Certificate Policy for the WidePoint[1]
Non Federal Issuer

Version 1.3.1

WidePoint Cybersecurity Solutions Corporation
11250 Waples Mill Road
South Tower, Suite 210
Fairfax, Virginia 22030

31 July 2019

[1] See “Notice” on next page regarding corporate name change.

***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.*

RECORD OF CHANGES

Change Number / Version	Section	Date	Current CP Version Changes
1	All	4-26-10	CP established in support of PIV-I Non-Federal Issuer requirements, and in conformance to RFC 3647
2	All	10-07-08	Updated for cross-certification with FBCA PIV-I requirements
3	All	12-6-10	Updated in response to compliance mapping performed against “FPKI Certification Applicant Requirements” by eValid8
4	All	1-3-11	Final edits resulting from mapping performed against “FPKI Certification Applicant Requirements” by eValid8
5	All	3-8-11	Edits resulting from CPWG review of CP mapping.
6	All	3-30-11	Further edits resulting from CPWG review of CP mapping.
7	Sections 8 & 9	6-3-11	Updates in response to CPWG review
8	Section 1.2, Table 1	8-7-11	Correction of typographical errors (spaces in OID names and OID field removed)
9	Section 1.3.1.4; Section 8; Section 8.4; Section 8.6; Glossary	6-5-2013	Updates in response to changes resulting from FBCA CP v2.26.
10	Section 1.2	2-18-2014	Addition of new WidePoint OIDs to be issued starting 4-1-2014; set date of 3-31-2014 for cessation of issuing RSA OIDs.
11	Sections: 1.2; 2.2.1; 3.3.1; 4.1.2; 4.9.3; 5.2.1.1; 5.2.4; 5.3.2; 5.4.8; 5.5.4; 5.6; 5.7.3; 5.7.4; 6.1.1.1; 6.1.1.2; 6.1.7; 6.2.4.4; 6.3.2; 6.7; 7.1.2; Appendix B	9-30-2014	Updates to address mapping with FBCA CP.
12	Sections 3.2.3.1.3; 5.1.2.1; 5.1.2.4; 5.2.1; 6.2.4.2; 6.2.4; 7.1.2; 8; Appendix lettering	3-28-2016	Updates to reflect WidePoint legal name change to Widepoint: adjust for Cert-on-Device capability; further updates to address mapping w/FBCA CP.
13	Notice	4-28-2016	Insert of “Notice” to clarify legal name change and its implication.
14	Section 1.2	7-21-2016	Certificate policy description update
1.2	All	8-29-2018	Annual review and update
1.3	All	3-14-2019	
1.3.1		7-31-2019	Updates to address comments from FPKI in review of annual audit package.

TABLE OF CONTENTS

SECTION **PAGE**

1 INTRODUCTION

This WidePoint Non-Federal Issuer (NFI) Certificate Policy (CP) includes seven distinct certificate policies: a policy for users with software cryptographic modules, a policy for users with hardware cryptographic modules, a policy for Personal Identity Verification – Interoperable (PIV-I) hardware cryptographic modules, a PIV-I card authentication policy, a policy for a Device (hardware device or software program), a policy for Device Hardware, and a PIV-I content signing policy. Where a specific policy is not stated, the policies and procedures in this specification apply equally to all seven policies.

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

A PKI that uses this CP 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.)

The user policies require subscribers to use FIPS 140 validated cryptographic modules for cryptographic operations and the protection of trusted public keys. The device policy also requires use of FIPS 140 validated cryptographic modules for cryptographic operations and the protection of trusted public keys.

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

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

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

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

Framework.

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

1.1 OVERVIEW

1.1.1 Certificate Policy (CP)

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

1.1.2 Relationship Between the WidePoint NFI CP and the WidePoint NFI CA's Certification Practice Statements (CPS)

The WidePoint NFI CP states what assurance can be placed in a certificate issued by a WidePoint NFI CA. Each WidePoint NFI CA shall provide a detailed Certification Practice Statement (CPS) which states how the WidePoint NFI CA establishes that assurance in accordance with this WidePoint NFI CP.

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 this CP and those in the FBCA CP.

The WidePoint NFI CP is intended to map to the FBCA Medium-Hardware [PIV-I] and Medium levels of assurance for all of the certificates identified in Section 1.2

1.1.4 Scope

The WidePoint NFI PKI exists to facilitate trusted electronic business transactions for State and Local Governments, and non-Federal organizations and individuals. This WidePoint NFI CP describes the following:

- Roles, responsibilities, and relationships among the CAs, Registration Authorities (RAs), Certificate Manufacturing Authorities (CMAs), Repositories, Subscribers, Relying Parties, and the Policy Authority (PA) (referred to collectively herein as "Program Participants") authorized to participate in the PKI described by this 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

This WidePoint NFI CP provides a high level description of the policies and operation of the WidePoint NFI PKI. Specific detailed requirements for the services outlined in this document may be found in each WidePoint NFI CA's CPS.

1.1.5 Interaction with PKIs External to the Federal Government

The WidePoint NFI CP, and individual WidePoint NFI CAs' CPS, collectively ensures interoperability between all WidePoint NFI CAs. MOAs with the FPKIPA and other entities ensure interaction and interoperability with authorized Federal Government and non-government CAs.

1.2 Document Identification

This Policy has been assigned the object identifiers (OIDs) described below which define the WidePoint NFI Certificate Policies and levels of assurance asserted by digital certificate issued under this policy. All WidePoint NFI certificates issued under this CP shall reference the WidePoint NFI CP by including the appropriate OID in the *Certificate Policies* field of the WidePoint NFI certificate. Only WidePoint NFI OIDS may be used within WidePoint NFI certificates, except as specifically authorized by this CP. OIDs listed below are WidePoint OIDs under the Operational Research Consultants, Inc. arc 1.3.6.1.4.1.3922, registered with IANA:

WidePoint NFI CP Description	Description	Policy OID
WidePoint NFI Authorized CA	id-orc-nfissp-ca	::= {1.3.6.1.4.1.3922.1.1.1.100}
WidePoint NFI Medium	id-orc-nfissp-medium	::={ 1.3.6.1.4.1.3922.1.1.1.3}
WidePoint NFI Medium Hardware	id-orc-nfissp-mediumhardware	::={ 1.3.6.1.4.1.3922.1.1.1.12}
WidePoint NFI PIV-I Hardware	id-orc-nfissp-pivi-hardware	::={ 1.3.6.1.4.1.3922.1.1.1.18}
WidePoint NFI PIV-I Card Authentication	id-orc-nfissp-pivi-cardAuth	::={ 1.3.6.1.4.1.3922.1.1.1.19}
WidePoint NFI PIV-I Content Signing	id-orc-nfissp-pivi-contentSigning	::={ 1.3.6.1.4.1.3922.1.1.1.20}
WidePoint NFI Device	id-orc-nfissp-mediumDevice	::={ 1.3.6.1.4.1.3922.1.1.1.37}
WidePoint NFI Device Hardware	id-orc-nfissp-mediumDeviceHardware	::={ 1.3.6.1.4.1.3922.1.1.1.38}

WidePoint NFI Object Identifiers (under ORC arc)

Certificates issued to CAs may contain any or all of these OIDs. Certificates issued to subscribers to support digitally signed documents or key management may contain either an, Id-orc-nfissp-medium, Id-orc-nfissp-mediumhardware or Id-orc-nfissp-pivi-hardware. Certificates issued to devices under this policy may contain the Id-orc-nfissp-mediumDevice, Id-orc-nfissp-mediumDeviceHardware, or Id-orc-nfissp-pivi-contentSigning. In this document, 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 shall assert policies id-orc-nfissp-mediumDevice, id-orc-nfissp-mediumDeviceHardware, or id-orc-nfissp-pivi-contentSigning policies. All other policies defined in this document should be reserved for human subscribers when used in End-Entity certificates.

Certificates issued to subscribers supporting authentication but not digital signature may contain Id-orc-nfissp-pivi-hardware. Certificates issued to subscribers supporting authentication where the private key can be used without user authentication may contain Id-orc-nfissp-pivi-cardAuth or Id-orc-nfissp-pivi-contentSigning. 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 Object Identifiers 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.

id-orc-nfissp-medium::={ 1.3.6.1.4.1.3922.1.1.1.3}
Maps to FBCA Medium Assurance. For subscribers with software cryptographic modules. Uses: digital signature, client authentication, encryption.

id-orc-nfissp-mediumhardware ::={ 1.3.6.1.4.1.3922.1.1.1.12}
Maps to FBCA mediumHardware. For subscribers 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.

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-mediumDevices ::={ 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-mediumDevicesHardware ::={ 1.3.6.1.4.1.3922.1.1.1.38}
For subscribers with hardware cryptographic modules on devices only; requires a human sponsor. Uses: device authentication, encryption.

Certificates issued to a WidePoint NFI PKI CA may contain any or all of these OIDs. Certificates issued to Subscribers to support digitally signed documents or key management may contain the id-orc-nfissp-medium, or id-orc-nfissp-mediumHardware. Certificates issued to subscribers supporting authentication but not digital signature may contain id-orc-nfissp-pivi-hardware. Certificates issued to subscribers supporting authentication where the private key can be used without user authentication may contain id-orc-nfissp-pivi-cardAuth. These Policy Object Identifiers are populated in accordance with CPS section 7.1.6.

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 is responsible for organizing and administering this WidePoint NFI CP; and for the operations and maintenance of all WidePoint NFI PKI components in accordance with this CP.

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 CA signing keys
- Ensuring that all aspects of the WidePoint NFI CA services and WidePoint NFI CA operations and infrastructure related to WidePoint NFI Certificates issued under this CP are performed in accordance with the requirements, representations, and warranties

of this CP (the only exception being when the Government, pursuant to agreement between WidePoint, Relying Parties, and the WidePoint NFI CAs provides defined portions of the RA role and function).

1.3.1.4 Certificate Status Server

The WidePoint NFI PKI shall include an Online Certificate Status Protocol (OCSP) responder to provide online, near-real-time status information. The OCSP responder is also identified as a Certificate Status Server (CSS), and included in certificates as an authoritative source for revocation information (i.e., authority information access [AIA] certificate extension).

1.3.1.5 Cross-Certification with the FBCA

In accordance with the MOA, the WidePoint NFI CA cross-certifies directly with the FBCA . 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 federal bridge. No CA or end-entity certificate shall have more than one path back to the Federal Bridge Certification Authority.

1.3.1.6 WidePoint PKI Policy Management Authority

The WidePoint NFI Policy Authority is responsible for maintaining the entity PKI CP and for ensuring that all WidePoint NFI PKI components (e.g., CAs, CSSs, CMSs, RAs) are operated in compliance with the entity WidePoint CP. This body is referred to as the WidePoint PKI Policy Management Authority (PMA) within this CP.

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

1.3.1.7 Key Escrow Database (KED)

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

1.3.2 Registration Authority (RA)

The WidePoint NFI 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 WidePoint NFI KRA is an individual who, using a two-party control procedure with a second WidePoint NFI KRA, is authorized, as specified in the applicable WidePoint NFI KRPS, to interact with the WidePoint NFI KED in order to extract an escrowed key. The WidePoint NFI

KRAs send the recovered key to the Requestor. The WidePoint NFI KRAs have high level, sensitive access to the WidePoint NFI KED and are considered Trusted Roles (see Section 5.2.1). WidePoint NFI Registration Authorities (RA) as defined in the WidePoint NFI CP may fill the role of WidePoint NFI KRA; however, because WidePoint NFI KRAs can recover large numbers of keys, the number and location of WidePoint NFI KRAs should be closely controlled. In some cases, WidePoint NFI KRAs may be employed by a Subscriber organization distinct from the organization that operates the Issuing WidePoint NFI CA. WidePoint NFI KRAs that do not belong to the Issuing WidePoint NFI CA are authorized to recover keys of subscribers from the WidePoint NFI KRAs' Organization/ Enterprise only.

1.3.4 Card Management System (CMS)

The Card Management System is responsible for managing smart card token content. In the context of this policy, the CMS requirements are associated with the PIV-I policies only. WidePoint NFI CAs issuing PIV-I certificates are responsible for ensuring that all WidePoint NFI CMS’ meet the requirements described in this document, including all requirements specified in APPENDIX B, CARD MANAGEMENT SYSTEM REQUIREMENTS. Any CMS operated by the WidePoint NFI PKI Policy Management Authority shall not be issued certificates which express the PIV-I Hardware or Id-orc-nfissp-pivi-cardAuth policy OID.

1.3.5 Subscribers

A Subscriber is the entity whose name appears as the subject in a certificate. A subscriber asserts that the key and certificate are used in accordance with the certificate policy asserted in the certificate. Note that CAs are sometimes technically considered “subscribers” in a PKI; however, the term “subscriber” as used in this CP does not refer to CAs.

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.

1.3.7 Relying Parties

A Relying Party uses a Subscriber’s certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the Subscriber. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. A Relying Party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

This CP makes no assumptions or limitations regarding the identity of Relying Parties. While Relying Parties are generally Subscribers, Relying Parties are not required to have an established relationship with WidePoint or a WidePoint NFI CA.

1.3.8 Key Recovery Requestors

A Requestor is the person who requests the recovery of a decryption private key. A Requestor may be the Subscriber (for self-recovery, when permitted) or a third party (e.g., supervisor, corporate officer or law enforcement officer) authorized to request recovery of a Subscriber's escrowed key on behalf of the Subscriber or on behalf of the organization. Any individual who can demonstrate a verifiable authority and a need to obtain a recovered key may be considered a requestor.

1.3.8.1 Subscriber

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

1.3.8.2 Internal Third-Party Requestor

An Internal Third-Party Requestor is any Requestor who is in the Subscriber's supervisory chain or otherwise authorized to obtain the Subscriber's key for the Issuing Organization. The Issuing Organization shall identify authorized Requestors and the WidePoint NFI KRS shall implement the WidePoint NFI KRP so that the existing Issuing Organization Policy regarding access and release of sensitive information can be met.

1.3.8.3 External Third-Party Requestor

An External Third-Party Requestor is someone (e.g. investigator) outside the Issuing Organization (i.e. the organization on behalf of which the WidePoint NFI CA issues certificates to subscribers) with a court order or other legal instrument to obtain the decryption private key of the Subscriber. An External Third-Party Requestor must submit the key recovery request via an Internal Third-Party Requestor unless the law requires the WidePoint NFI KED to release the Subscriber's private key without 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. The WidePoint NFI KRS and Issuing Organizations shall appoint authorized personnel and implement the WidePoint NFI KRP so that the existing Issuing Organization policies regarding release of sensitive information can be met.

1.3.9 Other Participants

The WidePoint NFI PKI may require the services of other security, community, and application authorities. The WidePoint NFI CPS shall identify the parties, define the services, and designate the mechanisms used to support these services.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

Subscribers and WidePoint NFI CAs may use WidePoint NFI digital signature certificates to mutually authenticate Subscribers and Relying Party Applications. Subscribers and Applications may use encryption certificates to employ the confidentiality service on the data exchanged.

The sensitivity of the information processed or protected using certificates will vary significantly. Relying Parties must evaluate the environment and associated threats and vulnerabilities, and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each Relying Party for its application and is not controlled by this CP.

All WidePoint NFI certificates, where the issuance of the certificate is based on “in-person” verification of identity prior to issuance, are intended to be used at the Medium level of assurance 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.

All WidePoint NFI certificates, where the issuance of the certificate is based on “in-person” verification of identity prior to issuance and the key pairs are generated in an approved hardware device (i.e., token, smart card) are intended to be used at the Medium Hardware level of assurance 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 CP is intended to support applications involving unclassified information, which can include sensitive unclassified data protected pursuant to Federal statutes and regulations.

1.4.2 Prohibited Certificate Uses

Certificates that assert the Id-orc-nfissp-pivi-cardAuth OID shall only be used to authenticate the hardware token containing the associated private key and shall not 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 CP.

1.5.2 Contact Person

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

1.5.3 Person Determining Certification Practices Statement (CPS) Suitability for this Policy (CP)

The CPS must conform to this CP. The WidePoint PKI Policy Authority is responsible for ensuring that the CPSs of WidePoint NFI CAs conform to this CP.

The determination of suitability of a CPS shall be based on an independent compliance auditor's results and recommendations. See Section 8, Compliance Audits and Other Assessments, for further details.

1.5.4 CPS Approval Procedures

The CPS and the results and recommendations of the independent, trusted third-party shall be submitted to the WidePoint PKI Policy Authority for approval. WidePoint NFI CAs shall comply with all requirements of this CP.

The CA and RA must meet all requirements of an approved CPS before commencing operations. In some cases, the FPKIPA may require the additional approval of an authorized agency. The FPKIPA will make this determination based on the nature of the system function, the type of communications, or the operating environment.

1.6 DEFINITIONS AND ACRONYMS

See Sections 12 and 13.

