.

5.5.3 Protection of Archive

<REDACTED>.

5.5.4 Archive Backup Procedures

<REDACTED>.

5.5.5 Requirements for Time-Stamping of Records

<REDACTED>.

5.5.6 Archive Collection System

<REDACTED>.

5.5.7 Procedures to Obtain and Verify Archive Information

<REDACTED>.

5.6 Key Changeover

<REDACTED>.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

<REDACTED>.

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

<REDACTED>.

5.7.3 Entity (CA) Private Key Compromise Procedures

<REDACTED>.

5.7.4 Business Continuity Capabilities after a Disaster

<REDACTED>.

5.7.5 Customer Service Center

<REDACTED>.

5.8 Authority Termination

<REDACTED>.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

<REDACTED>.

6.1.1.2 Subscriber Key Pair Generation

<REDACTED>.

6.1.2 Private Key Delivery to Subscriber

The WidePoint NFI PKI Subscriber's private key is generated directly on the Subscriber's token, or in a key generator that benignly transfers the key to the Subscriber's token. The Subscriber is in possession and control of the private key from the time of generation or benign transfer.

6.1.3 Public Key Delivery to Certificate Issuer

<REDACTED>

Public keys are delivered to the certificate issuer in a PKCS#10 or Certificate Request Message Format (CRMF) certificate request.

6.1.4 CA Public Key Delivery to Relying Parties

The WidePoint NFI PKI supports delivery of WidePoint NFI CA and trust anchor public keys via a web interface to a protected server using TLS. The public key is stored such that it is unalterable and not subject to substitution. <REDACTED>.

6.1.5 Key Sizes

All FIPS-approved signature algorithms will be considered acceptable; additional restrictions on key sizes are detailed below.

For WidePoint NFI CAs that generate certificates and CRLs under this policy, all valid certificates will be signed with keys of at least 2048 bits for RSA or at least 224 bits for ECDSA. <REDACTED>.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters for signature algorithms defined in the Digital Signature Standard (DSS) are generated in accordance with FIPS 186. Parameter quality checking (including primality testing for prime numbers) is performed in accordance with FIPS 186; additional tests may be specified by the WidePoint DAA. <REDACTED>.

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

The WidePoint NFI PKI certifies keys for use in signing or encrypting, but not both. The use of a specific key is determined by the key usage extension. The key usage extension is included in all

certificates and is always marked critical in order to limit the use of public key certificate for its intended purpose, as stipulated in the X.509 Certificate and CRL Extensions Profile. WidePoint NFI Device certificates do not assert the *nonRepudiation* bit. Nor does any WidePoint NFI CA issue certificates that assert *dataEncipherment*, *encipherOnly*, or *decipherOnly*. WidePoint NFI PKI contentSigning certificates are required to include an extended key usage of *id-PIV-content-signing*, in accordance with [CCP-PROF].

Certificate type	**Key usage assertion bit**
id-orc-nfissp-pivi-hardware	*digitalSignature* (only)
id-orc-nfissp-pivi-cardAuth	*digitalSignature* (only)
RSA public keys for key transport	*keyEncipherment*
WidePoint NFI CA certificate public key for verifying other certificates	*keyCertSign*
WidePoint NFI CA certificate public key for verifying CRLs	*cRLSign*
WidePoint NFI CA certificate public key for verifying OCSP responses	*digitalSignature*; and/or *nonRepudiation*
WidePoint NFI PKI Device certificates for digital signature (including authentication)	*digitalSignature*
WidePoint NFI PKI Device certificate with RSA public keys for key transport	*keyEncipherment*
WidePoint NFI PKI Device certificate for both digital signature and key management	*digitalSignature*

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 Security Requirements for Cryptographic Modules [current version of FIPS140]. Cryptographic modules are validated to the FIPS 140 Level identified in this section.

Subscribers will use cryptographic modules that have been validated to meet at least the criteria specified for FIPS 140 Level 1. FIPS 140 Level 2 must be used to receive a Medium Hardware Assurance certificate. The WidePoint NFI PKI will use FIPS 140-1 or FIPS 140-2, validated cryptographic modules that adhere, as a minimum, to the following additional requirements:

Assurance Level	CA, CMS & CSS	Subscriber	RA
Medium	Level 2 (Hardware)	Level 1	Level 2 (Hardware)
Medium Hardware	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)
PIV-I Hardware	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)
PIV-I Card Authentication	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)

Table 8: Cryptographic Module requirements

PIV-I Cards are PKI tokens that have private keys associated with certificates asserting policies mapped to PIV-I hardware or PIV-I-cardAuth. PIV-I Cards will only 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. 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 FPKIPA/FPKIMA. On an annual basis, for each PCI configuration used (as defined by the FIPS 201 Evaluation Program), one populated, representative sample PIV-I Card shall be submitted to the FIPS 201 Evaluation Program for testing.

All WidePoint NFI CA certificates are signed using a hardware cryptographic module that has been validated to meet FIPS 140-2 Level 3. WidePoint NFI CA private keys are protected by a hardware cryptographic module that are FIPS 140-2 Level 3 validated for key storage, as listed on the NIST website.

<REDACTED>.

Section 6.1.1 stipulates cryptographic module requirements for key generation.

6.2.1.1 Custodial Subscriber Key Stores

<REDACTED>.

6.2.2 Private Key (n out of m) Multi-person Control

<REDACTED>.

6.2.3 Private Key Escrow

6.2.3.1 Escrow of CA Private Signature Key

Under no circumstances is a WidePoint NFI CA signature key (used to sign certificates or CRLs) escrowed.

6.2.3.2 Escrow of CA Encryption Key

The WidePoint NFI PKI does not escrow CA encryption keys.

6.2.3.3 Escrow of Subscriber Private Signature Key

Under no circumstances will a signature key be escrowed.

6.2.3.4 Escrow of Subscriber Private Encryption Key

See section 4.12.1, "Key Escrow and Recovery Policy and Practices".

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Private Signature Key

<REDACTED>.

6.2.4.2 Backup of Subscriber Private Signature Key

Backup of private signature keys for the sole purpose of key recovery will not be made.

In the case of individual Subscriber certificates on a smart card asserting a id-nfissp-pivihardware or id-nfissp-pivicardAuth, private signing keys are generated on the smart card and are not backed up.

6.2.4.3 Backup of Subscriber Private Key Management Key

Subscribers are permitted to back-up their own private keys. Backed up Subscriber private key management keys may not be stored in plain text form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the Subscriber's cryptographic module.

6.2.4.4 Backup of CSS Private Key

<REDACTED>.

6.2.4.5 Backup of PIV-I Content Signing Key

At present, the WidePoint NFI PKI does not back-up Content Signing private signature keys. In the future, should back-up of Content Signing private keys become standard practice, the backup procedure will require multi-person control.

6.2.5 Private Key Archival

Under no circumstances is a non-repudiation signature or authentication key archived. Archival of confidentiality keys is recommended if any information encrypted with those keys is archived in its encrypted state.

<REDACTED>.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Private keys are generated by and in a cryptographic module. For the WidePoint NFI CA and CSS, the cryptographic module must be a FIPS 140-2 Level 3 module. <REDACTED>.

6.2.7 Private Key Storage on Cryptographic Module

Private keys can be stored in any form on cryptographic module as long as the keys are not accessible without authentication mechanism in compliance with FIPS 140-2.

6.2.8 Method of Activating Private Key

<REDACTED>.

6.2.9 Method of Deactivating Private Key

<REDACTED>.

6.2.10 Method of Destroying Private Key

<REDACTED>.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Archival of public keys is achieved via certificate archival.

6.3.2 Certificate Operational Periods and Key Usage Periods

<REDACTED>.

6.3.3 Restrictions on CA Private Key Usage

<REDACTED>.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

<REDACTED>.

6.4.2 Activation Data Protection

<REDACTED>.

6.4.3 Other Aspects of Activation Data

<REDACTED>.

6.5 Computer Security Controls

<REDACTED>.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Individuals filling trusted roles within the WidePoint NFI PKI facility use security management tools and procedures to ensure that the operational systems and networks adhere to the security requirements that check the integrity of the system data, software, discretionary access controls, audit profiles, firmware, and hardware to ensure secure operation.

<REDACTED>.

6.6.2 Security Management Controls

<REDACTED>.

6.6.3 Object Reuse

<REDACTED>.

6.6.4 Life Cycle Security Controls

<REDACTED>.

6.7 Network Security Controls

<REDACTED>.

6.8 Time-Stamping

The WidePoint NFI PKI provides time stamps for use in audit record generation. The WidePoint NFI PKI synchronizes internal information system clocks. <REDACTED>.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

WidePoint NFI PKI Certificates contain public keys used for authenticating the sender and receiver of an electronic message and verifying the integrity of such messages, i.e., public keys used for digital signature verification.

WidePoint NFI PKI creates and maintains certificates that conform to the ITU-T Recommendation X.509, "The Directory: Authentication Framework," June 1997.

All WidePoint NFI PKI certificates include a reference to a certificate policy object identifier for this CPS within the appropriate field, and contain the required certificate fields according to this CPS and the GSA NFI MOA.

Complete certificate profile information, including key generation methods, for WidePoint NFI PKI certificates can be found in the FPKI X.509 Certificate and CRL Extensions Profile and the applicable WidePoint CA build document.

7.1.1 Version Number(s)

WidePoint NFI PKI issues X.509 v3 NFI certificates (populate version field with integer 2).

7.1.2 Certificate Extensions

WidePoint NFI PKI certificate profiles are in accordance with the requirements of the certificate profiles described in the WidePoint NFI CP and the applicable WidePoint NFI CA build document.

Access control information may be carried in the subjectDirectoryAttributes non-critical extension. The syntax is defined in detail in [SDN702].

7.1.3 Algorithm Object Identifiers

Certificates issued by WidePoint NFI CAs may use the following OIDs for signatures.

id-dsa-with-sha1	{ iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3 }
sha-1WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }
sha256WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
id-RSASSA-PSS	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10 }
ecdsa-with-SHA1	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) 1 }
ecdsa-with-SHA224	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 1 }
ecdsa-with-SHA256	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2 }

ecdsa-with-SHA384	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }
ecdsa-with-SHA512	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4 }

The WidePoint NFI PKI does not implement RSA with PSS padding.

Certificates issued under this CP use the following OIDs to identify the algorithm associated with the subject key.

id-dsa	{ iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1 }
RsaEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }
Dhpublicnumber	{ iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1 }
id-ecPublicKey	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1 }

Where a certificate contains an elliptic curve public key, the parameters will be specified as one of the following named curves:

ansip192r1	{ iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 1 }
ansit163k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 1 }
ansit163r2	{ iso(1) identified-organization(3) certicom(132) curve(0) 15 }
ansip224r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 33 }
ansit233k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 26 }
ansit233r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 27 }
ansip256r1	{ iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7 }
ansit283k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 16 }
ansit283r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 17 }
ansip384r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 34 }
ansit409k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 36 }

ansit409r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 37 }
ansip521r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 35 }
ansit571k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 38 }
ansit571r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 39 }

7.1.4 Name Forms

Where required as set forth in Section 3.1.1, the subject and issuer fields of the base certificate will be populated with an X.500 Distinguished Name, with the attribute type as further constrained by RFC 5280.

The subject alternative name extension will be present and include a UUID name type in certificates issued under id-orc-nfissp-pivi-hardware and id-orc-nfissp-pivi-cardAuth.

7.1.5 Name Constraints

Not applicable.

7.1.6 Certificate Policy Object Identifiers

Certificates issued by the WidePoint NFI CAs assert the certificate policy object identifier appropriate to the level of assurance with which it was issued, as defined in Section 1.2, “Document Name and Identification”.

7.1.7 Usage of Policy Constraints Extension

The WidePoint NFI CAs may assert policy on constraints in CA certificates. When this extension appears, at least one of requireExplicitPolicy or inhibitPolicyMapping will be present. When present, this extension should be marked as noncritical, to support legacy applications that cannot process policyConstraints. For Subordinate CA certificates inhibitPolicyMappings, skip certs will be set to 0. For cross-certificates inhibitPolicyMappings, skip certs will be set to 1, or 2 for the Federal Bridge CA. When requireExplicitPolicy is included skip certs will be set to 0.

7.1.8 Policy Qualifiers Syntax and Semantics

The certificates issued under this CPS will not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

The WidePoint NFI PKI does not set the certificate policies extension to be critical. Relying Parties whose client software does not process this extension operate in this regard at their own risk. Processing semantics for the critical certificate policy extension used by WidePoint NFI PKI conforms to [PIV-I Profile].

7.1.10 Inhibit Any Policy Extension

The WidePoint NFI CAs may assert InhibitAnyPolicy in CA certificates. When present, this extension should be marked as noncritical, to support legacy applications that cannot process InhibitAnyPolicy. Skip Certs shall be set to 0, since certificate policies are required in the Federal PKI.

7.2 CRL Profile

WidePoint NFI PKI CRL profiles addressing the use of each extension are provided in and conform to X.509 Certificate and CRL Extensions Profile and the applicable WidePoint CA build document.

7.2.1 Version Number(s)

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

7.2.2 CRL and CRL Entry Extensions

Detailed CRL profiles covering the use of each extension are available and described in the X.509 Certificate and CRL Extensions Profile and are in accordance with the WidePoint NFI CP CRL profile. The CA supports CRL Distribution Points (CRL DP) in all EE certificates. The CRL DP is as follows:

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

In the case of subordinate CAs: http://crl-server.orc.com/CRLs/<ORC Root>.crl

7.3 OCSP Profile

OCSP requests are not required to be signed (refer to RFC6960 for detailed syntax). OCSP requests and responses contain the following formats.