2 PUBLICATION & REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

WidePoint NFI CAs shall operate and maintain repositories to support their PKI operations and for retention of certificate information for all certificates issued, and provide anonymous read/bind access. Information contained in those repositories is protected in accordance with the Privacy Act of 1974, as set forth in the WidePoint NFI CA's Privacy Policy and Procedures documents.

2.1.1 Repository Obligations

A Repository is responsible for maintaining a secure system for storing and retrieving currently valid WidePoint NFI Certificates, a current copy of this CP and other information relevant to WidePoint NFI Certificates, and for providing certificates status services for a Relying Party.

The Repository shall implement access controls to prevent unauthorized modification or deletion of information.

WidePoint NFI CAs may post certificates and CRLs in additional replicated repositories for performance enhancements. Such repositories may be operated by the WidePoint NFI CA or other parties (i.e., state agencies).

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 Publication of Certificates and Certificate Status

Each WidePoint NFI CA shall operate a secure online Repository available to Subscribers and Relying Parties that shall have the capability to contain:

- Currently valid Certificates issued by a WidePoint NFI CA that have been accepted by the Subscriber
- Certificate Revocation List (CRL) and online certificate status information
- WidePoint NFI CA Certificate for its signing key
- Other relevant information about the certificates

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

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

WidePoint NFI CA certificates, CRLs, and online certificate status information shall be available for retrieval 24 hours a day, seven 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 CA Information

The following CA information shall be published and publicly available at https://www.orc.com/nfi/policies/:

- Copy of this CP
- Redacted version of the WidePoint NFI CPS

2.2.3 Interoperability

WidePoint NFI CAs shall:

- Support interoperability between all WidePoint NFI CAs
- Ensure interoperability with the FBCA Repository

2.3 FREQUENCY OF PUBLICATION

This CP and any subsequent changes shall be made publicly available within thirty days of approval.

Publication requirements for CRLs are provided in Section 4.9 of this CP, Certificate Revocation and Suspension.

2.4 ACCESS CONTROLS ON REPOSITORIES

WidePoint shall make publicly available and not impose any access controls on this CP, the WidePoint NFI CA's certificate for its signing key, and past and current versions of the WidePoint NFI CA's CPS (may be redacted), as well as subscriber certificates and certificate status information.

WidePoint shall impose access controls to ensure authentication of Subscribers with respect to their own certificate(s) and the status of such certificate(s) and personal registration information that is separately managed from the public certificate and status Repository. Such controls shall restrict access in accordance with those regulations and guidelines cited in this CP and WidePoint policies and procedures for protecting personal and private information about individuals. Access to information in WidePoint NFI CA repositories shall be determined by the PA pursuant to its authorizing and controlling statutes.

At a minimum, the WidePoint NFI CA repository shall make CA certificates and CRLs issued by the CA and CA certificates issued to the CA available to Relying Parties.

For WidePoint NFI CA s, the CPS shall detail what information in the repository shall be exempt from automatic availability, and shall also specify to whom, and the conditions under which, the restricted information may be made available.

3 IDENTIFICATION & AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

All certificates issued to end entities shall include a non-NULL subject DN.

Certificates at all levels of assurance may include alternative name forms. This CP does not restrict the types of names which can be used.

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

Medium (all policies)	Non-Null Subject Name, and Subject Alternative Name if marked non-critical
PIV-I Card Authentication	Non-Null Subject Name and Subject Alternative Name

Table 1: Subject DN and SAN name

Medium Hardware and PIV-I Hardware certificates shall 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}

PIV-I Content Signing certificates shall 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 shall 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 shall be encoded within the serialNumber attribute using the UUID string representation defined in Section 3 of RFC 4122 (e.g., "f81d4fae-7dec-11d0-a765-00a0c91e6bf6").

3.1.2 Need for Names to Be Meaningful

Names used in the certificates issued by a WidePoint NFI CA must identify the person or object to which they are assigned in a meaningful way, as provided in Table 4.

Certificate Description	Name Meanings
WidePoint NFI CA Digital Signature Certificates	WidePoint NFI CAs shall implement the name constraint extension of the X.509 version 3, certificate profile in issuing CA certificates.
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; a unique device identification naming convention (e.g., FQDN, IP address, MAC address, IMEI, etc.); or an application name 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.
FBCA Cross-Certificates	WidePoint NFI CAs shall implement the name constraint extension of the X.509 version 3 certificate profile in issuing cross certificates.

Table 4, Naming Constraints

When DNs are used, the directory information tree must accurately reflect organizational structures.

When DNs are used, the common name must respect name space uniqueness requirements and must not be misleading. This does not preclude the use of pseudonyms as defined in Section 3.1.3.
Although WidePoint does not currently support the use of User Principal Names (UPN), if and when UPNs are used, they must be unique and accurately reflect organizational structures.

3.1.3 Anonymity or Pseudonymity of Subscribers

DNs in certificates issued by a WidePoint NFI CAs may contain a pseudonym (such as a large number) as long as name space uniqueness requirements are met.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting distinguished name forms are specified in X.500. Rules for interpreting email addresses are specified in RFC 2822. The WidePoint NFI PIV-I certificate profiles are established by the WidePoint PKI Policy Authority and conform to the PIV-I-PROF.

3.1.5 Uniqueness of Names

Name uniqueness must be enforced. WidePoint NFI CAs and RAs shall enforce name uniqueness within the X.500 name space for which they have been authorized. When other name forms are used, they too must be allocated such that name uniqueness is ensured.

WidePoint NFI CAs shall document, in their respective CPSs, how they will assign subject names within the Subscriber community to guarantee name uniqueness among current and past Subscribers (e.g., if Joe Smith leaves a CA's community of Subscribers, and a new, different Joe Smith enters the community of Subscribers, how will these two people be provided unique names?).

For distinguished names, name uniqueness is applicable for the entire name rather than a particular attribute.

At a minimum, name uniqueness within a WidePoint NFI CA, including subordinate CAs, shall be ensured through a combination of certificate serial number, common name, and the WidePoint NFI CA name issuing the certificate.

The WidePoint PKI Policy Authority is responsible for ensuring name uniqueness in certificates issued by the WidePoint NFI CA.

3.1.6 Recognition, Authentication, and Role of Trademarks

A corporate entity is not guaranteed that its name will contain a trademark if requested. The WidePoint NFI CA shall not knowingly issue a certificate including a name that a court of competent jurisdiction has determined infringes the trademark of another. It is not subsequently required to issue that name to the rightful owner if it has already issued one sufficient for identification. A WidePoint NFI CA shall not be obligated to research trademarks or resolve trademark disputes.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

In all cases where the subject named in a certificate generates its own keys, that subject shall be required to prove possession of the private key that corresponds to the public key in the certificate request.

For signature keys, this may be done by the Subscriber using its private key to sign a value and providing that signed value to a WidePoint NFI CA. The WidePoint NFI CA shall then validate the signature using the Subscriber's public key.

The WidePoint NFI CPS shall specify the mechanisms for proving possession of the private key.

In the case where key generation is performed by the WidePoint NFI CA or RA either (1) directly on the Subscriber's hardware or software token, or (2) in a key generator that benignly transfer the key to the party's token, then proof of possession is not required.

3.2.2 Authentication of Sponsoring Organization Identity

If the applicant is requesting an organizationally affiliated certificate, in addition to verifying the applicant's individual identity and authorization to represent the Sponsoring Organization, the WidePoint NFI CA shall also verify the Sponsoring Organization's current operating status. In conducting its review and investigation, the WidePoint NFI CA shall provide validation of information concerning the Sponsoring Organization, including legal company name, type of entity, address (number and street, city, ZIP code), and telephone number.

For key recovery, a third-party requestor shall have their authority to act on behalf of the organization validated.

3.2.3 Authentication of Individual Identity

If the applicant passes identity proofing verification as specified in the following sections of this CP, WidePoint NFI CA shall, at a minimum, record the following transaction data:

- Applicant's name as it appears in the certificate's Common Name field
- Method of application (i.e., online, in-person)
- For each data element accepted for proofing, including electronic forms:
  - Name of document presented for identity proofing
  - Issuing authority
  - 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
- Identity of the person performing the verification
- All associated error messages and codes, if any
- Date/time of process completion
- A unique identifying number from the ID of the verifier and from the ID of the applicant.

If the applicant fails identity proofing verification performed by the WidePoint NFI CA, the WidePoint NFI CA shall notify the applicant of the verification failure via out-of-band notification process linked to the certificate applicant's physical postal address.

The WidePoint NFI CAs and/or RAs shall ensure that the applicant's identity information and public key are properly bound.

If an applicant is unable to perform face-to-face registration alone, the applicant shall be represented by a trusted person already issued a digital certificate by the WidePoint NFI CA. The trusted person will present information sufficient for registration at the level of the certificate being requested by the applicant, for both himself/herself and the applicant who the trust person is representing.

An entity certified by a government organization as being authorized to confirm identities may perform in-person authentication of identity as a Trusted Agent RA, or on behalf of the RA. The certified entity forwards the information collected from the application directly to the WidePoint NFI CA or RA for verification of the information a secure manner. If the Trusted Agent performs all or part of the verification of identity, that information shall also be forwarded directly to a WidePoint NFI CA or RA. Packages secured in a tamper-evident manner by the certified entity satisfy this requirement. Other secure methods may also be acceptable, as approved by the WidePoint NFI PA.

PIV-I Hardware certificates shall only be issued to human subscribers. For human subscribers, this CP allows a certificate to be issued only to a single entity. Certificates shall not be issued that contain a public key whose associated private key is shared.

3.2.3.1 Authentication of Human Subscribers

For all Medium Assurance Widepoint NFI PKI certificates, authentication of the identity of human subscribers shall be established no more than 30 days before initial certificate issuance. For Subscribers, the Widepoint NFI CA and/or associated RAs shall ensure that the applicant's identity information is verified in accordance with the process established by this CP and the applicable CPS.

The Widepoint NFI PKI shall record the information set forth below for issuance of each certificate:

- The identity of the person performing the identification;
- A signed declaration by that person that he or she verified the identity of the applicant as required using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law. The signature on the declaration may be either a handwritten or digital signature using a certificate that is of equal or higher level of assurance as the credential being issued;
- If in-person identity proofing is done, a unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- The date of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature or appropriate digital signature (see Practice Note) and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

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

For pseudonymous certificates that identify subjects by their organizational roles, the WidePoint NFI CA shall validate that the individual either holds that role or has been delegated the authority to sign on behalf of the role.

3.2.3.1.1 Authentication of Digital Signature and Encryption

For Digital Signature and Encryption Certificates, identity shall be established by in-person appearance before the Registration Authority or Trusted Agent. Information provided shall be checked to ensure its legitimacy. Credentials required are either one Federal Government-issued Picture I.D., or two ID's, one of which shall be a non-Federal Government photo ID (e.g., a Driver's License), and the second of which shall be Government issued ID or one of the following membership-type ID, as listed below. Any credentials presented must be unexpired.

The applicant's identity must be personally verified prior to the certificate being enabled. The applicant shall appear personally before either:

- A WidePoint NFI CAA
- A trusted Agent or RA approved by the WidePoint NFI CA or appointed by name in writing by the WidePoint NFI CA
- A person certified by a State or Federal Government as being authorized to confirm identities (such as Notaries Public), who uses a stamp, seal, or other mechanism to authenticate their identity confirmation.

The WidePoint NFI CA, RA or Trusted Agent shall verify:

- That the applicant is a duly authorized representative of the Sponsoring Organization as an employee, partner, member, agent, or other association, and
- The Sponsoring Organization's identity as specified in Section 3.2.2

The applicant shall personally appear before one of the required identity verifiers at any time prior to application of the WidePoint NFI CA's signature to the applicant's certificate, or alternatively, when private keys are delivered to Subscribers via hardware tokens.

3.2.3.1.2 Authentication of PIV-I Hardware and PIV-I Card Authentication

For PIV-I Certificates the following biometric data shall be collected during the identity proofing and registration process, and shall be formatted in accordance with [NIST SP 800-76]:

- An electronic facial image used for printing facial image on the card, as well as for performing visual authentication during card usage. A new facial image shall be collected each time a card is issued; and

- Two electronic fingerprints to be stored on the card for automated authentication during card usage.

For PIV-I, credentials required are 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 PIV-I, the use of an in-person antecedent is not applicable.

3.2.3.1.3 Authentication of Cert-on-device Person ID

For WidePoint NFI Cert-on-device certificates, identity shall be verified in accordance with the requirements specified in [SP 800-63] for issuing E-Authentication Level 3.

3.2.3.1.4 Other Certificates

Nothing in this policy prohibits WidePoint from requiring other certificates to meet specific needs of participating organizations.

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 Device Identity

Some computing and communications devices will be named as certificate subjects. In such cases, the device must have a human sponsor. The PKI sponsor is responsible for providing the following registration information:

- Registered domain name or IP address
- Equipment public keys
- Equipment authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or RA to communicate with the sponsor when required

The registration information shall be verified to an assurance level commensurate with the certificate assurance level being requested. For certificates issued at the mediumDevice and mediumDeviceHardware policies, registration information shall be verified commensurate with the Medium assurance level. Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

- Verification of digitally signed messages sent from the sponsor using a certificate of equivalent or greater assurance than that being requested (i.e., Medium or Medium Hardware)

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

These certificates shall be issued only to devices under the sponsoring organization's control (i.e., require registration and validation that meets all issuing WidePoint NFI CA's requirements, as well as requiring re-validation prior to being re-issued). In the case a human sponsor is changed, the new sponsor shall review the status of each device under his/her sponsorship to ensure it is still authorized to receive certificates. The CPS shall describe procedures to ensure that certificate accountability is maintained.

3.2.3.5 KRA Authentication

The WidePoint NFI KRA shall authenticate to the WidePoint NFI KED directly or using a public key certificate issued by the associated WidePoint NFI PKI. The assurance level of the certificate shall be the same as or greater than that of the certificate whose companion private key is being recovered.

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 3.2.3.1, "Authentication of Human Subscribers".

Identity authentication shall be commensurate with the assurance level of the certificate associated with the key being recovered. Identity shall be established using one of the following methods:

- Procedures specified by the WidePoint NFI CPS for authentication of an individual identity during initial registration for the specified certificate policy assurance level (an assurance level equal to or greater than the assurance level of the certificate whose companion private key is being recovered).
- Certificate-based authentication (e.g., digitally signed e-mail or client-authenticated TLS) that can be verified using current, valid (i.e., un-revoked) public key certificates issued by the Issuing Organization's PKI at the specified certificate policy assurance level (an assurance level equal to or greater than the assurance level of the certificate whose companion private key is being recovered).

The WidePoint NFI KRA shall verify the identity of the Requestor prior to initiating the key recovery request.

3.2.4 Non-verified Subscriber Information

Subscriber information that is not verified shall not be included in a WidePoint NFI certificates.

3.2.5 Validation of Authority

Before issuing certificates that assert organizational authority (i.e., code signing certificates), the WidePoint NFI CA shall validate the individual's authority to act in the name of the organization.

3.2.5.1 Requestor Authorization Validation

The WidePoint NFI KRA shall validate the authorization of the Requestor in consultation with WidePoint management and/or legal counsel, as appropriate.

3.2.5.2 Subscriber Authorization Validation

Current Subscribers are authorized to recover their own escrowed key material.

3.2.5.3 KRA Authorization Validation

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

3.2.6 Criteria for Interoperation

The MOA(s) with the FPKIPA and other entities ensure interaction and interoperability with WidePoint NFI CAs, authorized State and Local Government agencies, and non-government CAs. At no point shall CA or end-entity certificates issued under this Certificate Policy have more than one path back to the Federal Bridge Certification Authority.

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

When a WidePoint NFI CA updates its private signature key and thus generates a new public key and certificate, the WidePoint NFI CA shall notify the Policy Authority, RAs, and Subscribers, indicating that the CA's public certificate has been changed, in addition to publishing the certificate in the repository and making it publicly available.

Subscribers of WidePoint NFI CAs shall identify themselves for the purpose of re-keying as required in the table below.

Assurance Level	Routine Re-key Identity Requirements for Subscriber Signature, Authentication and Encryption Certificates

Medium (all policies)	Identity may be established through use of current signature key, except that identity shall be established through initial registration process at least once every nine years from the time of initial registration. For mediumDevice and mediumDeviceHardware certificates, identity may be established through the use of current signature key or using means commensurate with the strength of the certificate being requested, except that identity shall 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 shall be established through initial registration process at least once every nine years from the time of initial registration.

Table 5: Re-Key Identity Requirements

3.3.2 Identification and Authentication for Re-key after Revocation

After a certificate has been revoked other than during a renewal or update action, the subscriber is required to go through the initial registration process described in Section 3.2 to obtain a new certificate.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

WidePoint NFI CAs shall provide for the revocation of certificates when requested, at any time and for any reason.