Field	Expected Value
Version	V1 (0)
Requester Name	Not Required
Request List	List of certificates – generally this should be the list of two certificates: WidePoint NFI PKI certificate and end entity certificate
Signature	Not Required
Extensions	Not Required

OCSP Request Format

The following table lists which fields are populated by a WidePoint NFI PKI OCSP 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[1], thisUpdate, nextUpdate[2],
Extension	
Nonce	Will be present if nonce extension is present in the request
Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Signature	Present
Certificates	Applicable certificates issued to the OCSP Responder

OCSP Response Format

7.3.1 Version Number(s)

The WidePoint NFI PKI CSS operated under this CPS uses OCSP version 1.

7.3.2 OCSP Extensions

Critical OCSP extensions are not used.

8 Compliance Audit and Other Assessments

The WidePoint NFI PKI conducts a compliance audit, at least annually, to ensure that the requirements of this CPS are being implemented and enforced. The WidePoint NFI PKI Policy Management Authority is responsible for ensuring audits are performed for all WidePoint NFI PKI functions regardless of how or by whom the WidePoint NFI PKI components are managed and operated.

8.1 Frequency of Audit or Assessment

The WidePoint NFI PKI systems are periodically, at a minimum annually, independently audited for conformance to the appropriate policies and procedures. WidePoint operates primary and secondary (backup) secure data centers in conformance with DoD, NSA, GSA and commercial practices. As GSA requirements apply to GSA systems, and NSA/DoD guidelines apply to other systems, where there is a difference in requirements, the most restrictive guideline ("high water mark") is used.

As an alternative to a full annual compliance audit against the entire CPS, the compliance audit of the CAs and RAs may be carried out in accordance with the requirements specified in the FPKI Compliance Audit Requirements document [AUDIT].

The WidePoint NFI PKI has developed Certification, accreditation, and security assessment policies and procedures that are reviewed and updated periodically, in accordance with the certification, accreditation, and security assessment policies and procedures developed and maintained by the GSA as set forth in GSA Order CIO P 2100.1D, GSA Information Technology (IT) Security Policy and CIO IT Security Procedural Guide 06-30, Managing Enterprise Risk, dated October 16, 2007. Policies and procedures are also contained in the Certificate Practice Statements.

Security controls are reviewed annually and updated accordingly on an annual basis for the purpose of determining the extent to which controls are correctly implemented and operating, and meeting the system's security needs.

The completion of the most recent security assessment is cited in the WidePoint System Security Plan.

Subsequent to the WidePoint NFI PKI being granted Authorization to Operate (ATO), which is primarily based upon a Certification and Accreditation (C&A) review performed by an external auditor, the C&A process will be performed every three years.

8.2 Identity/ Qualifications of Assessor

The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the WidePoint NFI CA's CP and this CP. The compliance auditor must perform such compliance audits as a regular ongoing business activity. WidePoint NFI PKI contracts qualified external auditor(s) and budgets for C&A, annual audits, and any additional auditing requirements as part of each year's fiscal planning. In addition to the previous requirements, it is preferable that the auditor be a certified information system auditor (CISA) or

IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

A certified IT auditing firm (approved by the NFI PMO) audits the WidePoint NFI PKI annually, in accordance with industry best practices for compliance (e.g., FISMA). WidePoint may also be audited aperiodically by: GSA, DoD and NSA. The WidePoint NFI PKI has an independent internal department that performs continuous monitoring procedures in order to attest to the WidePoint NFI PKI's compliance with this CPS. Audit and inspection is accomplished in accordance with the NIST SP 800-53 or current industry accepted standards and practices.

8.3 Assessor's Relationship to Assessed Entity

The compliance auditor either will be a private firm that is independent from the WidePoint NFI PKI (CAs and RAs) being audited, or it will be sufficiently organizationally separated from those entities to provide an unbiased, independent evaluation. An example of the latter situation may be the Corporate Security Auditor. To insure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining the entity's CA Facility or certificate practices statement. The FPKIPA will determine whether a compliance auditor meets this requirement.

The Organization/Agency PMA is responsible for identifying and engaging a qualified auditor of organization/agency operations implementing aspects of this CP.

The WidePoint NFI PKI relies upon the combined efforts of an independent external IT auditor, which is an entity separate from WidePoint, and an internal audit capability that is sufficiently organizationally separated from those entities operating the CA, so as to provide an unbiased, independent evaluation. The WidePoint NFI PKI performs internal audits of NFI CSS, RA and LRA facilities, conducted by a WidePoint NFI PKI Corporate Security Auditor, as defined herein.

8.4 Topics Covered by Assessment

The purpose of WidePoint NFI compliance audits is to verify that the WidePoint NFI PKI and its recognized trusted roles comply with all the requirements of the current versions of the WidePoint NFI CP and this CPS, as well as any MOAs between the WidePoint NFI PKI and any other PKI. Components other tha WidePoint NFI CAs may be audited fully or by using a representative sample. If statistical sampling is used, all PKI components, PKI component managers and operators will be considered in the sample. The samples will vary on an annual basis. All aspects of the WidePoint NFI PKI operation are subject to compliance audit inspections.

8.5 Actions Taken as a Result of Deficiency

When a compliance auditor finds a discrepancy between a WidePoint NFI PKI CMA's operation and the stipulations of this CPS, the following actions will occur:

The compliance auditor will note the discrepancy

The compliance auditor will notify the parties identified in Section 8.6 of the discrepancy

The WidePoint NFI PKI will propose a remedy, including expected time for completion, to the NFI Program Office.

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

Remedies will be defined by the WidePoint NFI PKI PA and communicated to WidePoint as soon as possible to limit the risks created. The WidePoint NFI PKI WidePoint NFI PKI will determine a time for completion. The implementation of remedies will be coordinated between the WidePoint NFI PKI PA and the WidePoint NFI PKI and subsequently communicated to the appropriate authority. A special audit may be required to confirm the implementation and effectiveness of the remedy.

8.6 Communication of Results

The results of any inspection or audit will be communicated, in whole, to the WidePoint NFI PKI and to the NFI Program Office by the auditor. Required remedies will be defined and communicated to the WidePoint NFI PKI as soon as possible to limit the risks created. The implementation of remedies will be communicated to the appropriate authority. A special audit may be required to confirm the implementation and effectiveness of the remedy.

If a WidePoint NFI PKI CMA entity is found not to be in compliance with this CPS, or the policy identified in the WidePoint NFI CP, the WidePoint NFI PKI will notify the NFI PA immediately upon completion of the audit.

The WidePoint NFI PKI will annually submit an audit compliance package to the FPKIPA, prepared in accordance with the “Compliance Audit Requirements” document and include an assertion from the WidePoint NFI PA that all PKI components have been audited, including any components that may be separately managed and operated. If necessary, the results will be communicated as set forth in Section 8.5 above.

Results of the initial C&A and all subsequent C&A reviews will be made available to FBCA, to be used in determining the WidePoint NFI CA’s suitability for initial and continued performance as a cross-certified CA.

9 Other Business and Legal Matters

9.1 Fees

All fees are set in accordance with the terms of the WidePoint NFI PKI MOA. Fees are published on the WidePoint NFI PKI website or established contractually. Fees are published at http://www.orc.com/NFI and may change with a 7-day notice.