A Certificate revocation request that is submitted electronically may be authenticated on the basis of a digital signature using the Certificate’s associated key pair. Requests to revoke a certificate may be authenticated using that certificate's public key, regardless of whether or not the associated private key has been compromised. The identity of the person submitting a revocation request in any other manner shall be authenticated in accordance with Section 4.9. Other revocation request authentication mechanisms may be used as well, including a request in writing signed by the Subscriber and sent via U.S. Postal Service first-class mail, or equivalent.

These authentication mechanisms must balance the need to prevent unauthorized revocation requests against the need to quickly revoke certificates.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

This section specifies requirements for initial application for certificate issuance.

4.1.1 Application Initiation

The following persons may initiate the Certificate application process:

Potential Subscriber	Authorized Initiator
Unaffiliated Individual	Potential Subscriber only
Business Representative	Sponsoring Organization or potential Subscriber
State and Local Government Employee	Sponsoring Organization or potential Subscriber
Relying Party Applications	Duly authorized representative of the Relying Party
Devices	Sponsor responsible for the device receiving the certificate

Table 6: Certificate Application Process Initiators

For key recovery, Subscribers may request their own escrowed keys. Key recovery may also be requested by internal third-party requestors permitted by WidePoint policy, and by authorized external third-party requestors (e.g., law enforcement personnel) with a court order from a competent court.

4.1.2 Enrollment Process and Responsibilities

Applications for WidePoint NFI Certificates may be communicated from the applicant to a WidePoint NFI CAA or an authorized RA, and authorizations to issue Certificates may be communicated from an authorized RA to a WidePoint NFI CAA:

- Electronically, provided that all communication is secure
- By U.S. Postal Service first-class mail
- In person.

All electronic transmissions and communications supporting application and issuance processes shall be authenticated and protected from modification.

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

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

4.1.3 Key Escrow Process and Responsibilities

Subscriber private keys (i.e., decryption private keys) associated with a key management certificate shall be securely escrowed by the WidePoint NFI KED. The WidePoint NFI CA shall ensure that the keys are successfully escrowed prior to issuance of the key management certificates.

Subscriber private keys shall be protected during transit and storage using cryptography at least as strong as the key being escrowed.

As part of the key escrow process, Subscribers shall be notified that the private keys associated with their encryption certificates will be escrowed.

4.1.4 Key Recovery Process and Responsibilities

Communications between the various key recovery participants (WidePoint NFI KED, WidePoint NFI KRA, Requestor and Subscriber) shall be secured from protocol threats such as disclosure, modification, replay, and substitution. The strength of all cryptographic protocols shall be equal to or greater than that of the keys they protect. During delivery, escrowed keys shall be protected against disclosure to any party except the Requestor. When any mechanism that includes a shared secret (e.g., a password) is used to protect the key in transit, the mechanism shall ensure that the Requestor and the transmitting party are the only holders of this shared secret.

Subscribers may use electronic or manual means to request their own escrowed keys from the WidePoint NFI KRS. The Subscriber may submit the request to the WidePoint NFI KED or WidePoint NFI KRA. If the request is made electronically, the subscriber shall digitally sign the request using an associated PKI-issued authentication or signature certificate with an assurance level equal to or greater than that of the escrowed key. Manual requests shall be on paper and shall be signed by hand.

Third party Requestors may use electronic or manual means to request the Subscribers' escrowed keys. The Requestor shall submit the request to the WidePoint NFI KRA. If the request is made electronically, the Requestor shall digitally sign the request using an associated PKI-issued authentication or signature certificate with an assurance level equal to or greater than that of the escrowed key. Manual requests shall be on paper and shall be signed by hand.

4.1.4.1 Key Recovery through KRA

The WidePoint NFI KRA shall provide access to a copy of an escrowed key only in response to a properly authenticated and authorized key recovery request. Such access shall require the

Practice Note: A combination of physical, procedural and technical security controls shall be used to enforce continuous two-person control during recovery and delivery of escrowed keys. The WidePoint NFI KRS shall be designed to maximize the ability to enforce two-person control technically.

actions of at least two WidePoint NFI KRAs. All copies of escrowed keys shall be protected using two-person control procedures during recovery and delivery to the authenticated and authorized Requestor. Split key or password procedures are considered adequate two-person controls.
The strength of the confidentiality provided by the delivery mechanism for copies of escrowed keys shall be equal to or greater than that provided by the key being protected.

4.1.4.2 Automated Self-Recovery

A current Subscriber’s escrowed keys may be provided directly to the Subscriber without imposition of two-person control requirements. The WidePoint NFI KED shall only provide escrowed keys to current Subscribers without two-person control upon:

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

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

- Ensuring that the escrowed keys are being sent only to the authenticated Subscriber associated with the escrowed keys; and
- Ensuring that the escrowed keys are encrypted during transmission using cryptography of equal or greater strength than provided by the escrowed keys.

4.1.4.3 Key History Recovery to Hardware Token

When a subscriber is issued a new certificate on a hardware token, prior encryption keys for the subscriber may be recovered as part of the issuance process as long as the WidePoint NFI KED uses secure means, such as Global Platform Secure Channel Protocol (SCP), to inject the key history onto the hardware token directly. The hardware token shall meet FIPS 140-2 Level 2 hardware requirements and the key history shall be injected into the card such that it is not thereafter exportable. The KED shall notify subscribers of all attempts to recover the subscriber’s escrowed keys during token issuance.

4.2 CERTIFICATE APPLICATION PROCESSING

An applicant for a Widepoint NFI PKI Certificate shall complete a Certificate application and provide requested information in a form prescribed by the WidePoint NFI CA and this CP. Information in the certificate application shall be verified as accurate before certificates are issued as specified in Section 3.2.

4.2.1 Performing Identification and Authentication Functions

The identification and authentication of the Subscriber shall meet the requirements specified for Subscriber authentication in Sections 3.2 and 3.3. The components of the WidePoint NFI CAs responsible for authenticating the Subscriber's identity in each case are specified in Section 1.3.

4.2.2 Approval or Rejection of Certificate Applications

Applications for all Certificates shall be approved only after successful completion of verification and authentication of the identity of the applicant.

WidePoint NFI CAs may suspend or end the current applicant registration process, as determined by the WidePoint NFI CA, and shall, at a minimum, provide the following verification information to the certificate applicant:

- Indicate failure of identity verification process
- Inform the applicant of the process necessary to resume processing

The WidePoint NFI shall record the following transaction data:

- Applicant's name as it appears in the applicant's request for a certificate
- Method of application (i.e., online, in-person) for each data element accepted for proofing, including electronic forms
- Name of document presented for identity proofing
- Issuing authority
- 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., in-person)
- Date/time of verification
- Names of the individual completing the identity verification
- Fields that failed verification
- Status of current registration process (suspended, ended, etc.)
- All identity verification data
- All associated error messages and codes
- Date/time of process completion or suspension

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions during Certificate Issuance

At the time the Subscriber applies for a certificate, the WidePoint NFI CA shall authenticate itself to the applicant prior to collecting any identity information. Upon issuance of a Certificate, the WidePoint NFI CA warrants to all Program Participants that:

- The WidePoint NFI CA will manage the Certificate in accordance with the requirements in this CP.
- The WidePoint NFI CA has complied with all requirements in this CP when identifying the Subscriber and issuing the Certificate.
- There are no misrepresentations of fact in the Certificate known to the WidePoint NFI CA and the WidePoint NFI CA has verified the information in the Certificate. It is the responsibility of the WidePoint NFI CA to verify the source of the certificate request, and to ensure that Subscriber information submitted in the application process is correct and accurate. Information will be verified to ensure legitimacy as per Section 3.2, Initial Identity Validation.
- Information provided by the Subscriber for inclusion in the Certificate has been accurately transcribed to the Certificate.
- The Certificate meets the material requirements of this CP.

While the Subscriber may do most of the data entry, it is still the responsibility of the WidePoint NFI CA to verify that the information is correct and accurate. This may be accomplished either through a system approach linking databases containing personal information, other equivalent authenticated mechanisms, or through personal contact with the Subscriber's sponsoring organization. If databases are used to confirm Subscriber attributes, then these databases must be protected from unauthorized modification to a level commensurate with the level of assurance specified for the certificates conveying the Subscriber attributes.

Public keys shall be delivered to the certificate issuer in a way that binds the applicant's verified identification to the public key being certified. This binding shall be accomplished using means that are as secure as the security offered by the keys being certified. The binding shall be accomplished using cryptographic, physical, procedural, and other appropriate methods. The methods used for public key delivery shall be stipulated in the WidePoint NFI CA's CPS.

In those cases where public/private key pairs are generated by the WidePoint NFI CA on behalf of the Subscriber, the WidePoint NFI CA shall implement secure mechanisms to ensure that the token on which the public/private key pair is held is securely sent to the proper Subscriber, and that the token is not activated prior to receipt by the proper Subscriber.

WidePoint NFI CAs shall verify the source of a certificate request before issuance.

4.3.2 Notification to Subscriber of Certificate Issuance

Upon successful completion of the Subscriber identification and authentication process in accordance with this CP, the WidePoint NFI CA shall create the requested Certificate, notify the applicant thereof, and make the Certificate available to the applicant. The WidePoint NFI CA shall use an out-of-band notification process linked to the Certificate applicant's physical U.S. postal mail address, or equivalent, and deliver the Certificate only to the Subscriber.

4.4 CERTIFICATE ACCEPTANCE

Prior to issuing the Certificate by the WidePoint NFI CA, the Subscriber shall indicate and agree to the Subscriber obligations under Section 9.6.3, Subscriber Representations and Warranties.

4.4.1 Conduct Constituting Certificate Acceptance

Prior to issuing the Certificate, the Subscriber shall indicate acceptance or rejection of the Certificate to the WidePoint NFI CA. By accepting the Certificate, the Subscriber is warranting that all information and representations made by the Subscriber that are included in the Certificate are true. In the absence of an overt indication of acceptance, failure to object to the certificate or its contents will constitute acceptance of the certificate.

4.4.2 Publication of the Certificate by the WidePoint NFI CA

As specified in Section 2.2.1, Publication of Certificates and Certificate Status, WidePoint NFI CA certificates shall be maintained and published in a repository and made available to the public and Relying Parties.

4.4.3 Notification to FBCA 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 shall be included in the MOA between the Widepoint NFI PKI and the FBCA. The notification will assert 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

4.5.1 Subscriber Private Key and Certificate Usage

The responsibilities of each applicant for a Certificate are to:

- Provide complete and accurate responses to all requests for information made by the WidePoint NFI CA (or an authorized RA) during the applicant registration, certificate application, and authentication of identity processes
- Generate a key pair using a reasonably trustworthy system, and take reasonable precautions to prevent any compromise, modification, loss, disclosure, or unauthorized use of the private key

- Upon issuance of an Certificate naming the applicant as the Subscriber, review the Certificate to ensure that all Subscriber information included in it is accurate, and to expressly indicate acceptance or rejection of the Certificate
- Use the Certificate and the corresponding private key exclusively for purposes authorized by this Policy and only in a manner consistent with this Policy
- Instruct the issuing WidePoint NFI CA (or an authorized RA) to revoke the Certificate promptly upon any actual or suspected loss, disclosure, or other compromise of the private key, or, in the case of and Government Employee Certificates, whenever the Subscriber is no longer affiliated with the Sponsoring Organization
- Respond as required to notices issued by the WidePoint NFI CA

Subscribers who receive certificates from a WidePoint NFI CA shall comply with these CP requirements.

Restrictions in the intended scope of usage for a private key are specified through certificate extensions, including the key usage and extended key usage extensions, in the associated certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each Relying Party for each application and is not controlled by this CP.

Parties who rely upon the certificates issued under this CP should preserve original signed data, the applications necessary to read and process those data, and the cryptographic applications needed to verify the digital signatures on those data for as long as it may be necessary to verify the signature on that data.

4.6 CERTIFICATE RENEWAL

Certificate renewal consists of issuing a new certificate with a new validity period and serial number while retaining all other information in the original certificate, including the public key.

After certificate renewal, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.6.1 Circumstance for Certificate Renewal

A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the Subscriber name and attributes are unchanged. In addition, the validity period of the certificate must meet the requirements specified in Section 6.3.2, Certificate Operational Periods and Key Usage Periods.

Certificates may also be renewed when a WidePoint NFI CA re-keys.

4.6.2 Who May Request Renewal

Requests for certificate renewal shall only be accepted from subscribers, sponsoring organizations, or RAs on behalf of subscribers and sponsoring organizations. Additionally, WidePoint NFI CAs may perform renewal of subscriber certificates without a corresponding request, such as when the CA re-keys.

4.6.3 Processing Certificate Renewal Requests

WidePoint NFI CAs shall accept Certificate renewal requests from their Subscribers within 90 days from the scheduled end of the operational period (expiration date) of the Certificate, provided the Certificate is not revoked, suspended, or expired. Certificates may be renewed in one, two, and three-year increments, in accordance with Section 3.3.2, Identification and Authentication for Renewal.

4.6.4 Notification of New Certificate Issuance to Subscriber

WidePoint NFI CAs shall notify subscribers of new certificate issuance in accordance with the notification processes specified in Section 4.3.2, Notification to Subscriber of Certificate Issuance.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Conduct constituting acceptance of a renewed certificate shall be in accordance with the processes specified in Section 4.4.1, Conduct Constituting Certificate Acceptance.

4.6.6 Publication of the Renewal Certificate by the WidePoint NFI CA

Publication of all renewed WidePoint NFI CA certificates shall be in accordance with section 4.4.2, Publication of the Certificate by the WidePoint NFI CA.

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

WidePoint NFI CAs shall provide notification of certificate issuance to other inter-organizations entities in accordance with the notification processes specified in Section 4.4.3, Notification of Certificate Issuance by the WidePoint NFI CA to Other Entities.

4.7 CERTIFICATE RE-KEY

Re-keying a certificate consists of creating new certificates with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key.

Subscribers of Entity CAs shall authenticate themselves for the purpose of re-keying as required in Section 3.3.1, Identification and Authentication for Routine Re-Key.

After certificate re-key, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.7.1 Circumstance for Certificate Re-Key

Certificate re-keying shall be accomplished through the limitation on certificate renewals. The minimum requirement for all certificate re-keying, with the exception of the WidePoint NFI CA certificates, shall be once every three years, in accordance with Section 6.3.2, Certificate Operational Periods and Key Usage Periods.

4.7.2 Who May Request Certification of a New Public Key

For WidePoint NFI CAs that support re-key, such requests shall only be accepted from the subject of the certificate or PKI Sponsors. Additionally, CAs and RAs may initiate re-key of a subscriber’s certificates without a corresponding request.

Subscribers with a currently valid certificate may request certification of a new public key. WidePoint NFI CA s, sponsoring organizations, and RAs may request certification of a new public key on behalf of subscribers.

4.7.3 Processing Certificate Re-Key Requests

Before processing certificate re-key requests, the WidePoint NFI CA shall identify and authenticate the subscriber in accordance with Section 3.2, Initial Identity Validation, and Section 3.3., Identification & Authentication for Re-Key and Renewal.

4.7.4 Notification of New Certificate Issuance to Subscriber

WidePoint NFI CAs shall notify subscribers of new certificate issuance in accordance with the notification processes specified in Section 4.3.2, Notification to Subscriber of Certificate Issuance.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Conduct constituting acceptance of a re-keyed certificate shall be in accordance with the processes specified in Section 4.4.1, Conduct Constituting Certificate Acceptance.

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

Publication of the re-keyed WidePoint NFI CA certificate shall be in accordance with Section 4.4.2, Publication of the Certificate by the WidePoint NFI CA.

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

WidePoint NFI CAs shall provide notification of certificate issuance to other inter-organizations entities in accordance with the notification processes specified in Section 4.4.3, Notification of Certificate Issuance by the WidePoint NFI CA to Other Entities.

4.8 MODIFICATION

Certificate modification consists of creating new certificates with subject information (e.g., a name or email address) that differs from the old certificate. For example, a WidePoint NFI CA may perform certificate modification for a Subscriber whose characteristics have changed (e.g., has just received a medical degree). The new certificate may have the same or different subject public key.

After certificate modification, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.8.1 Circumstance for Certificate Modification

WidePoint NFI CAs may modify their own CA certificate or OCSP responder certificate whose characteristics have changed (e.g., assert new policy OID). The new certificate may have the same or a different subject public key.

A WidePoint NFI CAs may perform certificate modification for a subscriber whose characteristics have changed (e.g., name change due to marriage). The new certificate shall have a different subject public key.

4.8.2 Who May Request Certificate Modification

Subscribers with a currently valid certificate may request certificate modification. WidePoint NFI CA s, sponsoring organizations, and RAs may request certificate modification on behalf of subscribers.

4.8.3 Processing Certificate Modification Requests

Proof of all subject information changes must be provided to the WidePoint NFI CA and verified before the modified certificate is issued.

4.8.4 Notification of New Certificate Issuance to Subscriber

WidePoint NFI CAs shall notify subscribers of new certificate issuance in accordance with the notification processes specified in Section 4.3.2, Notification to Subscriber of Certificate Issuance.