9.1.1 Certificate Issuance or Renewal Fees

A fee per validity year, unless otherwise negotiated, is levied by the WidePoint NFI PKI to issue certificates to human and device Subscribers. Likewise, a fee per each additional year, unless otherwise negotiated, is levied by the WidePoint NFI PKI to renew a WidePoint NFI PKI certificate. A fee per encryption certificate is levied for the escrowing of encryption keys.

A fee, unless otherwise negotiated, is levied by the WidePoint NFI PKI for the replacement of certificates and or tokens when the Subscriber's private key has not been compromised and there are no changes to the certificate.

Fees for tokens are separate from Certificate Issuance, Renewal, and Replacement Fees.

9.1.2 Certificate Access Fees

The WidePoint NFI PKI does not impose any certificate access fees on Subscribers with respect to its own WidePoint NFI PKI certificate(s) or the status of those certificate(s). No fee is levied by the WidePoint NFI PKI for access to information about any certificate issued by the WidePoint NFI PKI that is requested under a court order. The WidePoint NFI PKI assesses a fee from Subscribers and Relying Parties for recovering archived certificates.

9.1.3 Revocation or Status Information Access Fees

No fee is assessed for certificate validation services as set forth in the WidePoint NFI PKI MOA.

9.1.4 Fees for other Services

No fee is levied for online access to policy information. A reasonable fee to cover media reproduction and distribution costs may be levied for a physical media copy of this policy information. A consulting fee per hour is levied for certificate support required in addition to the detailed instructions delivered with the notification of Subscriber certificate issuance. This additional support includes documentation, telephone and on-site support.

9.1.5 Refund Policy

Refunds may be negotiated on a case-by-case basis.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

WidePoint NFI CA information not requiring protection is made publicly available. Public access to organizational information, as determined by the WidePoint NFI PKI and the respective organization, is provided via means determined by the WidePoint NFI PKI and the respective organization.

9.3.1 Scope of Confidential Information

WidePoint NFI CAs take steps to protect the confidentiality of any WidePoint NFI PKI entity, Relying Party, Subscriber, or other Government information provided to the Authorized WidePoint NFI PKI. These steps include vetting of personnel placed in trusted roles; protection of confidential data in transit and while at rest; physical and logical controls; archive protection; all of which are described throughout this CPS. Such information is used only for the purpose of providing WidePoint NFI CA Services and carrying out the provisions of this CPS, and are not disclosed in any manner to any person except as may be necessary for the performance of the WidePoint NFI CA Services in accordance with the this CPS and any existing MOA(s).

9.3.2 Information not within the Scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

The WidePoint NFI PKI takes steps, as required, to protect the confidentiality of any Relying Party, Subscriber, or other Government information provided to the WidePoint NFI CA. Such information is used only for the purpose of providing WidePoint NFI CA Services and carrying out the provisions of the WidePoint NFI PKI Certificate Policy, and is not disclosed in any manner to any person except as may be necessary for the performance of the WidePoint NFI CA Services in accordance with the WidePoint NFI CP.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

The WidePoint NFI PKI protects all Subscriber identifying information. All Subscriber identifying information will be maintained in accordance with applicable laws. Further, WidePoint maintains internal policy 0-0, “IA-IDM Privacy Policy”, and procedure 0-0, “Privacy Act Statement Notification”, supporting operations protecting Subscriber information.

9.4.2 Information Treated as Private

Information requested from individuals during the certificate issuance process other than that information, which is specifically included in the certificate, is withheld from release. This information may include personal information as described in Section 3.1 and is subject to the Privacy Act. All information in the WidePoint NFI PKI record (not repository) is handled as SBU, and access will be restricted to those with official needs.

Certificate private keys are considered sensitive and access will be restricted to the certificate owner, except as stipulated in the WidePoint NFI PKI. Private keys held by the WidePoint NFI PKI will be held in strictest confidence. Under no circumstances will any private key appear unencrypted outside the WidePoint NFI PKI hardware. Private keys held by the WidePoint NFI PKI will be released only to a trusted authority in accordance with this CPS, or law enforcement official, in accordance with U.S. law, the WidePoint NFI CP, and this CPS.

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

9.4.3 Information not Deemed Private

No sensitive information will be held in certificates, as certificate information is publicly available in repositories. Information not considered sensitive includes the Subscriber's name, electronic mail address, certificate public key, and certificate validity period.

9.4.4 Responsibility to Protect Private Information

The WidePoint NFI PKI will not disclose certificate-related information to any third party unless authorized by the NFI Policy, required by law, government rule or regulation, or order of a court of competent jurisdiction. The WidePoint NFI PKI will authenticate any request for release of information. This does not prevent WidePoint from disclosing the certificate and certificate status information (e.g., CRL, OCSP Requests and Responses, etc.).

9.4.5 Notice and Consent to Use Private Information

WidePoint may provide notice or request consent for the use of Subscriber information deemed Private.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

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

Certificates and CRLs are the sole property of the WidePoint NFI PKI. Permission is granted to reproduce and distribute certificates issued by the WidePoint NFI PKI on a nonexclusive, royalty-free basis, provided that they are reproduced and distributed in full. Certificates and CRLs will not be published in any publicly accessible repository or directory without the express written permission of WidePoint.

This CPS is the sole property of Widepoint Cyber Security Solutions (formerly Operational Research Consultants, Inc.).

Private keys are the personal property of the Subscribers who rightfully use or are capable of using them (or their employer or principal), regardless of the physical medium within which they are stored and protected

Public keys are the personal property of Subscribers (or their employer or principal), regardless of the physical medium within which they are stored and protected

WidePoint NFI PKI certificates, including WidePoint NFI PKI public keys, are the property of the WidePoint NFI PKI. The WidePoint NFI PKI licenses relying parties to use such keys only in conjunction with FIPS 140-2 validated encryption modules

Distinguished names are the property of the individuals named or their employer.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

The WidePoint NFI PKI warrants that its procedures are implemented in accordance with this CPS, and that any issued certificates that assert the certificate policy object identifiers detailed in section 1.2, Document Name and Identification, are issued in accordance with the stipulations of this CPS. The WidePoint NFI PKI warrants that CRLs issued and keys generated by the WidePoint NFI PKI are in conformance with this CPS.

The WidePoint NFI PKI warrants that any WidePoint NFI PKI RA, LRA, Code Signer Certificate Subscriber or designated authority will operate in accordance with the applicable sections of this CPS.

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

Subscriber (applicant) organizations that authorize and employ PKI Sponsor(s), LRA(s) and/ or Code Signer Certificate Subscriber(s) warrant that:

The PKI Sponsor(s), LRA(s) and/ or Code Signer Certificate Subscriber(s) procedures are implemented in accordance with the WidePoint NFI CP and this CPS

All PKI Sponsor(s), LRA(s) and/ or Code Signer Certificate Subscriber(s) actions are accomplished in accordance with this CPS

The PKI Sponsor(s), LRA(s) and/ or Code Signer Certificate Subscriber(s) operate in accordance with the applicable sections of this CPS

The PKI Sponsor(s), LRA(s) and/ or Code Signer Certificate Subscriber(s) meet the personnel and training requirements stipulated in this CPS

The applicant organization will cooperate and assist WidePoint in monitoring and auditing that authorized PKI Sponsor(s), LRA(s) and/ or Code Signer Certificate Subscriber(s) are operating in accordance with the applicable sections of this CPS

Network security controls to the PKI Sponsor(s), LRA(s) and/ or Code Signer Certificate Subscriber(s) equipment are in accordance with the applicable sections of this CPS

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

9.6.2 RA Representations and Warranties

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

When validating Subscriber requests for certificates issued under this CPS, a WidePoint NFI PKI RA accepts the following obligations:

- To validate the accuracy of all information contained in the Subscriber's certificate request
- To validate that the named Subscriber actually requested the certificate
- To verify to the RA that the certificate request originated from the named Subscriber and that the information contained in the certificate request is accurate
- To use the RA certificate only for purposes associated with the RA function
- To use private keys only on the machines which are protected and managed using commercial best practices.
- To request revocation and verify reissue requirements of a Subscriber's certificate upon notification of changes to information contained in the certificate
- To request revocation of the certificates of Subscribers found to have acted in a manner counter to Subscriber obligations
- To inform Subscribers and the RA of any changes in status
- To protect the RA certificate private keys from unauthorized access
- To immediately revoke their own RA certificate and report if private key compromise is suspected

- To ensure that obligations are imposed on Subscribers in accordance with 6.3, Other Aspects of Key Pair Management
- To inform Subscribers of the consequences of not complying with those obligations

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

9.6.3 Subscriber Representations and Warranties

When requesting and using a certificate issued under this CPS, a Subscriber accepts the following obligations:

- To accurately represent themselves in all communications with the WidePoint NFI PKI
- To protect the certificate private key from unauthorized access in accordance with Section 6.2, Private Key Protection and Cryptographic Module Engineering Controls, as stipulated in their certificate acceptance agreements, and local procedures. Only the person named in the certificate is authorized to access the private key.
- To immediately report to an RA or LRA and request certificate revocation if Private Key Compromise is suspected. (If Subscriber knows, or suspects, that her certificates are being used by someone else; or if Subscriber's certificates, or certificate export/back-up files, are on a device or computer which has been lost or stolen, she is obligated to notify WidePoint.)
- To use the certificate only for applications which have met the requirements of the WidePoint NFI CP and this CPS
- To use the certificate only for the purpose for which it was issued, as indicated in the key usage extension
- To use private keys only on the machines which are protected and managed using commercial best practices
- To report any changes to information contained in the certificate to the appropriate WidePoint NFI PKI RA or LRA for certificate reissue processing
- To not use the signature private key after the associated certificate has been revoked or expired.
- In the case of revoked or expired encryption certificates, to use associated decryption private key solely to decrypt previously encrypted information.
- To signify and guarantee that the Subscriber's application does not interfere with or infringe upon the rights of any others regarding their trademarks, trade names or any other intellectual property; and to hold WidePoint harmless for any losses resulting from any such act.
- Abide by all the terms, conditions, and restrictions levied upon the use of their private keys and 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.

9.6.4 Relying Party Representations and Warranties

WidePoint will publicly post a summary of this CPS on the WidePoint NFI PKI website to provide the relying party information regarding the expectation of the WidePoint NFI PKI. When accepting a certificate issued under this 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
- To ensure that the certificate is being used for an appropriate approved purpose
- To check for certificate revocation prior to reliance
- Use the certificate for the purpose for which it was issued, as indicated in the certificate information (i.e., the key usage extension)
- To verify the digital signature of the WidePoint NFI CA which issued the certificate they are about to rely on as stipulated in the WidePoint NFI CP
- To establish trust in the WidePoint NFI CA which issued the certificate by verifying the chain of CA certificates starting from a trust anchor of the relying party in accordance with the guidelines set by the X.509 Version 3 Amendment (for WidePoint NFI, this trust anchor will be the NFI Root CA with no additional chaining)
- To acknowledge all warranty and liability limitations
- 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
- To abide by all the terms, conditions and restrictions levied upon the use of the issued private key(s) and certificate(s) as stipulated in the WidePoint NFI CP

Note: Data format changes associated with application upgrades may invalidate digital signatures and must be avoided

Relying parties that do not abide by these obligations assume all risks associated with the certificates upon which they are relying.

Check each certificate for validity, using procedures described in the X.509 standard [ISO 9594-8], prior to reliance.

9.6.5 KRA Representations and Warranties

- WidePoint NFI PKI KRAs will operate in accordance with this CPS.
- WidePoint NFI PKI KRAs will protect Subscribers' escrowed keys from unauthorized disclosure, including the encrypted files and associated decryption keys.

- WidePoint NFI PKI KRAs will protect all information associated with key recovery, including the their own key(s), which could be used to recover subscribers' escrowed keys.
- WidePoint NFI PKI KRAs will release Subscribers' escrowed keys only for properly authenticated and authorized requests from Requestors.
- WidePoint NFI PKI KRAs will protect all information regarding all occurrences of key recovery.
- WidePoint NFI PKI KRAs will not communicate any information concerning a key recovery to the Subscriber except when the Subscriber is the Requestor.

9.6.6 Requestor Representations and Warranties

Prior to receiving a recovered key, the Requestor must formally acknowledge and agree to the obligations described here.

- Requestors will protect Subscribers' recovered key(s) from compromise. Requestors must use a combination of computer security, cryptographic, network security, physical security, personnel security, and procedural security controls to protect their keys and recovered Subscribers' keys.
- Third-party Requestors will destroy Subscribers' keys when no longer required (i.e., when the data has been recovered).
- Requestors will request and use the Subscriber's escrowed key(s) only to recover Subscriber's data they are authorized to access.
- Requestors will accurately represent themselves to all entities during any key recovery service.
- The Third-Party Requestor will protect information concerning each key recovery operation.
- The Third-Party Requestor will communicate information concerning the recovery to the Subscriber when appropriate as determined by the reason for the recovery. The decision to notify the Subscriber will be based on the law and WidePoint policies and procedures for third party information access.
- In the event that the Third-Party Requestor notifies the Subscriber of a key recovery, the Requestor will consult with the Subscriber to determine whether or not the recovery circumstances warrant revoking the associated public key certificate.
- As a condition of receiving a recovered key, a Requestor will sign an acknowledgement of agreement to follow the law and WidePoint policies relating to protection and release of the recovered key.
- Prior to receipt of the recovered key(s), the Third-Party Requestor will sign[2] an attestation to the effect:

[2] Acceptable examples include a signed paper or a document digitally signed using the credential issued by the WidePoint NFI PKI.