4.8.5 Conduct Constituting Acceptance of a Modified Certificate

Conduct constituting acceptance of a modified certificate shall be in accordance with the processes specified in Section 4.4.1, Conduct Constituting Certificate Acceptance.

4.8.6 Publication of the Modified Certificate by the WidePoint NFI CA

Publication of the modified WidePoint NFI CA certificate shall be in accordance with section 4.4.2, Publication of the Certificate by the WidePoint NFI CA.

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

WidePoint NFI CAs shall provide notification of certificate issuance to other inter-organizations entities in accordance with the notification processes specified in Section 4.4.3, Notification of Certificate Issuance by the WidePoint NFI CA to Other Entities.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

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

For certificates asserting id-orc-nfissp-medium, id-orc-nfissp-mediumHardware, id-orc-nfissp-device, id-orc-nfissp-deviceHardware, id-orc-nfissp-pivi-hardware, id-orc-nfissp-pivi-cardAuth, or id-orc-nfissp-pivi-contentSigning, WidePoint NFI CAs shall publish CRLs. Revocation requests must be authenticated. Requests to revoke or suspend a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised.

WidePoint NFI CAs shall 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 shall be checked before posting to ensure that all information is correct.

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.

Certificates associated with the recovered private keys shall not be revoked simply because of key recovery. This does not prohibit subscribers from revoking their own certificates for any reason.

4.9.1 Circumstances for Revocation

For WidePoint NFI CAs, a certificate shall 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 (3) circumstances under which certificates issued by a WidePoint NFI CA may be revoked:

- The first circumstance is when the WidePoint PKI Policy Authority requests a WidePoint NFI-issued certificate be revoked. This will be the normal mechanism for revocation in cases where the WidePoint 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 WidePoint 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 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 or other personnel as designated by the WidePoint CSO.

The WidePoint PKI Policy Authority shall meet as soon as practicable to review the emergency revocation.

WidePoint NFI CAs that implement certificate revocation shall revoke certificates upon receipt of sufficient evidence of compromise or loss of the subscriber's corresponding private key.

WidePoint NFI CAs that implement certificate revocation shall, at a minimum, revoke certificates for the reason of key compromise upon receipt of an authenticated request from an appropriate entity and the associated certificate being revoked shall be placed on the CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

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

4.9.1.1 Permissive Revocation

A Subscriber may request revocation of his/her/its Certificate at any time for any reason. A Sponsoring Organization may request revocation of a Certificate issued to its Employee at any time for any reason.

4.9.1.2 Required Revocation

A Subscriber or a Sponsoring Organization (where applicable), is responsible for promptly requesting revocation of a Certificate:

- When any of the identifying information or affiliation components of any names and other information in the certificate (e.g., privilege attributes asserted) become invalid
- When the private key, or the media holding the private key, associated with the Certificate is, or is suspected of having been, compromised
- When the individual named as an Employee no longer represents, or is no longer affiliated with, the Sponsoring Organization
- When the Subscriber can be shown to have violated the stipulations of the subscriber agreement
- The Subscriber or other authorized party (as defined in the WidePoint NFI CA's CPS) asks for his/her certificate to be revoked

Failure to request revocation under these circumstances is at the Subscriber's risk.

The WidePoint NFI CA shall revoke the certificate:

- If the private key is suspected of compromise
- If the Subscriber can be shown to have violated the stipulations of its Subscriber agreement
- If WidePoint learns, or reasonably suspects, that the Subscriber's private key has been compromised
- If the issuing WidePoint NFI CA determines that the Certificate was not properly issued in accordance with this Policy and/or the WidePoint NFI CA's CPS

Whenever any of the above circumstances occur, the WidePoint NFI CAs shall include all revoked certificates in all new publications of certificate status information until the certificate expires.

4.9.2 Who Can Request Revocation

The only persons permitted to request revocation of a Certificate issued pursuant to this CP are the Subscriber, the Sponsoring Organization (where applicable), and the issuing WidePoint NFI CA or RA.

4.9.3 Procedure for Revocation Request

A Certificate revocation request should be promptly communicated to the issuing WidePoint NFI CA, either directly or through the RA authorized to accept such notices on behalf of the WidePoint NFI CA. WidePoint NFI CAs shall revoke certificates upon receipt of sufficient evidence of compromise or loss of the subscriber's corresponding private key. A Certificate revocation request may be communicated electronically if it is digitally signed with the private key of the Subscriber or the Sponsoring Organization (where applicable). Alternatively, the Subscriber, or Sponsoring Organization (where applicable), may request revocation by contacting the issuing WidePoint NFI CA or its RA in person and providing adequate proof of identification in accordance with this CP.

The procedure to request the revocation of a certificate shall identify the certificate to be revoked, identify the reason for revocation, and authenticate the identity of the individual making the request. If the revocation is being requested for reason of key compromise or suspected fraudulent use, then the Subscriber's or the RA's revocation request must so indicate. If a RA makes a revocation request on behalf of a Subscriber, a formal, signed message format known to the CA shall be employed. All requests shall be authenticated (e.g., digitally or manually signed). For signed requests from the certificate subject, or from an RA, verification of the signature is sufficient.

Where Subscribers using hardware tokens, (e.g., applications, Employees) end their relationship with a sponsoring organization, they shall, prior to departure, surrender to the organization (through any accountable mechanism) all cryptographic hardware tokens that were issued by or on behalf of the sponsoring organization. The token shall be zeroized or destroyed promptly upon surrender and shall be protected from malicious use between surrender and zeroization or destruction. If the Subscriber leaves an organization and the hardware tokens cannot be obtained, then all certificates associated with the unretrieved tokens shall be immediately revoked.

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

WidePoint NFI CAs (or delegate) shall collect and destroy PIV-I Cards from Subscribers whenever the cards are no longer valid, whenever possible. WidePoint NFI CAs (or delegate) shall record destruction of PIV-I Cards.

4.9.4 Revocation Request Grace Period

There is no grace period for a certificate revocation request.

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

The WidePoint NFI CAs shall revoke certificates as quickly as practical upon receipt of a valid revocation request. Revocation requests shall be processed before the next CRL is published or status made available via OCSP, excepting those requests validated within two hours of publication. Revocation requests validated within two hours of publication shall be processed before the following publication.

4.9.6 Revocation Checking Requirements for Relying Parties

Use of revoked certificates could have damaging or catastrophic consequences. The matter of how often new revocation data should be obtained is a determination to be made by the Relying

Party, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed.

4.9.7 CRL Issuance Frequency

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

CRLs shall be published periodically, even if there are not changes to be made, to ensure timeliness of information. CRLs may be issued more frequently than specified below.

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

For WidePoint NFI CAs that are operated in an off-line manner, routine CRLs may be issued less frequently than specified above if the WidePoint NFI CA only issues:

- CA Certificates
- (Optionally) CSS certificates, and
- (Optionally) end user certificates solely for the administration of the WidePoint NFI CA

However, the interval between routine CRLs shall not exceed 31 days.

WidePoint
All WidePoint NFI CAs must meet the requirements specified in section 4.9.12, Special Requirements Related to Key Compromise, for issuing Emergency CRLs.

4.9.8 Maximum Latency of CRLs

CRLs shall be published within four (4) hours of generation. Each CRL shall be published no later than the time specified in the *nextUpdate* field of the previously issued CRL for the same scope.

4.9.9 Online Revocation/Status Checking Availability

WidePoint NFI CAs shall validate online, near-real-time the status of the Certificates indicated in a Certificate validation request message via OCSP. The status information must be updated and available to relying parties within 24 hours of revocation.

The latency of certificate status information distributed by the WidePoint NFI CA or their delegated status responders must meet or exceed the requirements for CRL issuance as stated in 4.9.7, CRL Issuance Frequency.

All WidePoint NFI CAs shall use OCSP and CRLs (following RFC 2560) to distribute status information.

4.9.10 Online Revocation Checking Requirements

Use of revoked certificates could have damaging or catastrophic consequences. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed.

4.9.11 Other Forms of Revocation Advertisements Available

WidePoint NFI CAs may also use other methods to publicize the certificates it has revoked. Any alternative method must meet the following requirements:

- The alternative method must be described in the WidePoint NFI CA's approved CPS.
- The alternative method must provide authentication and integrity services commensurate with the assurance level of the certificate being verified.
- The alternative method must meet the issuance and latency requirements for CRLs stated in Sections 4.9.7, CRL Issuance Frequency, and 4.9.8, Maximum Latency of CRLs.

4.9.12 Special Requirements Related to Key Compromise

For WidePoint NFI CAs, when a CA certificate is revoked or Subscriber certificate is revoked because of compromise, or suspected compromise, of a private key, a CRL must be issued as specified below:

Assurance Level	Maximum Latency for Emergency CRL Issuance
Medium (all policies)	18 hours after notification
PIV-I Card Authentication	18 hours after notification

Table 7. Maximum Latency for Emergency CRL Issuance by Assurance Level

4.9.13 Circumstances for Suspension

Suspension shall not be used by the WidePoint NFI CA.

4.9.14 Who can Request Suspension

Suspension shall not be used by the WidePoint NFI CA.

4.9.15 Procedures for Suspension Request

Suspension shall not be used by the WidePoint NFI CA.

4.9.16 Limits on Suspension Period

Suspension shall not be used by the WidePoint NFI CA.

4.10 CERTIFICATE STATUS SERVICES

All WidePoint NFI CAs shall use OCSP and CRLs to distribute status information. To the extent practical, the contents of changes in status shall be checked before posting to ensure that all information is correct.

4.10.1 Operational Characteristics

WidePoint NFI CAs shall validate the online, near-real-time the status of the Certificate indicated in a Certificate validation request message in accordance with OCSP [RFC 2560].

4.10.2 Service Availability

See Section 2.2.1, Publication of Certificates and Certificate Status.

4.10.3 Optional Features

No stipulation.

4.11 END OF SUBSCRIPTION

No stipulation.

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

Subscriber key management keys (e.g., encryption, decryption) may be escrowed to provide key recovery. WidePoint NFI CAs that support private key escrow for key management keys shall document their key recovery practices and identify that document in their CPS and/or other referenced documents. Escrowed keys shall be protected at no less than the level of security in which they are generated, delivered, and protected by the subscriber.

Under no circumstances shall a subscriber signature key be held in trust by a third party.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

WidePoint NFI CAs that support session key encapsulation and recovery shall document the practices and identify that document in their CPS.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

Each WidePoint NFI CA, and all associated CMSs, RAs, CMAs, KRS components, and Repositories, shall implement appropriate physical security controls and restrict access to the hardware and software (including the server, workstations, and any cryptographic software and hardware modules or tokens) used in connection with providing WidePoint NFI CA services at all times to protect against theft, loss, and unauthorized use. Access to such hardware and software shall be limited to those personnel performing in a Trusted Role. All the physical control requirements specified for the CA apply to the CMS as well.

The WidePoint NFI CA's physical and environmental security program shall address access controls, water exposures, fire safety, failure of supporting utilities, media storage, waste disposal, off-site backup capabilities, structural collapse, interception of data, and mobile and portable systems, in accordance with regulations, and other supporting security guidelines cited in this CP.

5.1.1 Site Location and Construction

WidePoint NFI CAs shall implement the physical security requirements in accordance with WidePoint security guidelines, as follows:

- The location and construction of the facility housing the WidePoint NFI CA equipment shall be consistent with facilities used to house high value, sensitive information.
- The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors shall provide robust protection against unauthorized access to WidePoint NFI CA equipment and records.

5.1.2 Physical Access

The WidePoint NFI CA shall provide physical access controls designed to provide protections against unauthorized access to system resources.

5.1.2.1 Physical Access for CA Equipment

Physical security of WidePoint NFI CA equipment shall encompass the following:

- WidePoint NFI CA, CMS, CSS and RA equipment shall always be protected from unauthorized access, and especially while the cryptographic module is installed and activated.
- Physical access controls shall be implemented to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the equipment environment.

- Ensure no unauthorized access to the hardware is permitted.
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers.
- Ensure that the physical site is manually or electronically monitored for unauthorized intrusion at all times.
- Ensure that an access log is maintained and inspected periodically
- Require two-person physical access control to both the cryptographic module and computer system.
- Restrict the entry and exit of personnel, equipment and media from any area containing a local area network (LAN) server.

Removable cryptographic modules, activation information used to access or enable cryptographic modules, and other sensitive CA and CSS equipment shall be placed in secure containers when not in use. Activation data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.

If the facility is left unattended, a security check of the facility housing WidePoint NFI CA, CMS and CSS equipment shall be conducted. At a minimum, this check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., cryptographic modules are in place when open, and secured when closed).
- Any security containers are properly secured.
- Physical security systems (e.g., door locks, vent covers) are functioning properly.
- The area is secured against unauthorized access.

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

5.1.2.2 Physical Access for RA Equipment

RA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. The RA shall implement physical access controls to reduce the risk of equipment tampering, even when the cryptographic module is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the RA equipment environment.

5.1.2.3 Physical Access for CSS Equipment

Physical access control requirements for CMS and CSS equipment (if implemented), shall meet the CA physical access requirements specified in Section 5.1.2.1, Physical Access for CA Equipment.

5.1.2.4 Physical Access for CMS Equipment

Physical access control requirements for CMS equipment containing a PIV-I Content Signing key shall meet the CA physical access requirements specified in Section 5.1.2.1.

5.1.3 Power and Air Conditioning

The WidePoint NFI CAs shall provide power and air conditioning in accordance with regulations, WidePoint policy, and other supporting WidePoint security guidelines cited in the this CP.

The WidePoint NFI CAs shall provide for backup power sources sufficient to supply uninterruptible operation, or backup capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. In addition, the CA directories (containing CA issued certificates, CRLs, and certificate status information) shall be provided with uninterrupted power sufficient for a minimum of six hours of operation in the absence of commercial power. WidePoint NFI CAs shall employ appropriate mechanisms to ensure availability of repositories as specified in Section 2.2.1, Publication of Certificates and Certificate Status.

5.1.4 Water Exposures

WidePoint NFI CA equipment shall be installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors).

Potential water exposure from fire prevention and protection measures (e.g., sprinkler systems) is excluded from this requirement.

5.1.5 Fire Prevention and Protection

The WidePoint NFI CAs shall provide fire prevention and protection in accordance with regulations, WidePoint policy, and other supporting WidePoint security guidelines cited in this CP.

5.1.6 Media Storage

WidePoint NFI CA media shall be stored so as to protect them from accidental damage (water, fire, electromagnetic) and shall be protected from unauthorized physical access.

5.1.7 Waste Disposal

The WidePoint NFI CAs shall provide waste disposal in accordance with regulations, WidePoint policy, and other supporting WidePoint security guidelines cited in this CP.

Sensitive media and documentation that are no longer needed for operations shall be destroyed in a secure manner (e.g., sensitive paper documentation shall be shredded, burned, or otherwise rendered unrecoverable).

5.1.8 Off-site Backup

Systems shall be in place for backing up electronic records that guard against the loss of records information because of equipment defects, human error, or theft. These backup procedures shall be properly documented, understood by IT personnel, and be integrated/coordinated with the organization’s disaster recovery plan.

Backups shall be performed by WidePoint NFI CAs and stored offsite not less than once per week. Weekly, monthly and yearly backup of magnetic media shall be rotated and transported to an offsite storage facility. Full system backups, sufficient to recover from system failure, shall be made on a periodic schedule, described in the WidePoint NFI CA’s CPS. At least one full backup copy shall be stored at an off-site location (separate from the WidePoint NFI CA equipment). Only the latest full backup need be retained.

Backup media will be stored at a secured alternate data storage site which meets physical and environmental security requirements commensurate to that of the operational WidePoint NFI CA, and which is sufficiently distant from the operating facility to provide adequate protection against major natural disasters (e.g., earthquakes and hurricanes).

5.2 PROCEDURAL CONTROLS

The WidePoint PKI Policy Authority is responsible and accountable for the operation of the WidePoint NFI PKI program.

5.2.1 Trusted Roles

WidePoint NFI CAs shall utilize commercially reasonable practices to ensure that one person acting alone cannot circumvent safeguards. To increase the likelihood that these roles can be successfully carried out, the functions are distributed among more than one person, so that any malicious activity would require collusion.

The requirements of this policy are defined in terms of four roles. These four roles are employed at the CA, RA, KED, and CSS locations, as appropriate:

> ***Administrator*** – authorized to install, configure, and maintain the CA; establish and maintain CA user accounts; configure profiles and audit parameters; and generate component keys.

Officer – authorized to request or approve certificates or certificate revocations; register new subscribers and request the issuance of certificates; verify the identity of subscribers and accuracy of information included in certificates.

Auditor – authorized to maintain audit logs; perform or oversee internal compliance audits to ensure that the CA is operated in accordance with its CPS.

Operator – authorized to perform system backup and recovery.

Some roles may be combined. The roles required for each level of assurance are identified in Section 5.2.4, Separation of Roles. Separation of duties shall comply with 5.2.4, and requirements for two person control with 5.2.2, regardless of the titles and numbers of Trusted Roles.