> "I hereby state that I have legitimate and official need to recover this key in order to obtain (recover) the encrypted data that I have authorization to access. I acknowledge receipt of a recovered encryption key associated with the Subscriber identified here *[Subscriber Name]*. I certify that I have accurately identified myself to WidePoint, and truthfully described all reasons that I require access to data protected by the recovered key. I acknowledge my responsibility to use this recovered key only for the stated purposes, to protect it from further exposure, and to destroy all key materials or return them to WidePoint when no longer needed. I understand that I am bound by WidePoint policies, applicable laws and Federal regulations concerning the protection of the recovered key and any data recovered using the key."

9.6.7 Representations and Warranties of Affiliated Organizations

WidePoint requires proof of Subscriber affiliation in the form of company photographic identification or a Letter of Affiliation on company letterhead signed by an authorized official.

9.7 Disclaimers of Warranties

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

WidePoint NFI PKI KRS' operating under this CPS may not disclaim any responsibilities described in this CPS.

The WidePoint NFI PKI disclaims all warranties and obligations of any type other than those listed.

9.8 Limitations of Liability

9.8.1 Loss Limitation

The WidePoint NFI PKI disclaims any liability for loss due to use of certificates issued by the WidePoint NFI PKI provided that the certificate was issued in accordance with the WidePoint NFI CP and this CPS and that the relying party has used validation information that complies with the WidePoint NFI CP and this CPS. The WidePoint NFI PKI acknowledges professional liability with respect to the WidePoint NFI PKI, WidePoint NFI PKI CMAs and/or the WidePoint NFI PKI RAs and LRAs.

The limit for losses per transaction due to improper actions by the WidePoint NFI PKI or a WidePoint NFI PKI CMA is limited to $1,000 (U.S. Dollars). The limit for losses per incident due to improper actions by the WidePoint NFI or a WidePoint CMA is $1 million (U.S. Dollars).

9.8.2 Other Exclusions

Certificate applicants and 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. Certificate applicants and Subscribers will hold WidePoint harmless for any losses resulting from any such act.

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

9.8.3 U.S. Federal Government Liability

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

WidePoint will have no claim for loss against the WidePoint NFI PKI PA, including but not limited to the revocation of the WidePoint NFI PKI certificate.

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

9.9 Indemnities

Agents of the WidePoint NFI PKI (e.g., RA, Trusted Agents, etc.) assume no financial responsibility for improperly used certificates.

9.10 Term and Termination

9.10.1 Term

This CPS will remain in effect until the WidePoint NFI PKI PA approves a new WidePoint NFI CP, an updated WidePoint NFI CPS that supplants this CPS, or the WidePoint NFI PKI is terminated.

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

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

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

9.11 Individual Notices and Communications with Participants

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

The WidePoint NFI will communicate to the FPKIPA any planned change to the infrastructure that has the potential to affect the FPKI operational environment at least two weeks prior to implementation, and all new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the change will be provided to the FPKIPA within 24 hours following implementation.

9.12 Amendments

9.12.1 Procedure for Amendment

The WidePoint NFI PKI PA will review the WidePoint NFI CP at least once every year. Corrections, updates, or changes to the WidePoint NFI CP will be publicly available. Suggested changes to the WidePoint NFI CP will be communicated to the contact in Section0, The WidePoint Policy Authority is responsible for all aspects of this CPS.

Contact Person; such communication must include a description of the change, a change justification, and contact information for the person requesting the change.

9.12.1.1 CPS and External Approval Procedures

The WidePoint NFI PKI PA will make the determination that this CPS complies with the policy object indentifiers detailed in Section 1.2, Document Name and Identification.

9.12.2 Notification Mechanism and Period

The WidePoint NFI PKI will publish information (including this CPS with sensitive data redacted) on a web site.

9.12.3 Circumstances Under Which Certificate Policy Identifier Must be Changed

The certificate policy object identifier will only change if the change in the WidePoint NFI CP results in a material change to the trust by the relying parties.

9.13 Dispute Resolution Provisions

The NFI Program Office will be the sole arbiter of disputes over the interpretation or applicability of the WidePoint NFI CP.

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

9.14 Governing Law

The laws of the United States of America will govern the enforceability, construction, interpretation, and validity of this CPS with respect to the WidePoint NFI CP and the schedule operated by WidePoint (i.e., the NFI provider) under the GSA Federal Supply Schedule (FSS).

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

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 that all applicable laws and regulations are adhered to.

9.15 Compliance with Applicable Law

Operation of the WidePoint NFI CA(s) are required to comply with applicable law.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

All contracts negotiated, for the purpose of providing WidePoint NFI PKI services under the policy, will contain clauses that ensure continuity and stability of the WidePoint NFI PKI operation.

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

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

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other Provisions

No stipulation.

9.17.1 Waivers

No stipulation.

10 Certificate Format

See the WidePoint NFI CP.

11 Bibliography

Refer to Appendix C, Applicable Federal and GSA Regulations.

12 Acronyms and Abbreviations

AID	Application Identifier
CA	Certification Authority
CARL	Certification Authority Revocation List
CMS	Card Management System
COMSEC	Communications Security
CP	Certificate Policy
CPS	Certification Practices Statement
CRL	Certificate Revocation List
CSOR	Computer Security Object Registry
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ERC	Enhanced Reliability Check
FAR	Federal Acquisition Regulation
FBCA	Federal Bridge Certification Authority
FPKI MA	Federal Public Key Infrastructure Management Authority
FED-STD	Federal Standard
FIPS PUB	(US) Federal Information Processing Standard Publication
FPKI	Federal Public Key Infrastructure
FPKI-E	Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile
FPKISC	Federal PKI Steering Committee
FPKIPA	Federal PKI Policy Authority

GPEA	Government Paperwork Elimination Act
GSA	General Services Administration
HTTP	Hyper Text Transfer Protocol
HSM	Hardware Security Module
IETF	International Engineering Task Force
ISO	International Organization of Standards
ISSO	Information System Security Officer
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector
ITU-TSS	International Telecommunications Union – Telecommunications System Sector
KRS	Key Recovery System
LDAP	Lightweight Directory Access Protocol
MOA	Memorandum of Agreement (as used in the context of this CPS, between an Entity such as WidePoint and the FPKIPA allowing interoperation between the FBCA and WidePoint's Principal CA)
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PIV-I	Personal Identity Verification - Interoperable
PKCS	Public Key Certificate Standard

PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request for Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA-1	Secure Hash Algorithm, Version 1
S/MIME	Secure Multipurpose Internet Mail Extension
SSL	Secure Socket Layer
TSDM	Trusted Software Development Methodology
UPN	User Principal Name
UPS	Universal Power Supply
URL	Uniform Resource Locator
U.S.C.	United States Code
UUID	Universally Unique Identifier (defined by RFC 4122)
WWW	World Wide Web

13 Glossary

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 Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Affiliated Organization	Organizations that authorize affiliation with Subscribers of PIV-I certificates.
Applicant	The Subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]
Archive	Long-term, physically separate storage.
Attribute Authority	An entity, recognized by the FPKIPA or comparable Entity body 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"]
Authenticate	To confirm the identity of an entity when that identity is presented.
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 human being.