The following subsections provide a detailed description of the responsibilities for each role.

5.2.1.1 Administrator

The Administrator role is responsible for:

- Installation, configuration, and maintenance of the CA
- Establishing and maintaining CA system accounts
- Establishing and maintaining system accounts
- Configuring certificate profiles or templates and audit parameters
- Generating and backing up CA keys

Administrators do not issue certificates to Subscribers.

5.2.1.2 Officer

The Officer role is responsible for:

- Issuing certificates, that is:
  - Registering new Subscribers and requesting the issuance of certificates
  - Verifying the identity of Subscribers and accuracy of information included in certificates
  - Requesting, approving and executing the issuance of certificates
  - Requesting, approving and executing the revocation of certificates
- Key recovery

5.2.1.3 Auditor

The Auditor role is responsible for:

- Reviewing, maintaining, and archiving audit logs

- Performing or overseeing internal compliance audits to ensure that the WidePoint NFI CA is operating in accordance with its CPS

5.2.1.4 Operator

The Operator role is responsible for the routine operation of the CA equipment and operations such as system backups and recovery, or changing recording media.

5.2.2 Number of Persons Required per Task

Two or more persons are required per task for the following tasks:

- CA key generation
- CA signing key activation
- CA private key backup
- KED key generation
- KED private key backup

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

Under no circumstances shall a WidePoint NFI KRA perform a trusted role for a WidePoint NFI KED. Under no circumstances shall a WidePoint NFI KRA perform its own compliance audit function.

Physical access to the CAs does not constitute a task as defined in this section. Therefore, two-person physical access control may be attained as required in Section 5.1.2.1.

5.2.3 Identification and Authentication for Each Role

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

5.2.4 Separation of Roles

Individual personnel shall be specifically designated to the four roles defined in Section 5.2.1, Trusted Roles. Individuals may only assume one of the Officer, Administrator, and Auditor roles, but any individual may assume the Operator role. The CA, CMS and RA software and hardware shall identify and authenticate its users and shall ensure that no user identity can assume both the Administrator and the Officer roles, assume both the Administrator and Auditor roles, or assume both the Auditor and Officer roles. No individual shall have more than one identity.

5.3 PERSONNEL CONTROLS

Each WidePoint NFI CA and its RA, CMA, KED and its KRA, and Repository subcontractors shall formulate and follow personnel and management policies sufficient to provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties in a manner consistent with this CP.

Contractor personnel employed to perform functions pertaining to a WidePoint NFI CA shall meet applicable requirements set forth in this CP, the WidePoint NFI CPS, the WidePoint System Security Plan, and WidePoint policies, procedures, and guidelines cited in this CP. WidePoint shall take appropriate administrative and disciplinary actions against personnel who have performed unauthorized actions involving a WidePoint NFI CA or its repository.

5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity. Each person filling a trusted role must satisfy at least one of the following:

- The person shall be a citizen of the country where the CA is located; or
- For WidePoint NFI CAs operated on behalf of multinational governmental organizations, the person shall be a citizen of one of the member countries; or
- For WidePoint NFI CAs located within the European Union, the person shall be a citizen of one of the member States of the European Union; or
- The person shall have a security clearance equivalent to U.S. Secret or higher issued by a NATO member nation or major non-NATO ally as defined by the International Traffic in Arms Regulation (ITAR) – 22 CFR 120.32; or
    - For RA personnel only, in addition to the above, the person may be a citizen of the country where the RA is located.

For the Authorized WidePoint NFI trusted roles that have been issued current valid Federal employee certificates, all trusted roles are required to be held by U.S. citizens.

The requirements governing the qualifications, selection, and oversight of individuals who operate, manage, oversee, and audit the WidePoint NFI CA shall be set forth in the CPS.

5.3.2 Background Check Procedures

WidePoint NFI CA personnel shall, at a minimum, pass a background investigation covering the following areas:

- Employment
- Education
- Place of residence
- Law Enforcement
- References

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

Adjudication of the background investigation shall be performed by a competent adjudication authority using a process consistent with Executive Order 12968 August 1995, or equivalent.

If a formal clearance or other check is the basis for background check, the background refresh shall be in accordance with the corresponding formal clearance or other check. Otherwise, the background check shall be refreshed every ten years.

5.3.3 Training Requirements

All WidePoint NFI CAs shall provide for the mandatory periodic training in all operational duties, computer security awareness and accepted computer security practices of all employees who are involved with the management, use, or operation of the WidePoint NFI CA computer system. All personnel shall receive appropriate security briefings upon arrival and before beginning their assigned duties.

All security awareness and training programs shall be developed and implemented in accordance with Federal laws, regulations, and guidelines, as well as WidePoint security policy and supporting security guidelines (See Appendix B).

All personnel performing duties with respect to the operation of the WidePoint NFI CA shall receive training, or demonstrate competence, in the following areas:

- CA/RA security principles and mechanisms
- All PKI software versions in use on the CA system
- All PKI duties they are expected to perform
- Disaster recovery and business continuity procedures
- Stipulations of this CP

Documentation shall be maintained identifying all personnel who received training and the level of training completed. Where competence was demonstrated in lieu of training, supporting documentation shall be maintained.

5.3.4 Retraining Frequency and Requirements

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

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

5.3.5 Job Rotation Frequency and Sequence

Any job rotation frequency and sequencing procedures shall provide for continuity and integrity of the WidePoint NFI CA services.

5.3.6 Sanctions for Unauthorized Actions

The WidePoint NFI CA shall take appropriate administrative and disciplinary actions against personnel who have performed actions involving the CA or it's RAs that are not authorized in this CP, WidePoint NFI CA CPS, Federal regulations, or WidePoint policies, procedures, and guidelines.

5.3.7 Independent Contractor Requirements

All personnel employed to perform WidePoint NFI CA functions are subject to all personnel requirements stipulated in this CP.

WidePoint NFI CAs shall establish procedures to ensure that any subcontractors perform in accordance with this CP and the WidePoint NFI CA CPS.

5.3.8 Documentation Supplied to Personnel

The WidePoint NFI CA shall make available to its CA and RA personnel this CP, relevant portions of the CPS, and any relevant statutes, policies, and guidelines. Documentation sufficient to define duties and procedures for each trusted role shall be provided to the personnel filling that role.

5.4 AUDIT LOGGING PROCEDURES

Audit logs for all security events on each WidePoint NFI CA and KED system shall be generated. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained securely and in accordance with Section 5.5.2, Retention Period for Archive.

5.4.1 Types of Events Recorded

All security auditing capabilities of the WidePoint NFI CA and KED operating system and WidePoint NFI CA and KED applications shall be enabled during installation.

At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event
- The date and time the event occurred
- A success or failure indicator when executing the WidePoint NFI CA's signing process
- The identity of the entity and/or operator that caused the event

A message from any source requesting an action by the WidePoint NFI CA is an auditable event; the corresponding audit record must also include message date and time, source, destination, and contents.

All security auditing capabilities of the WidePoint NFI CA operating system and WidePoint NFI CA applications required by this CP shall be enabled. As a result, most of the events identified below shall be automatically recorded. Where events cannot be automatically recorded, the WidePoint NFI CA shall implement manual procedures to satisfy this requirement.

SECURITY AUDIT:

- Any changes to the Audit parameters, e.g., audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs
- Obtaining a third-party time-stamp

IDENTIFICATION AND AUTHENTICATION:

- Successful and unsuccessful attempts to assume a role
- The value of maximum authentication attempts is changed
- Maximum unsuccessful authentication attempts occur during user login
- An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
- An Administrator changes the type of authenticator, e.g., from password to biometrics

LOCAL DATA ENTRY:

- All security-relevant data that is entered in the system

REMOTE DATA ENTRY:

- All security-relevant messages that are received by the system

DATA EXPORT AND OUTPUT:

- All successful and unsuccessful requests for confidential and security-relevant information

KEY GENERATION:

Whenever the CA generates a key (not mandatory for single session or one-time use symmetric keys)

PRIVATE KEY LOAD AND STORAGE:

- The loading of Component private keys
- All access to certificate subject private keys retained within the CA for key recovery purposes

TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE:

- All changes to the trusted public keys, including additions and deletions

SECRET KEY STORAGE:

- The manual entry of secret keys used for authentication

PRIVATE AND SECRET KEY EXPORT:

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

CERTIFICATE REGISTRATION:

- All certificate requests

CERTIFICATE REVOCATION:

- All certificate revocation requests

CERTIFICATE STATUS CHANGE APPROVAL:

- The approval or rejection of a certificate status change request

CA CONFIGURATION:

- Any security-relevant changes to the configuration of the CA

ACCOUNT ADMINISTRATION:

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

CERTIFICATE PROFILE MANAGEMENT:

- All changes to the certificate profile

REVOCATION PROFILE MANAGEMENT:

- All changes to the revocation profile

CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT:

- All changes to the certificate revocation list profile

MISCELLANEOUS:

- Appointment of an individual to a trusted role
- Designation of personnel for multiparty control
- Installation of the operating system
- Installation of the CA
- Installing hardware cryptographic modules
- Removing hardware cryptographic modules
- Destruction of cryptographic modules
- System startup
- Logon attempts to CA applications
- Receipt of hardware/software
- Attempts to set passwords
- Attempts to modify passwords
- Backing up CA internal database
- Restoring CA internal database
- File manipulation (e.g., creation, renaming, moving)
- Posting of any material to a repository

- Access to CA internal database
- All certificate compromise notification requests
- Loading tokens with certificates
- Shipment of tokens
- Zeroizing tokens
- Re-key of the CA
- Configuration changes to the CA server involving:
    - Hardware
    - Software
    - Operating system
    - Patches
    - Security profiles

PHYSICAL ACCESS / SITE SECURITY:

- Personnel access to room housing CA
- Access to the CA server
- Known or suspected violations of physical security

ANOMALIES:

- Software error conditions
- Software check integrity failures
- Receipt of improper messages
- Misrouted messages
- Network attacks (suspected or confirmed)
- Equipment failure
- Electrical power outages
- Uninterruptible power supply (UPS) failure
- Obvious and significant network service or access failures
- Violations of certificate policy
- Violations of certification practice statement
- Resetting operating system clock

5.4.2 Frequency of Processing Log

Audit logs shall be reviewed at least once every two months.

Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the log. All significant events shall be explained in an audit log summary. Actions taken as a result of these reviews shall be documented.

A statistically significant set of security audit data generated by WidePoint NFI CA since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity. This amount shall be described in the WidePoint NFI CA CPS.

The WidePoint NFI CA shall implement procedures to ensure that the security audit data are transferred prior to overwriting or overflow of automated security audit log files.

5.4.3 Retention Period for Audit Logs

All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

For Medium and Medium Hardware Assurance, audit logs shall be retained on-site until reviewed, as well as being retained in the manner described below.
Audit logs shall be retained onsite for at least two months as well as being retained in the manner described below and in Section 5.5, Records Archive.

The individual who removes audit logs from the WidePoint NFI CA system shall be an official different from the individuals who, in combination, command a WidePoint NFI CA signature key.

5.4.4 Protection of Audit Logs

WidePoint NFI CA and KRS system configuration and procedures must be implemented together to ensure that:

- Only authorized persons have read access to the logs
- Only authorized persons may archive or delete audit logs
- Audit logs are not modified

The entity performing audit log archive need not have modify access, but procedures must be implemented to protect archived data from deletion or destruction prior to the end of the audit log retention period (note that deletion requires modification access).

The off-site storage location for audit logs shall be a safe, secure location separate from the WidePoint NFI CA and KRS equipment.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up at least monthly, and a copy of the audit log shall be sent off-site in accordance with the CPS on a monthly basis.

5.4.6 Audit Collection System (Internal vs. External)

The audit collection system may or may not be external to the WidePoint NFI CA and KRS systems. Audit processes shall be invoked at system or application startup, and cease only at system or application shutdown. Audit collection systems shall be configured such that security audit data are protected against loss (e.g., overwriting or overflow of automated log files). Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the WidePoint DAA shall determine whether to suspend WidePoint NFI CA operations until the problem is remedied.

5.4.7 Notification to Event-Causing Subject

There is no requirement to provide notice that an event was audited to the individual, organization, device or application that caused the event. No one, including the subscriber shall be notified of a third-party key recovery.

5.4.8 Vulnerability Assessments

The WidePoint NFI CAs will perform routine self-assessments of security controls for evidence of malicious activity.

Practice Note: The security audit data should be reviewed by the security auditor for events such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. Security auditors should check for continuity of the security audit data.

The KRA, system administrator, and other supporting personnel shall watch for attempts to violate the integrity of the KRS, including the equipment, physical location, and personnel. The audit logs shall be reviewed by the audit administrator for events such as repeated failed actions, requests for escrowed keys, attempted access of escrowed keys, unauthenticated requests, or other suspicious or unusual activity. The audit administrator shall also check for continuity of the audit log.

A statistically significant sample of KED audit records of successful key recoveries shall be reconciled against the KRA audit logs and requests. The objective of this reconciliation shall be to ensure that all key recoveries are being made by authorized parties and for legitimate reasons. All KED audit records of unsuccessful key recoveries shall be analyzed to determine the cause and to ensure that the KRS is operating correctly and securely and is not vulnerable to hacking and unauthorized users.

5.5 RECORDS ARCHIVE

The WidePoint NFI KRS shall follow the General Records Schedules established by the National Archives and Records Administration.

The WidePoint NFI KRS components (i.e., WidePoint NFI KED, WidePoint NFI KRA workstation) shall maintain a trusted archive of information they store and of transactions they carry out. The primary objective of the archive is reconstruction of key recovery activities, in case of dispute. Examples of disputes may include:

- Validation of key recovery request forms
- Validation of the identity of the recipient of a copy of the subscriber's escrowed key;
- Verification of authorization and need of requestor to obtain the escrowed key copy;
- Verification of transfer of custody of escrowed keys to authorized requestor; and
- Establishment of the circumstances under which a copy of the escrowed key was provided.

5.5.1 Types of Events Archived

The WidePoint NFI CA shall retain and archive all data. WidePoint NFI CA archive records shall be sufficiently detailed to establish the proper operation of the WidePoint NFI CA , or the validity of any certificate (including those revoked or expired) issued by the WidePoint NFI CA .

At a minimum, the following data shall be recorded for archive in accordance with each assurance level:

- CA accreditation (if applicable)
- Certificate policy
- Certification practice statement
- Contractual obligations
- Other agreements concerning operations of the CA
- System and equipment configuration
- Modifications and updates to system or configuration
- Certificate requests
- All certificates issued and/or published
- Record of CA re-key
- Compliance Auditor reports
- Any changes to the Audit parameters, e.g., audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs
- Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)
- All access to certificate subject private keys retained within the CA for key recovery purposes
- Security audit data (in accordance with Section 5.4.1, Types of Events Recorded)
- Revocation requests
- Subscriber identity authentication data (per Section 3.2.3, Authentication of Individual Identity)
- Documentation of receipt and acceptance of certificates (if applicable).

- Subscriber agreements
- Documentation of loading, shipping, receipt, and zeroizing of tokens
- All CRLs issued and/or published
- Other data or applications to verify archive contents
- Documentation required by compliance auditors
- All changes to the trusted public keys
- All routine certificate validation transactions
- Export of private keys
- Escrowed keys
- The approval or rejection of a certificate status change request
- Appointment of an individual to a Trusted Role
- Destruction of cryptographic modules
- All certificate compromise notifications
- Remedial action taken as a result of violations of physical security
- Violations of Certificate Policy
- Violations of Certification Practice Statement

5.5.2 Retention Period for Archive

The minimum retention period for archive records is ten (10) years and six (6) months. Applications required to process the archive data shall also be maintained for a period determined by the U.S. National Archives and Records Administration (NARA). Escrowed keys shall be maintained within the WidePoint NFI KED for a minimum of one year after the expiration of the associated public key certificate.

5.5.3 Protection of Archive

The archive media must be protected at least at the level required to maintain and protect all Subscriber information and data from disclosure, modification, or destruction.

No unauthorized user shall be permitted to write to, modify, or delete the archive. The WidePoint NFI CA shall maintain a list of people authorized to modify or delete the archive, and make this list available during CP compliance audits.

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site. Applications required to process the archive data shall also be maintained for a period determined by NARA.

Archive media shall be stored in a safe, secure storage facility separate from the WidePoint NFI CA itself.

5.5.4 Archive Backup Procedures

WidePoint NFI archive records shall be backed up. The WidePoint NFI CA's CPS and/or other referenced documents shall describe how archive records are backed up and managed.

5.5.5 Requirements for Time-Stamping of Records

WidePoint NFI CA and KRS archive records shall be automatically time-stamped as they are created. The WidePoint NFI CA CPS shall describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

5.5.6 Archive Collection System

The archival collection system shall be documented in the CPS.

5.5.7 Procedures to Obtain and Verify Archive Information

Procedures detailing how to create, verify, package, transmit, and store archive information shall be published in the WidePoint NFI CA CPS.

The contents of the archive shall not be released except as determined by the WidePoint DAA or as required by law; however, records of individual transactions may be released upon request of any Subscribers involved in the transaction or their legally recognized agents.

5.6 KEY CHANGEOVER

WidePoint NFI CAs shall provide for the extension and/or continuation of their self-signed root certificates prior to their expiration as directed in the applicable WidePoint NFI CA's CPS. WidePoint NFI CAs will have a plan in place for the extension and/or continuation of their self-signed root certificates prior to their expiration.

To minimize risk from compromise of the WidePoint NFI CA's private signing key, that key should be changed often. Upon key changeover, only the new key will be used for certificate signing purposes. The older valid certificate will be available to verify old signatures until all of the certificates signed using the associated private key have also expired. If the old private key is used to sign CRLs that contain certificates signed with that key, the old key must be retained and protected.

The WidePoint NFI CA's signing key shall have a validity period as described in Section 6.3.2, Certificate Operational Periods and Key Usage Periods.

> *When a WidePoint NFI CA updates its private signature key and thus generates a new public key, the WidePoint NFI CA shall notify all CAs, RAs, and subscribers that rely on the WidePoint NFI CA's certificate that it has been changed. When a WidePoint NFI CA that distributes self-signed certificates updates its private signature key, the WidePoint NFI CA shall generate key rollover certificates, where the new public key is signed by the old private key, and vice versa. This permits acceptance of newly issued certificates and CRLs without distribution of the new self-signed certificate to current users. WidePoint NFI CAs either must establish key rollover certificates or must obtain a new CA certificate for the new public key from the issuers of their current certificates.*

WidePoint NFI CAs cross certified with the FBCA must be able to continue to interoperate with the FBCA after the FBCA performs a key rollover, whether or not the FBCA DN is changed.

WidePoint NFI CAs either must establish key rollover certificates as described above or must obtain a new CA certificate for the new public key from the issuers of their current certificates

WidePoint NFI KED keys shall be changed when necessary to ensure they are at least as strong as the keys being protected.

A WidePoint NFI KRA shall be considered an end entity whose key shall be changed in accordance with the requirements set forth in this CP and the WidePoint NFI Certificate Practice Statement.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

The WidePoint DAA shall be notified if any WidePoint NFI CAs operating under this policy experiences the following:

- Suspected or detected compromise of the WidePoint NFI CA systems
- Suspected or detected compromise of a certificate status server (CSS) if:
  - The CSS certificate has a lifetime of more than 72 hours and
  - The CSS certificate cannot be revoked (e.g., an OCSP responder certificate with the id-pkix-ocsp-nocheck extension)
- Physical or electronic penetration of the WidePoint NFI CA systems
- Successful denial of service attacks on the WidePoint NFI CA components
- Any incident preventing the WidePoint NFI CA from issuing a CRL within 24 hours of the issuance of the previous CRL

The WidePoint NFI CA shall re-establish operational capabilities in accordance with WidePoint policies and guidelines and procedures as set forth in the WidePoint NFI CA's CPS.

In the event of an incident as described above, the WidePoint NFI will notify the FPKIMA within 24 hours of incident discovery, along with preliminary remediation analysis.

Within 10 business days of incident resolution, the WidePoint NFI will post a notice on its public web page identifying the incident and provide notification to the FPKIPA. The public notice will include the following:

1. Which WidePoint NFI components were affected by the incident
2. The WidePoint NFI's interpretation of the incident
3. Who is impacted by the incident
4. When the incident was discovered
5. A complete list of all certificates that were either issued erroneously or not compliant with the WidePoint NFI CP/CPS as a result of the incident
6. A statement that the incident has been fully remediated

The notification provided directly to the FPKIPA will also include detailed measures taken to remediate the incident.

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

All WidePoint NFI CAs will retain back-up storage media to facilitate restoration to full operation. When computing resources, software, and/or data are corrupted, the WidePoint NFI CA shall respond as follows:

- Before returning to operation, ensure that the system's integrity has been restored.
- If the WidePoint NFI CA signature keys are not destroyed**,** CA operation shall be reestablished, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in 4.9.7, CRL Issuance Frequency.
- If the WidePoint NFI CA signature keys are destroyed**,** CA operation shall be reestablished as quickly as possible, giving priority to the generation of a new CA key pair.

WidePoint DAA shall be notified as soon as possible.

In the event of an incident as described above, the WidePoint NFI will post a notice on its public web page identifying the incident and provide notification to the FPKIPA. See Section 5.7.1 for contents of the notice.

5.7.3 WidePoint NFI CA Private Key Compromise Procedures

Each WidePoint NFI CA must have in place an appropriate key compromise plan that addresses the procedures that will be followed in the event of a compromise of the private signing key used by a WidePoint NFI CA to issue Certificates. Such plan shall include procedures for (and documentation of) revoking all affected Certificates it has issued, and promptly notifying all Subscribers and all Relying Parties.

If the WidePoint NFI CA signature keys are compromised or lost (such that compromise is possible even though not certain):

- All affiliated entities and the WidePoint DAA shall be immediately informed, as well as any superior or cross-certified CAs and any entities known to be distributed the WidePoint NFI CA certificate (e.g., in a root store).
- The WidePoint NFI CA shall revoke all affected certificates it has issued.
- A new WidePoint NFI CA key pair shall be generated by the WidePoint NFI CA in accordance with Section 6.1.1, Key Pair Generation.
- New WidePoint NFI CA certificates shall be issued to subordinate CAs in accordance with the CPS.

- The WidePoint Board shall investigate and report what caused the compromise or loss and what measures have been taken to preclude recurrence.

If the WidePoint NFI CA distributed a Trusted Certificate, the WidePoint NFI CA shall perform the following operations:

- Generate a new Trusted Certificate.
- Securely distribute the new Trusted Certificate as specified in Section 6.1.4, WidePoint NFI CA Public Key Delivery to Relying Parties.
- Initiate procedures to notify subscribers of the compromise.

The WidePoint NFI Program Manager shall investigate what caused the compromise or loss, and what measures have been taken to preclude recurrence. This may include revocation of certificates associated with the compromised private keys stored in the WidePoint NFI KED.

The WidePoint NFI will post a notice on its public web page describing the compromise. See Section 5.7.1 for contents of the notice.

In the event that the WidePoint NFI KED is compromised or is suspected to be compromised, the FPKIPA shall be notified. The FPKIPA shall be granted sufficient access to information to determine the extent of the compromise.

If a WidePoint NFI KRA certificate is revoked due to compromise, the potential exists for some subscribers' escrowed keys to have been exposed during a recovery process. The audit administrator shall review the audit records to identify all potentially exposed escrowed keys. Each of the potentially exposed escrowed keys shall be revoked, according to procedures specified in the WidePoint NFI Certificate Practice Statement, Section 4.9.3, and the subscriber shall be notified of the revocation. It is recognized that this circumstance will constitute implicit notification to the subscriber of key recovery.

If a WidePoint NFI KRA certificate is revoked for any reason, but the WidePoint NFI KRA remains authorized to perform their duties, then the WidePoint NFI KRA shall request a new certificate from the WidePoint NFI PKI. The WidePoint NFI CA which revoked the WidePoint NFI KRA certificate shall ensure that all the requirements of the applicable CPS for revocation notification are met. The WidePoint NFI PKI shall follow the WidePoint NFI CPS for certificate issuance for the new WidePoint NFI KRA certificate.

5.7.4 Business Continuity Capabilities after a Disaster

WidePoint NFI CAs must have in place an appropriate disaster recovery/business resumption plan in accordance with guidelines provided by OMB Circular A-130, NIST SP 800-34, GSA Order 2100.1D, and all supporting WidePoint security guidelines. Such plan shall be detailed within the WidePoint NFI CA's CPS and other appropriate documentation made available to and approved by WidePoint.

The WidePoint NFI CA shall at the earliest feasible time securely advise [all affiliated and] member entities and the WidePoint DAA in the event of a disaster where the WidePoint NFI CA installation is physically damaged and all copies of the WidePoint NFI CA signature keys are destroyed.

WidePoint NFI CAs operating under this CP shall have recovery procedures in place to reconstitute the WidePoint NFI CA within 72 hours.

Relying parties may decide of their own volition whether to continue to use certificates signed with the destroyed private key pending reestablishment of the WidePoint NFI CA operation with new certificates.

WidePoint NFI KED may take more than 72 hours to restore depending on business needs.

5.7.5 Customer Service Center

WidePoint NFI CAs shall implement and maintain an a Customer Service Center to provide assistance and services to Subscribers and Relying Parties, and a system for receiving, recording, responding to, and reporting problems within its own organization and for reporting such problems to the WidePoint DAA. The WidePoint NFI CA shall ensure that there is a capability to provide help to subscribers when a security incident occurs in the system.

5.8 Authority Termination

5.8.1 CA or RA Termination

WidePoint NFI CAs shall perform the following in the event that the WidePoint NFI CA ceases operation or its participation as a WidePoint NFI CA or is otherwise terminated:

- All Subscribers, sponsoring organizations, and Relying Parties must be promptly notified of the cessation.
- All Certificates issued by a WidePoint NFI CA shall be revoked no later than the time of cessation.
- All current and archived identity proofing, certificate, validation, revocation/suspension, renewal, policy and practices, billing, and audit data shall be transferred to WidePoint within 24 hours of cessation and in accordance with this CP.
- Transferred data shall not include any non-WidePoint NFI data.

In the event that a WidePoint NFI CA terminates operation, the WidePoint DAA shall ensure that any certificates issued to that CA have been revoked.

WidePoint NFI CAs that have ceased issuing new certificates, and that are continuing to issue CRLs until all certificates have expired, are required to continue to conform to all relevant aspects of this CP (e.g., audit logging and archives).

In the event that a WidePoint NFI CA terminates operation, WidePoint shall provide notice to the FBCA and all affiliated entities prior to termination.

Whenever possible, the FPKIPA will be notified at least two weeks prior to the termination of any WidePoint NFI CA cross certified with the FBCA. For emergency termination, the WidePoint NFI will follow the notification procedures in Section 5.7.

5.8.2 KED Termination

Upon WidePoint NFI KED termination, the WidePoint NFI KRS shall provide archived data to an archive facility as specified in the WidePoint NFI CPS.

5.8.3 KRA Termination

Upon WidePoint NFI KRA termination, the WidePoint NFI KRS or WidePoint NFI KRA Organization shall take possession of all WidePoint NFI KRA archive records.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

6.1.1.1 WidePoint NFI CA Key Pair Generation

Cryptographic keying material used to sign certificates, CRLs or status information by WidePoint NFI CAs shall be generated in FIPS 140 Security Level 2 Hardware validated cryptographic modules or modules validated under equivalent international standards.

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

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

6.1.1.2 Subscriber Key Pair Generation

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

At the Medium-hardware assurance levels, subscriber key generation shall be performed using a validated hardware cryptographic module. For Medium and Basic assurance levels, either validated software or validated hardware cryptographic modules shall be used for key generation.

For PIV-I Hardware certificates, to be used for digital signatures and/or authentication, and PIV-I Card Authentication certificates, subscriber key generation shall be performed on hardware tokens that meet the requirements of Appendix A.

6.1.2 Private Key Delivery to Subscriber

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

When a WidePoint NFI CA or RA generates keys on behalf of the Subscriber, the private key must be delivered securely to the Subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases, the following requirements must be met:

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

The WidePoint NFI CA must maintain a record of the subscriber acknowledgement of receipt of the token.

6.1.3 Public Key Delivery to Certificate Issuer

The following requirements apply for WidePoint NFI CAs:

- Where key pairs are generated by the Subscriber or RA, the public key and the Subscriber’s identity must be delivered securely to the WidePoint NFI CA for certificate issuance in a way that ensures that:
    - It has not been changed during transit;
    - The sender possesses the private key that corresponds to the transferred public key; and
    - The sender of the public key is the legitimate user claimed in the certificate application.
- Subscriber public keys shall be delivered to the WidePoint NFI CA in a secure manner set forth in the WidePoint NFI CA’s CPS. If off-line means are used for public key delivery, they shall include identity checking as set forth in this CP and shall also ensure that proof of possession of the corresponding private key is accomplished.
- The delivery mechanism shall bind the Subscriber’s verified identity to the public key. If cryptography is used to achieve this binding, it must be at least as strong as the WidePoint NFI CA keys used to sign the certificate.

6.1.4 WidePoint NFI CA Public Key Delivery to Relying Parties

When a WidePoint NFI CA updates its signature key pair, the WidePoint NFI CA shall distribute the new public key in a secure fashion. The new public key may be distributed in a self-signed certificate, in a key rollover certificate, or in cross-certificates.

Self-signed certificates shall be conveyed to relying parties in a secure fashion to preclude substitution attacks. Acceptable methods for self-signed certificate delivery are:

- Loading a self-signed certificate onto tokens delivered to Relying Parties via secure mechanisms, such as:
  - The Trusted Certificate is loaded onto the token during the Subscriber's appearance at the RA.
  - The Trusted Certificate is loaded onto the token when the RA generates the Subscriber's key pair and loads the private key onto the token, which is then delivered to the Subscriber in accordance with Section 6.1.2.
- Secure distribution of self-signed certificates through secure out-of-band mechanisms
- Comparison of the hash of the self-signed certificate against a hash value made available via authenticated out-of-band sources (N.B. hashes posted in-band along with the certificate are not acceptable as an authentication mechanism).
- Loading certificates from Web sites secured with a currently-valid certificate of equal or greater assurance level than the certificate being downloaded.

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

Key rollover certificates are signed with the WidePoint NFI CA's current private key, so secure distribution is not required.

Practice Note: To ensure the availability of the new public key, the key rollover certificates shall be distributed using directories and other repositories.

6.1.5 Key Sizes

All approved algorithms shall be considered acceptable; additional restrictions on key sizes are detailed below:

For WidePoint NFI CAs that distribute self-signed certificates to Relying Parties, the WidePoint NFI CA's subject pubic keys in such certificates shall be at least 2048 bits for RSA, or at least 224 bits for ECDSA. For Those WidePoint NFI CAs that distribute self-signed certificates and whose key pairs were generated before September 13, 2005 may be 1024 bits for RSA.

WidePoint NFI CAs that generate certificates and CRLs under this policy shall use signature keys of at least 1024 bits for RSA or DSA, and at least 160 bits for ECDSA. Beginning

01/01/2011, all valid certificates shall be signed with keys of at least 2048 bits for RSA or at least 224 bits for ECDSA.

WidePoint NFI CAs that generate certificates and CRLs under this CP shall use the SHA-256, or SHA-384 hash algorithm when generating digital signatures. RSA signatures on certificates and CRLs that are issued after December 31, 2010, shall be generated using SHA-256. ECDSA signatures on certificates and CRLs that expire on or after December 31, 2010, shall be generated using SHA-256 or SHA-384, as appropriate for the key length. Signatures on certificates and CRLs that are issued after 12/31/2030 shall be generated using, at a minimum, SHA-256.

Where implemented, CSSs shall sign responses using the same signature algorithm, key size, and hash algorithm used by the WidePoint NFI CA to sign CRLs.

For WidePoint NFI CAs issuing certificates under this CP, end-entity certificates shall contain public keys that are at least 1024 bit for RSA, DSA, or Diffie-Hellman, or 160 bits for elliptic curve algorithms. The following special conditions also apply:

- End-entity certificates that include a keyUsage extension that only asserts the *digitalSignature* bit that expire on or after December 31, 2013, shall contain public keys that are at least 2048 bits for RSA or DSA, or 224 bits for elliptic curve algorithms.
- Beginning 01/01/2011, all valid end-entity certificates that include a keyUsage extension that asserts the *nonRepudiation*, *keyEncipherment*, *dataEncipherment*, or *keyAgreement* bit shall contain public keys that are at least 2048 bits for RSA, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms.
- Beginning 01/01/2011, all valid end-entity certificates that do not include a keyUsage extension shall contain public keys that are at least 2048 bits for RSA, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms.
- End entity certificates issued under WidePoint's NFI Polices that expire before January 1, 2014 shall contain RSA public keys that are 1024 or 2048 bits in length or elliptic curve keys that are 256 bits. End entity certificates issued under WidePoint's NFI Polices that expire on or after January 1, 2014 shall contain RSA public keys that are 2048 bits in length or elliptic curve keys that are 256 bits.

Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require a minimum of triple-DES or equivalent for the symmetric key, and at least 1024 bit RSA or equivalent for the asymmetric keys through 12/31/2010. Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum AES (128 bits) or equivalent for symmetric key, and at least 2048 bit RSA or equivalent for the asymmetric keys after 12/31/2010. All end-entity certificates associated with PIV-I shall contain public keys and algorithms that conform to [NIST SP 800-78].

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters for signature algorithms defined in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186.

Parameter quality checking (including primality testing for prime numbers) shall be performed in accordance with FIPS 186; additional tests may be specified by the WidePoint DAA.