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]. As used in this CPS, the term “Certificate” refers to certificates that expressly reference the OID(s) of this CPS in the “Certificate Policies” field of an X.509 v.3 certificate.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs.
Certification Authority Revocation List (CARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates, that have been revoked.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.
Certification Authority Software	Key Management and cryptographic software used to manage certificates issued to Subscribers.
Certificate Policy (CP)	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification Practices Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).
Certificate-Related Information	Information, such as a Subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.
Certificate Status Server	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.

Client (application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.
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]
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by the National Institute of Standards and Technology.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
Cross-Certificate	A certificate used to establish a trust relationship between two Certification Authorities.
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]
Custodial Subscriber Key	Custodial Subscriber Key Stores hold keys for a number Stores of Subscriber certificates in one location.
Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.
Dual Use Certificate	A certificate that is intended for use with both digital signature and data encryption services.
Duration	A field within a certificate which is composed of two subfields; "date of issue" and "date of next issue".
E-commerce	The use of network technology (especially the internet) to buy or sell goods and services.
Encrypted Network	A network that is protected from outside access by NSA approved high-grade (Type I) cryptography. Examples are SIPRNET and TOP SECRET networks.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.

End-entity	Relying Parties and Subscribers.
Entity	For the purposes of this document, “Entity” refers to an organization, corporation, community of interest, or government agency with operational control of a CA.
Entity CA	A CA that acts on behalf of an Entity, and is under the operational control of an Entity. The Entity may be an organization, corporation, or community of interest. For the Federal Government, an Entity may be any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Federal Government.
FBCA Management Authority (FPKI MA)	The Federal Public Key Infrastructure Management Authority is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the Federal Bridge Certification Authority.
Federal Public Key Infrastructure Policy Authority (FPKI PA)	The FPKIPA is a federal government body responsible for setting, implementing, and administering policy decisions regarding inter-Entity PKI interoperability that uses the FBCA.
Firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
High Assurance Guard (HAG)	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.
Information System Security Officer (ISSO)	Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, from design through disposal. [NS4009]
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]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
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	A deposit of the private key of a Subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the Subscriber, the terms of which require one or more agents to hold the Subscriber's private key for the benefit of the Subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]
Key Exchange	The process of exchanging public keys in order to establish secure communications.
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Key Pair	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.
Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community.
Memorandum of Agreement (MOA)	Agreement between the FPKIPA and WidePoint allowing interoperability between WidePoint and the FBCA.
Mission Support Information	Information that is important to the support of deployed and contingency forces.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
Naming Authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
National Security System	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]
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] Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.

Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI they are used to uniquely identify each of the seven policies and cryptographic algorithms supported.
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
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.
Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.
PKI Sponsor	Fills the role of a Subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this CPS.
Policy Management Authority (PMA)	Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies. For the FBCA, the PMA is the FPKIPA.
Principal CA	The Principal CA is a CA designated by an Entity to interoperate with the FBCA. An Entity may designate multiple Principal CAs to interoperate with the FBCA.
Privacy	Restricting access to Subscriber or Relying Party information in accordance with Federal law and Entity policy.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.
Relying Party	A person or Entity who has received information that includes 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.
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 database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
Responsible Individual	A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
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.
Signature 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.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).
Subscriber	A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device

Superior CA	In a hierarchical PKI, a CA who has certified the certificate signature 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.
System High	The highest security level supported by an information system. [NS4009]
Technical non-repudiation	The contribution public key mechanisms 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 an Entity in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfNFI with Certification Authorities.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure and 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.
Trustworthy System	Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.
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 recove

14 APPENDIX A

PIV-INTEROPERABLE SMART CARD DEFINITION

The intent of PIV-I is to enable issuers to issue cards that are technically interoperable with Federal PIV Card readers and applications, and that may be trusted for particular purposes through a decision of the relying Federal Agency. Thus, reliance on PIV-I Cards requires compliance with technical specifications and specific trust elements. This appendix defines the specific requirements of a PIV-I Card. It relies heavily on relevant specifications from the National Institute of Standards and Technology (NIST).

The following requirements apply to WidePoint NFI PKI PIV-I Cards:

1. To ensure interoperability with Federal systems, WidePoint NFI PKI PIV-I Cards use a smart card platform that is on GSA's FIPS 201 Evaluation Program Approved Product List (APL) and uses the PIV application identifier (AID).

2. WidePoint NFI PKI PIV-I Cards conform to [NIST SP 800-73].

3. WidePoint NFI PKI X.509 Certificates for Authentication are issued under a policy that is cross certified with the FBCA PIV-I Hardware certificate policy object identifier.

4. All WidePoint NFI PKI certificates issued a certificate policy object identifier cross certified with the PIV-I Hardware certificate policy object identifier conform to [PIV-I Profile].

5. WidePoint NFI PKI PIV-I Cards contain an asymmetric X.509 Certificate for Card Authentication that:

a. conforms to [PIV-I Profile];

b. conforms to [NIST SP 800-73]; and

c. is issued under the PIV-I Card Authentication policy.

6. WidePoint NFI PKI PIV-I Cards contain an electronic representation (as specified in SP 800-73 and SP 800-76) of the Cardholder's Facial Image printed on the card.

7. The X.509 Certificates for Digital Signature and Key Management described in [NIST SP 800-73] are optional for WidePoint NFI PKI PIV-I Cards.

8. Visual distinction of a WidePoint NFI PKI PIV-I Card from that of a Federal PIV Card is required to ensure no suggestion of attempting to create a fraudulent Federal PIV Card. At a minimum, images or logos on WidePoint NFI PKI PIV-I Cards are not placed entirely within Zone 11, Agency Seal, as defined by [FIPS 201].

Special attention is paid to UUID requirements for PIV-I.

9. WidePoint NFI PKI PIV-I Card physical topography includes, at a minimum, the following items on the front of the card:

a. Cardholder facial image;

b. Cardholder full name;

c. Organizational Affiliation, if exists; otherwise the issuer of the card; and

d. Card expiration date.

10. WidePoint NFI PKI PIV-I Cards have an expiration date not to exceed 5 years of issuance.

11. Expiration of a WidePoint NFI PKI PIV-I Card does not extend beyond the expiration of PIV-I Content Signing certificate on the card.

12. The digital signature certificate that is used to sign objects on a WidePoint NFI PKI PIV-I Card (e.g., CHUID, Security Object) contains a policy OID that has been mapped to the FBCA PIV-I Content Signing policy OID. WidePoint NFI PKI PIV-I Content Signing certificates conform to [PIV-I Profile].

13. WidePoint NFI PKI PIV-I Content Signing certificates and corresponding private key are managed within a trusted Card Management System as defined by Appendix B.

14. At issuance, the RA activates and releases the WidePoint NFI PKI 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, Authentication of Human Subscribers.

15. WidePoint NFI PKI PIV-I Cards may support card activation by the card management system to support card personalization and post-issuance card update. To activate the card for personalization or update, the card management system performs a challenge response protocol using cryptographic keys stored on the card in accordance with [SP800-73]. When cards are personalized, card management keys are set to be specific to each WidePoint NFI PKI PIV-I Card. That is, each WidePoint NFI PKI PIV-I Card contains a unique card management key. Card management keys meet the algorithm and key size requirements stated in Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification. [SP800-78]

16. The PIV-I identity proofing, registration and issuance process shall 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.

17. PIV-I Cards will only 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. 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 FPKIPA/FPKIMA.

APPENDIX B. CARD MANAGEMENT SYSTEM REQUIREMENTS

WidePoint NFI CAs have a responsibility to ensure a certain level of security from the CMS(s) that manage the token on which WidePoint NFI PKI certificates reside, and to which the WidePoint NFI PKI issues certificates for the purpose of signing PIV-I Cards. This appendix provides additional requirements to those found above that apply to WidePoint NFI PKI CMS(s) that are trusted under the Certificate Policy.

The Card Management Master Key will be maintained in a FIPS 140-2 Level 2 Cryptographic Module and conform to [NIST SP 800-78] requirements. Diversification operations will 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 will require strong authentication of Trusted Roles. Card management will be configured such that only the authorized CMS can manage issued cards.

The PIV-I identity proofing, registration and issuance process will 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.

All personnel who perform duties with respect to the operation of the CMS will receive comprehensive training. Any significant change to CMS operations will have a training (awareness) plan, and the execution of such plan will be documented.

Audit log files will be generated for all events relating to the security of the CMS and will be treated the same as those generated by the CA (see Sections 5.4 and 5.5).

A formal configuration management methodology will be used for installation and ongoing maintenance of the CMS.

WidePoint NFI PKI's Configuration Management Plan (CMP) enables system owners to proceed with system changes as needed while ensuring that the appropriate controls are in place to manage the level of risk during a configuration change. CM is conducted using four interrelated functions:

- Configuration Identification
- Change control
- Status Accounting
- Configuration Audits

The WidePoint CMP applies to all WidePoint projects or components.

The WidePoint CMP describes the use of a change control methodology to establish the system configuration baseline and define, schedule, review, and monitor changes to that configuration between baselines. It outlines roles, responsibilities, organizational relationships, functions, processes, and procedures that will be used to implement CM. The plan is designed to track any changes made to the components from the baseline throughout the lifecycle, in accordance with Federal laws, regulations, and IT Security Policy.

The WidePoint CMP incorporates rigorous change control processes and procedures. These controls ensure that the appropriate due diligence and evaluations have been completed, and that additional risks are not introduced into the without prior knowledge, careful consideration, and conscious acceptance. Strong configuration management processes also ensure that:

1. The status of system configuration activity is accurate and readily available.
2. System configuration change history is controlled and documented.
3. Each design requirement is traceable to the system configuration.
4. Each configuration item is uniquely identified.

To accomplish these goals, the WidePoint CMP includes the following CM best practices:

1. Configuration Identification – Configuration Identification is used to establish and maintain a definitive basis for control and status accounting throughout all life cycle phases of the project.

2. Configuration Control – Configuration Control is the systematic proposal, justification, evaluation, coordination, approval (or disapproval), and implementation of changes after formal establishment of a configuration baseline.

3. Configuration Status Accounting – Configuration Status Accounting is to record, store, maintain, correlate, and report the status of an evolving configuration item throughout the system life cycle.

4. Configuration Audits and Reviews – A Configuration Audit is a formal review of a project for the purpose of assessing compliance with the CMP. A Configuration Review is any activity that is conducted to evaluate the effectiveness of controls and status accounting.

The WidePoint CMP may be updated periodically to adapt to changes in procedures, rules, regulations, and best-practices as necessary to maintain proper CM practices and maintain coverage of all components.

The WidePoint NFI PKI \has documented incident handling procedures that are approved by the head of the organization responsible for operating the CMS. The documentation for incident handling is accomplished through the combination of the WidePoint Policy 18-0, Incident Reporting, WidePoint Procedure 18-1 Incident Reporting, and the WidePoint Contingency Plan. If the CMS is compromised, all certificates issued to the CMS will be revoked, if applicable. The damage caused by the CMS compromise will be assessed and all Subscriber certificates that may have been compromised will be revoked, and Subscribers will be notified of such revocation. The CMS will be re-established.

All Trusted Roles who operate a CMS will be allowed access only when authenticated using a method commensurate with PIV-I Hardware.

The computer security functions listed below are required for the CMS:

• 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)

- Enforce domain integrity boundaries for security critical processes; and
- Support recovery from key or system failure.

APPENDIX C. APPLICABLE GUIDANCE DOCUMENTS AND REGULATIONS

The following documents were used in part to either directly or indirectly develop this CPS:

ABADSG	Digital Signature Guidelines, 1996-08-01. http://www.abanet.org/scitech/ec/isc/dsgfree.html.
CIMC	Certificate Issuing and Management Components Family of Protection Profiles, version 1.0, October 31, 2001.
FIPS 140-2	Security Requirements for Cryptographic Modules May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
FIPS 186-2	Digital Signature Standard, January 27, 2000. http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf
FIPS 201	Personal Identity Verification (PIV) of Federal Employees and Contractors http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf
FOIACT	5 U.S.C. 552, Freedom of Information Act. http://www4.law.cornell.edu/uscode/5/552.html
FPKI-E	Federal PKI Version 1 Technical Specifications: Part E-X.509 Certificate and CRL Extensions Profile, 7 July 1997 http://csrs.nist.gov/pki/FPKI7-10.DOC
FPKI-Prof	Federal PKI X.509 Certificate and CRL Extensions Profile
ISO9594-8	Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 1997.
ITMRA	40 U.S.C. 1452, Information Technology Management Reform Act of 1996. http://www4.law.cornell.edu/uscode/40/1452.html
NAG69C	Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999.
NIST SP 800-73	InterfNFI for Personal Identity Verification (4 Parts) http://csrc.nist.gov/publications/PubsSPs.html
NIST SP 800-76	Biometric Data Specification for Personal Identity Verification http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf

NIST SP 800-78	Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV) http://csrc.nist.gov/publications/nistpubs/800-78-2/sp800-78-2.pdf
NSD42	National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990. http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt (redacted version)
NS4005	NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997.
NS4009	NSTISSI 4009, National Information Systems Security Glossary, January 1999.
PIV-I Profile	X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards, Date: April 23 2010, Reference Link: http://www.idmanagement.gov/fpkipa/documents/pivi_certificate_crl_profile.pdf
PKCS#12	Personal Information Exchange Syntax Standard, April 1997. ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf
RFC 2510	Certificate Management Protocol, Adams and Farrell, March 1999.
RFC 3647	Certificate Policy and Certification Practices Framework, Chokhani and Ford, Sabett, Merrill, and Wu, November 2003.

APPENDIX D. CERTIFICATE PROFILES

WidePoint NFI CAs shall issue certificates that comply with the Federal Public Key Infrastructure X.509 Certificate and CRL Extension Profile [FPKI-PROF].

WidePoint NFI CAs shall incorporate the associated Policy OIDs, listed in Section 1.2, for certificates issued in compliance with the [FPKI-PROF] for certificates issued in compliance with this CP and the FBCA CP.