Elliptic Curve public key parameters shall always be selected from the set specified in Section 7.1.3, Algorithm Object Identifiers.

6.1.7 Key Usage Purposes (as per X509 v3 Key Usage Field)

Public keys that are bound into certificates shall be certified for use in signing or encrypting, but not both, except as specified below. The use of a specific key is determined by the key usage extension in the X.509 certificate. All WidePoint certificates issued a policy OID cross certified with the PIV-I Hardware policy OID conform to [PIV-I Profile].

CA certificates issued by WidePoint NFI CAs shall set two key usage bits: *cRLSign* and/or *keyCertSign*. Where the subject signs OCSP responses, the certificate may also set the *digitalSignature* and/or *nonRepudiation* bits.

Subscriber certificates shall assert key usages based on the intended application of the key pair. In particular, certificates to be used for digital signatures (including authentication) shall set the *digitalSignature* and/or *nonRepudiation* bits. Certificates to be used for key or data encryption shall set the *keyEncipherment* and/or *dataEncipherment* bits. Certificates to be used for key agreement shall set the *keyAgreement* bit. For encryption certificates using a key encipherment mechanism, either the *keyEncipherment bit* or the *keyAgreement* bit shall be set to 1 and all other bits shall be 0. User certificates that assert WidePoint NFI Authentication or Card Authentication shall only assert the *digitalSignature* bit.
WidePoint NFI certificates asserting id-orc-nfissp-medium Assurance Level may include a single key for use with encryption and signature in support of legacy applications. Such dual-use certificates shall be generated and managed in accordance with their respective signature certificate requirements, except where otherwise noted in this CP. Such dual-use certificates shall never assert the non-repudiation key usage bit, and shall not be used for authenticating data that will be verified on the basis of the dual-use certificate at a future time. WidePoint NFI CAs are encouraged at all levels of assurance to issue Subscribers two key pairs, one for key management and one for digital signature and authentication.

6.2 PRIVATE KEY PROTECTION & CRYPTOGRAPHIC MODULE ENGINEERNG CONTROLS

6.2.1 Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is FIPS PUB 140, *Security Requirements for Cryptographic Modules.* Each WidePoint NFI CA, RA, and CMA will each protect its private key(s) in accordance with the provisions of this CP.

The WidePoint NFI PKI will use cryptographic modules that meet or exceed FIPS 140-1 or FIPS 140-2, Security Level 2 overall. 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.

Upon request, WidePoint NFI CAs shall provide at least FIPS 140-1 or FIPS 140-2, Level 3 validated cryptographic modules for key pair generation and storage of private keys.

The installation, removal, and destruction of all cryptographic modules shall be documented.

6.2.1.1 Custodial Subscriber Key Stores

Custodial Subscriber Key Stores hold keys for a number of Subscriber certificates in one location. When a collection of private keys for Subscriber certificates are held in a single location there is a higher risk associated with compromise of that cryptographic module than that of a single Subscriber. The WidePoint NFI does not offer custodial subscriber key stores with the exception of PIVI-Hardware encryption keys. PIVI-Hardware encryption keys are stored in accordance with the WidePoint NFI Key Recovery Policy and Key Recovery Practice Statements.

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

A single person shall not be permitted to activate or access any cryptographic module that contains the complete WidePoint NFI CA private signing key. Use of the WidePoint NFI CA private signing key shall require action by multiple parties, at a minimum under two-party control. WidePoint NFI CA signature keys may be backed up only under two-person control. Access to WidePoint NFI CA signing keys backed up for disaster recovery shall be under at least two-person control. The names of the parties used for two-person control shall be maintained on a list that shall be made available for inspection during compliance audits.

6.2.3 Private Key Escrow

6.2.3.1 Escrow of WidePoint NFI CA Private Signature Key

Under no circumstances shall a WidePoint NFI CA signature key used to sign certificates or CRLs be escrowed.

6.2.3.2 Escrow of WidePoint NFI CA Encryption Keys

No stipulation.

6.2.3.3 Escrow of Subscriber Private Signature Keys

Subscriber private signatures keys shall not be escrowed.

6.2.3.4 Escrow of Subscriber Private Encryption Keys

Subscriber key management keys may be escrowed to provide key recovery as described in Section 4.12.1, Key Escrow and Recovery Policy and Practices. Subscriber private dual use keys shall not be escrowed.

6.2.4 Private Key Backup

6.2.4.1 Backup of WidePoint NFI CA Private Signature Keys

The WidePoint NFI CA private signature keys shall be backed up under the same multi-person control as the original signature key. At least one copy of the private signature key shall be stored off-site. All copies of the WidePoint NFI CA private signature key shall be accounted for and protected in the same manner as the original. All access to certificate subject private keys retained within the WidePoint NFI CA for key recovery purposes must be documented. Hardware tokens containing WidePoint NFI CA private signature keys may be backed up in accordance with the security audit requires defined in this CP. Backup procedures shall be included in the WidePoint NFI CA's CPS.

6.2.4.2 Backup of Subscriber Private Signature Key

At the Medium-Hardware [PIV-I], Authentication or Card Authentication assurance levels, subscriber private signature keys may not be backed up or copied.

Backed up subscriber private signature keys shall not be stored in plaintext form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the Subscriber’s cryptographic module. Subscriber private signature keys may be backed up or copied, but must be held in the Subscriber’s control.

6.2.4.3 Backup of Subscriber Key Management Private Keys

Backed up subscriber private key management keys shall 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 and must be held in the Subscriber’s control.

6.2.4.4 Backup of CSS Private Key

CSS private keys may be backed up. If backed up, all copies shall be accounted for and protected in the same manner as the original.

6.2.4.5 Backup of PIV-I Content Signing Key

Backup of PIV-I Content Signing private signature keys may be required to facilitate disaster recovery. In such cases, Id-orc-nfissp-pivi-contentSigning private signature keys shall be backed up under multi-person control.

6.2.4.6 Backup of Device Private Keys

Device private keys may be backed up or copied, but must be held under the control of the device’s human sponsor or other authorized administrator. Backed up device private keys shall not be stored in plaintext form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the device’s cryptographic module.

6.2.5 Private Key Archival

WidePoint NFI CA private signature keys and subscriber private signatures keys shall not be archived. WidePoint NFI CAs that retain subscriber private encryption keys for business continuity purposes shall archive such subscriber private keys, in accordance with this CP.
At present, WidePoint 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.

6.2.6 Private Key Transfer into or from a Cryptographic Module

WidePoint NFI CA private keys may be exported from the cryptographic module only to perform CA key backup procedures as described in Section 6.2.4.1, Backup of WidePoint NFI CA Private Signature Keys. At no time shall the WidePoint NFI CA private key exist in plaintext outside the cryptographic module.

All other keys shall be generated by and in a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport; private keys must never exist in plaintext form outside the cryptographic module boundary.

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

6.2.7 Private Key Storage on a Cryptographic Module

No stipulation beyond that specified in FIPS 140.

6.2.8 Method of Activating Private Keys

WidePoint NFI CAs signing key activation requires multi-person control as specified in Section 5.2.2, Number of Persons Required per Task.

The Subscriber must be authenticated to the cryptographic module before the activation of any private key(s). Acceptable means of authentication include but are not limited to pass-phrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

In addition, PIV-I Content Signing key activation requires the same multiparty control established for the Entity CA (see Section 5.2.2).

For certificates issued under WidePoint NFI Card Authentication, subscriber authentication is not required to use the associated private key.

6.2.9 Method of Deactivating Private Keys

If cryptographic modules are used to store the WidePoint NFI CA private signing keys, then the cryptographic modules that have been activated shall not be left unattended or otherwise available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the WidePoint NFI CA's CPS. Hardware cryptographic or modules shall be removed and stored in a secure container when not in use.

6.2.10 Method of Destroying Private Keys

Individuals in trusted roles shall destroy WidePoint NFI CA, RA, and status server (e.g., OCSP server) private signature keys when they are no longer needed.

Subscriber private signature keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, this can be overwriting the data. For hardware cryptographic modules, this will likely be executing a zeroize command. Physical destruction of hardware should not be required.

To ensure future access to encrypted data, subscriber private key management keys should be secured in long-term backups or archived.

6.2.11 Cryptographic Module Rating

See Section 6.2.1. Cryptographic Module Standards and Controls.

6.3 OTHER ASPECTS OF KEY MANAGEMENT

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods and Key Usage Periods

WidePoint NFI CAs that distribute their self-signed certificates for use as trust anchors shall limit the use of the associated private key to a maximum of 20 years; the self-signed certificates shall have a lifetime not to exceed 37 years. For PIV-I, CSS certificates that provide revocation status have a maximum certificate validity period of 31 days.

For all other WidePoint NFI CAs, the WidePoint NFI CA shall limit the use of its private keys to a maximum of six years for subscriber certificates and ten years for CRL signing and OCSP responder certificates. WidePoint NFI CAs must not issue subscriber certificates that extend beyond the expiration date of the CA’s own certificates and public keys.
Code and content signers may use their private keys for three years; the lifetime of the associated public keys shall not exceed eight years.

Subscribers’ signature private keys and certificates have a maximum lifetime of three years. Subscriber key management certificates have a maximum lifetime of three years; use of subscriber key management private keys is unrestricted.

The validity period of the Subscriber certificate must not exceed the routine re-key Identity Requirements as specified in Section 3.3.1, Identification and Authentication for Routine Re-Key. Additionally, for PIV-I subscribers, certificate expiration shall not be later than the expiration date of the PIV-I hardware token on which the certificates reside.

6.3.3 Restrictions on WidePoint NFI CA’s Private Key Use

The private key used by WidePoint NFI CAs for issuing Certificates shall be used only for signing such Certificates and, optionally, CRLs or other validation services responses.

A private key held by a CMA, if any, and used for purposes of manufacturing Certificates is considered the WidePoint NFI CA’s signing key, is held by the CMA as a fiduciary, and shall not be used by the CMA for any other purposes, except as agreed by the WidePoint NFI CA. Any other private key used by a CMA for purposes associated with its CMA function shall not be used for any other purpose without the express permission of the WidePoint NFI CA.

The private key used by each RA employed by a WidePoint NFI CA in connection with the issuance of Certificates shall be used only for communications relating to the approval, issuance, or revocation of such certificates.

Under no circumstances shall the WidePoint NFI CA signature keys used to support non-repudiation services be escrowed by a third party.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

The activation data used to unlock WidePoint NFI CA or Subscriber private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected. Activation data may be user selected, including activation selected by each of the multiple parties holding that activation data). The strength of the activation data shall meet or exceed the requirements for authentication mechanisms stipulated in FIPS 140. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

Where the WidePoint NFI CA uses passwords as activation data for the CA signing key, at a minimum the activation data shall be changed upon CA re-key.

6.4.2 Activation Data Protection

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

- Memorized
- Biometric in nature, or
- Recorded and secured at the level of assurance associated with the activation of the cryptographic module, and shall not be stored with the cryptographic module

The protection mechanism shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the respective WidePoint NFI CA CPS. Passwords shall be encrypted.

6.4.3 Other Aspects of Activation Data

For PIV-I, in the event activation data must be reset, a successful biometric 1:1 match of the applicant against the biometrics collected in Section 3.2.3.1 is required. This biometric 1:1 match must be conducted by a trusted agent of the issuer.

6.5 COMPUTER SECURITY CONTROLS

The computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards in accordance with Federal laws, regulations, and guidelines as well as WidePoint security policy and supporting security guidelines.

6.5.1 Specific Computer Security Technical Requirements

For WidePoint NFI CAs, the following computer security functions listed below are required:

- Authenticate the identity of users before permitting access to the system or applications.

- Manage privileges of users to limit users to their assigned roles.
- Generate and archive audit records for all transactions (see Section 5.4. Audit Logging Procedures).
- Enforce domain integrity boundaries for security critical processes.
- Support recovery from key or system failure.

For Certificate Status Servers, the computer security functions listed below are required:

- Authenticate the identity of users before permitting access to the system or applications.
- Manage privileges of users to limit users to their assigned roles.
- Enforce domain integrity boundaries for security critical processes.
- Support recovery from key or system failure.

WidePoint does not allow for remote workstations to administer WidePoint NFI CAs or KEDs.

All communications between any PKI trusted role and the CA shall be authenticated and protected from modification.

WidePoint NFI KRA workstation operating systems shall meet the following requirements:

- Require authenticated logins
- Provide discretionary access control
- Provide a security audit capability
- Require identification and authentication
- Require a trusted path for identification and authentication
- Provide residual information protection for storage objects such as memory, disk sectors, device registers.
- Provide operating system self-protection
- Provide domain isolation for application processes

6.5.2 Computer Security Rating

No stipulation.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

The entire WidePoint NFI system development life cycle shall be controlled to ensure its integrity at all levels, including the use of best commercial practices. The system development controls are as follows:

- For commercial off-the-shelf software, the software shall be designed and developed under a formal, documented development methodology.
- Hardware and software developed specifically for a particular WidePoint NFI CA shall demonstrate that security requirements were achieved through a combination of software verification & validation, structured development approach, and controlled development environment.
- Where open source software has been utilized, the WidePoint NFI CA shall demonstrate that security requirements were achieved through software verification and validation and structured development/life-cycle management.
- Hardware and software procured to operate the WidePoint NFI CA shall be purchased and shipped in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).
- The WidePoint NFI CA hardware and software shall be dedicated to performing one task: the CA. There shall be no other applications, hardware devices, network connections, or component software installed that are not part of the WidePoint NFI CA operation. Where the WidePoint NFI CA operation supports multiple CAs, the hardware platform may support multiple CAs.
- Proper care shall be taken to prevent malicious software from being loaded onto the WidePoint NFI CA equipment. All applications required to perform the operation of the WidePoint NFI CA shall be obtained from documented sources. All hardware and software, including RA hardware and software, shall be scanned for malicious code on first use and periodically thereafter.
- Hardware and software updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of the WidePoint NFI CA system as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the WidePoint NFI CA software or configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance of the WidePoint NFI CA system. The WidePoint NFI CA software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use. The WidePoint NFI CA shall periodically verify the integrity of the software as specified in the WidePoint NFI CA CPS.

6.6.3 Object Reuse

When a storage object (e.g., core area, disk file, etc.) is initially assigned, allocated, or reallocated to a system user, the system shall assure that it has been cleared in accordance with Federal laws, regulations, and guidelines; as well as in accordance with WidePoint security policy and supporting security guidelines. WidePoint NFI CAs' CPSs shall specify procedures for sanitizing electronic media for reuse (e.g., overwrite or degaussing of electronic media) and controlled storage, handling, or destruction of spoiled media, or media that cannot be effectively sanitized for reuse.

All magnetic media used to store sensitive unclassified information shall be purged or destroyed when no longer needed. The WidePoint NFI CA system shall ensure that a user is not able to access the prior contents of a resource that has been allocated to that user by the system. Care shall be taken to ensure that the Recycle Bin does not store deleted files and procedures shall be established to ensure the proper disposal of printed output based on the sensitivity of the data.

6.6.4 Life Cycle Security Ratings

No stipulation.

6.7 NETWORK SECURITY CONTROLS

WidePoint NFI CAs, CMSs, RAs, directories and repositories shall employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Unused network ports and services shall be turned off. Any network software present on the WidePoint NFI CA equipment shall be necessary to the functioning of the WidePoint NFI CA. The Authorized WidePoint NFI CPS shall define the network protocols and mechanisms required for the operation of the WidePoint NFI CA and CMS.

Any boundary control devices used to protect the network on which WidePoint NFI CA or CMS equipment is hosted shall deny all but the necessary services to the equipment even if those services are enabled for other devices on the network. WidePoint NFI CA servers, routers, and other communication hardware essential for maintaining the operability of the system and its connectivity to the backbone network, as well as any other hardware used in support of production systems, shall be placed in a controlled access location (i.e., behind locked doors).

Remote access to the system shall be restricted to secure methods employing approved I&A as well as intrusion detection and unauthorized access monitoring.

WidePoint NFI CAs shall indicate if encryption is used to prevent unauthorized access to sensitive files as part of the system or application access control procedures. If encryption is used as part of the access controls, provide information about the following:

- The cryptographic methodology (e.g., secret key and public key) used
- If a specific off-the-shelf product is used, the name of the product
- That the product and the implementation method meet Federal standards, and include that information

- Cryptographic key management procedures for key generation, distribution, storage, entry, use, destruction, and archiving

A network guard, firewall, or filtering router shall protect network access to a WidePoint NFI KRA workstation. The network guard, firewall, or filtering router shall limit services allowed to and from the WidePoint NFI KRA workstation to those required to perform WidePoint NFI KRA functions.

Protection of WidePoint NFI KRA workstation shall be provided against known network attacks. All unused network ports and services shall be turned off. Any network software present on the WidePoint NFI KRA workstation shall be necessary to the functioning of the WidePoint NFI KRA application.

6.8 TIME STAMPING

WidePoint NFI PKI date/time stamps shall conform to the ITU-T Recommendation X.690 and the X.690 v2, Information Technology – ASN.1 Encoding Rules, 1994.

Asserted times shall be accurate to within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events, see Section 5.4.1, Types of Events Recorded.

7 CERTIFICATE, CARL/CRL, AND OCSP PROFILES FORMAT

7.1 CERTIFICATE PROFILE

WidePoint NFI certificate profiles are presented in Appendix C.

The WidePoint NFI CA shall create and maintain Certificates that conform to RFC 5280 and ITU-T Recommendation X.509, The Directory: Authentication Framework, June 1997. All certificates must include a reference to an OID for this Policy within the appropriate field, and contain the required certificate fields as specified in this CP.

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

7.1.1 Version Numbers

The WidePoint NFI CAs shall issue X.509 v3 certificates (populate version field with integer “2”).

7.1.2 Certificate Extensions

For all WidePoint NFI CAs, use of standard certificate extensions shall comply with [RFC 5280].
CA certificates issued by WidePoint NFI CAs shall not include critical private extensions.

Whenever private extensions are used in subscriber certificates, they shall be identified in the WidePoint NFI CA’s CPS. Critical private extensions shall be interoperable in their community of use.
All certificates issued a policy OID cross certified with the PIV-I policy OID shall conform to [PIV-I Profile].

Practice Note: *For WidePoint NFI CAs that issue PIV-I certificates, the associated CSS certificates will also comply with [PIV-I Profile]*.

7.1.3 Algorithm Object Identifiers

Certificates issued under this CP shall 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 }

Where certificates are signed using RSA with PSS padding, the OID is independent of the hash algorithm; the hash algorithm is specified as a parameter. RSA signatures with PSS padding may be used with the hash algorithms and OIDs specified below:

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

Certificates issued under this CP shall 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 shall 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 shall be populated with an X.500 Distinguished Name, with the attribute type as further constrained by RFC 5280.

The subject alternative name extension shall be present and include a PIV-I *UUID* [or equivalent] name type in certificates issued under WidePoint NFI Authentication and Card Authentication.

7.1.5 Name Constraints

No stipulations.

7.1.6 Certificate Policy Object Identifier

Certificates issued under this CP shall assert the OID appropriate to the type of certificate and level of assurance with which it was issued. See Section 1.2, Document Identification for specific OIDs.

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

Certificates may contain policy qualifiers identified in RFC 5280.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Processing semantics for the critical certificate policy extension used by WidePoint NFI CAs shall conform to [FPKI-PROF].

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

When ARLs and CRLs are used to distribute status information, detailed ARL/CRL profiles addressing the use of each extension shall conform to the Federal PKI X.509 Certificate and CRL Extension Profile and RFC 5280.

7.2.1 Version Numbers

The WidePoint NFI CAs shall issue X.509 Version two (2) CRLs.

7.2.2 CRL Entry Extensions

CRL extensions shall conform to [FPKI-PROF].

7.3 OCSP PROFILE

Certificate status servers (CSSs) operated under this CP shall sign responses using algorithms designated for CRL signing.

8 COMPLIANCE AUDITS AND OTHER ASSESSMENTS

WidePoint NFI CAs shall have a compliance audit mechanism in place to ensure that the requirements of their CPS are being implemented and enforced.

This specification does not impose a requirement for any particular CPS compliance assessment methodology.

The WidePoint NFI PMA shall be responsible for ensuring audits are conducted for all WidePoint NFI functions regardless of how or by whom the WidePoint NFI components are managed and operated.

The WidePoint NFI CA, including all of its RA, CMA, and Repository subcontractor(s) shall undergo an audit of NFI systems and controls consistent with the guidelines cited in Section 8.4. The purpose of the audit process shall be to verify that the WidePoint NFI CA has in place and follows a system that assures that the quality of its WidePoint NFI CA Services conforms to the above requirements and the requirements of this CP, as well as any MOAs between the Entity PKI and any other PKI (See Appendix B, Applicable Guidance documents).

Re-accreditation should occur after any significant change in the system, but at least every three years. It should be done more often where there is a high risk and potential magnitude of harm.

This specification does not impose a requirement for any particular assessment methodology.

8.1 FREQUENCY OF AUDIT OR ASSESSMENTS

The WidePoint NFI CAs and RAs and their subordinate CAs and RAs shall be subject to a periodic CP/CPS compliance audit at least once per year. Where a status server is specified in certificates issued by a WidePoint NFI CA, the status server shall be subject to the same periodic compliance audit requirements as the corresponding CA. For example, if an OCSP server is specified in the authority information access extension in certificates, that server must be reviewed as part of that WidePoint NFI CA’s compliance audit.

Alternative reviews of CA’s and RA’s may be substituted for full compliance audits under exceptional circumstances, and in accordance with the requirements as specified in the Triennial Audit Guidance document located at http://www.idmanagement.gov/fpkipa/. The conditions that permit an alternative review are as follows:

- If no changes to policies, procedures, or operations have occurred during the previous year, an assertion to that effect, signed by the cognizant executive (CIO or equivalent), is acceptable in lieu of a full compliance audit.
- If no significant changes to policies, procedures, or operations have occurred during the previous year, a delta compliance audit is acceptable in lieu of a full compliance audit.

However, a full compliance audit (see Section 8.4, Topics Covered by Assessment) must be completed every third year, regardless.

Practice Note: Examples of significant changes include but are not limited to: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to CA and or RA operating procedures; (iii) installation of a new or upgraded hardware platform or firmware component; and (iv) modifications to the certificate policy.

The WidePoint DAA reserves the right to perform periodic and aperiodic compliance audits or inspections of WidePoint NFI CA, subordinate CA, or RA operations to validate that the subordinate entities are operating in accordance with the security practices and procedures described in their respective CPS, System Security Plan, and Privacy Policies and Procedures. Further, the Federal PKI Policy Authority has the right to require aperiodic compliance audits of WidePoint NFI CAs (and, when needed, their subordinate CAs) that interoperate with the FBCA under this CP.

WidePoint NFI CAs shall undergo a witnessed key generation ceremony, and an initial audit prior to initial approval, to demonstrate compliance with this CP, their CPS, applicable regulations and guidelines, and WidePoint IT Security policies, procedures, and guidelines. Re-certification will be required every three years or at any time that a significant change in operations is made, whichever occurs first, to demonstrate continuing compliance (See Appendix B, Applicable Guidance documents).

8.2 IDENTITY AND QUALIFICATIONS OF ASSESSOR

The auditor must demonstrate competence in the field of compliance audits. At the time of the audit, the compliance auditor must be thoroughly familiar with requirements which the WidePoint NFI CA's CPS and this CP. The compliance auditor must perform such compliance audits as a regular ongoing business activity. In addition, the auditor must be a Certified Information System Auditor (CISA), IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The compliance auditor shall either be a private firm that is independent of the WidePoint NFI CA being audited, or an independent security audit firm acceptable to WidePoint that is qualified to perform a security audit on a CA. The WidePoint PKI Policy Authority shall determine whether a compliance auditor meets this requirement.

8.4 TOPICS COVERED BY ASSESSMENT

The purpose of a compliance audit of a WidePoint NFI CA shall be to verify that the WidePoint NFI CA is complying with the requirements of this CP and their CPS, as well as any MOAs between the WidePoint NFI CA and any other PKIs.

A full compliance audit for WidePoint NFI CAs covers all aspects within the scope identified above.

Where permitted by Section 8.1, Frequency of Audit or Assessments, the WidePoint NFI CA may perform a delta compliance audit in lieu of the full compliance audit. A delta compliance audit covers all changes to policies, procedures, or operations that have occurred during the previous year. The following topics must be addressed in a delta compliance audit even if no changes have occurred since the last full compliance audit:

- Personnel controls
- Separation of Duties
- Audit review frequency and scope
- Types of events recorded in physical and electronic audit logs
- Protection of physical and electronic audit data
- Physical security controls
- Backup and Archive generation and storage
- For Audit, the topics covered by the Audit shall be pursuant to the guidance provided in one of the following methodologies:
        - ▪ ISSO 21188, Public key infrastructure for financial services - Practices and policy framework
    - o FIPS 200, Minimum Security Requirements for Federal Information and Information Systems

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

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If the WidePoint NFI CA compliance auditor finds discrepancies between how the WidePoint NFI CA is designed or is being operated or maintained, the requirements of this CP, any applicable MOAs, and/or the WidePoint NFI CA CPS, the following actions shall be performed:

- The compliance auditor shall document the discrepancy and provide a copy to WidePoint.
- The compliance auditor shall notify the parties identified in Section 8.6, Communication of Results, of the discrepancy promptly.
- The WidePoint NFI CA shall determine what further notifications or actions are necessary to meet the requirements of this CP, WidePoint NFI CA CPS, and any relevant MOA provisions.
- WidePoint will address any identified deficiencies with the WidePoint NFI CA. The WidePoint NFI CA shall correct any deficiencies noted during these reviews as specified by WidePoint, including proposing a remedy and expected time for completion.

Results of the audit review will be made available to the WidePoint PKI Policy Authority, to be used in determining the CA’s suitability for initial and continued performance as a WidePoint NFI CA.

8.6 COMMUNICATION OF RESULTS

The results of audits shall be fully documented. The reports resulting from the compliance audit shall be submitted to the WidePoint DAA within 30 calendar days of the date of their completion.

The CP/CPS compliance report shall identify the versions of the CP and CPS used in the assessment.

On an annual basis, the Entity PKI PMA shall submit an audit compliance package to the FPKIPA. This package shall be prepared in accordance with the "Compliance Audit Requirements" document and include an assertion from the WidePoint NFI PMA that all NFI components have been audited - including any components that may be separately managed and operated. The package shall identify the versions of the WidePoint NFI CP and WidePoint NFI CPS used in the assessment. Additionally, where necessary, the results shall be communicated as set forth in Section 8.5 above.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 Certificate Issuance or Renewal Fees

No stipulation.

9.1.2 Certificate Access Fees

The WidePoint NFI CA shall not impose any certificate access fees on Subscribers with respect to the content of its own CA Certificate(s) or the status of such Certificate(s).

9.1.3 Revocation or Status Information Access Fee

Fees may be assessed for certificate validation services.

9.1.4 Fees for Other Services such as Policy Information

The WidePoint NFI CA shall not impose fees for access to policy information.

9.1.5 Refund Policy

No stipulation.

9.2 FINANCIAL RESPONSIBILITY

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

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 shall be made publicly available.

9.3.1 Scope of Confidential Information

The WidePoint NFI CA shall take steps as required to protect the confidentiality of any WidePoint, Relying Party, Subscriber, or other Government information provided to the WidePoint NFI CA. Such information shall be used only for the purpose of providing WidePoint NFI CA Services and carrying out the provisions of this Policy, and shall not be 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 MOA.

9.3.2 Information Not Within the Scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

WidePoint, Relying Party, Subscriber, and Government information provided to the WidePoint NFI CA shall be used only for the purpose of providing WidePoint NFI CA Services and carrying out the provisions of this CP, and shall not be disclosed in any manner to any person except as may be necessary for the performance of the WidePoint NFI CA Services in accordance with this CP and the MOA.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

Each WidePoint NFI CA shall maintain written Privacy Policies and Procedures (PPP) designed to ensure compliance with the requirements of 5 U.S.C. 552a, Appendix I to OMB Circular A-130. These policies and procedures shall be incorporated into the WidePoint NFI CA's CPS.

9.4.2 Information Treated as Private

The WidePoint NFI CA shall protect the confidentiality of personal information regarding Subscribers that is collected during the applicant registration, Certificate application, authentication, and certificate status checking processes. Such information shall be used only for the purpose of providing WidePoint NFI CA Services and carrying out the provisions of this CP, and shall not be disclosed in any manner to any person without the prior consent of the Subscriber, unless otherwise required by law, except as may be necessary for the performance of the WidePoint NFI CA Services in accordance with the MOA.

9.4.3 Information not Deemed Private

Information contained on a single Certificate or related status information shall not be considered confidential, when the information is used in accordance with the purposes of providing WidePoint NFI CA Services and carrying out the provisions of this CP. However, a compilation of such information about an individual shall be treated as confidential.

For WidePoint NFI CAs, certificates that contain the UUID in the subject alternative name extension shall not be distributed via publicly accessible repositories (e.g., LDAP, HTTP).

9.4.4 Responsibility to Protect Private Information

Each WidePoint NFI CA or employee of the WidePoint NFI CA to whom information may be made available or disclosed shall be notified in writing by the WidePoint NFI CA that information disclosed to such WidePoint NFI CA or employee can be used only for the purpose and to the extent authorized in this CP.

In addition, WidePoint NFI CAs shall store sensitive information securely, and may be released only in accordance with other stipulations in Section 9.4, Privacy of Personal Information.

9.4.5 Notice and Consent to Use Private Information

WidePoint is not required to provide any notice or obtain the consent of the Subscriber or WidePoint personnel in order to release private information in accordance with the stipulations of Section 9.4.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The WidePoint NFI CA shall not disclose private information to any third party unless authorized by this CP, required by law, Government rule or regulation, or order of a court of competent jurisdiction. Any request for release of information shall be processed according to the laws of the Commonwealth of Virginia.

9.4.7 Other Information Disclosure Circumstances

Personal information submitted by Subscribers:

- Must be made available by the WidePoint NFI CA to the Subscriber involved following an appropriate request by such Subscriber
- Must be subject to correction and/or revision by such Subscriber
- Must be protected by the WidePoint NFI CA in a manner designed to ensure the data's integrity
- Cannot be used or disclosed by the WidePoint NFI CA for purposes other than the direct operational support of unless such use is authorized by the Subscriber involved

9.5 INTELLECTUAL PROPERTY RIGHTS

Private keys shall be treated as the sole property of the legitimate holder of the corresponding public key identified in a Certificate. This CP is the property of WidePoint. Any other use of the above without the express written permission of WidePoint is expressly prohibited.

9.6 REPRESENTATIONS AND WARRANTIES

Policy Authority and WidePoint NFI Program Management Office will:

- Review periodic compliance audits to ensure that RAs and other components operated by the WidePoint NFI CA are operating in compliance with their approved CPSs.
- Review name space control procedures to ensure that distinguished names are uniquely assigned within each WidePoint NFI CA.

9.6.1 CA Representations and Warranties

Upon issuance of a Certificate, the WidePoint NFI CA warrants to all Program Participants that:

- The WidePoint NFI CA will manage the Certificate in accordance with the requirements in this CP.
- The WidePoint NFI CA has complied with all requirements in this CP when identifying the Subscriber and issuing the Certificate.
- There are no misrepresentations of fact in the Certificate known to the WidePoint NFI CA and the WidePoint NFI CA has verified the information in the Certificate. It is the responsibility of the WidePoint NFI CA to verify the source of the certificate request, and to ensure that Subscriber information submitted in the application process is correct and accurate. Information will be verified to ensure legitimacy as per Section 3, Identification and Authentication.
- Information provided by the Subscriber for inclusion in the Certificate has been accurately transcribed to the Certificate.
- The Certificate meets the material requirements of this CP.

For PIV-I, WidePoint NFI CAs shall maintain an agreement with Affiliated Organizations concerning the obligations pertaining to authorizing affiliation with Subscribers of PIV-I certificates.

9.6.2 RA Representations and Warranties

An RA who performs registration functions in support of a WidePoint NFI CA shall also comply with the requirements in the CP.

In addition, RAs supporting WidePoint NFI CAs shall conform to the following:

- Maintain operations in conformance to the stipulations of the approved WidePoint NFI CA CPS.
- Include only valid and appropriate information in certificate requests, and maintain evidence that due diligence was exercised in validating the information contained in the certificate.

- Ensure that obligations are imposed on subscribers in accordance with Section 9.6.3, Subscriber Representations and Warranties, and that subscribers are informed of the consequences of not complying with those obligations.

9.6.3 Subscriber Representations and Warranties

A Subscriber (or human sponsor for device certificates) shall be required to sign a document containing the requirements the Subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate.

Subscribers of WidePoint NFI CAs shall agree to the following:

- Provide complete and accurate responses to all requests for information made by the WidePoint NFI CA (or an authorized RA) during the applicant registration, certificate application, and authentication of identity processes.
- Generate a key pair using a reasonably trustworthy system, and take reasonable precautions to prevent any compromise, modification, loss, disclosure, or unauthorized use of the private key.
- Upon issuance of a Certificate naming the applicant as the Subscriber, review the Certificate to ensure that all Subscriber information included in it is accurate, and to expressly indicate acceptance or rejection of the Certificate.
- Use the Certificate and the corresponding private key exclusively for purposes authorized by this Policy and only in a manner consistent with this Policy.
- Instruct the issuing WidePoint NFI CA (or an authorized RA) to revoke the Certificate promptly upon any actual or suspected loss, disclosure, or other compromise of the private key, or, in the case of s, State and Local Governments, and Federal Employee Certificates, whenever the Subscriber is no longer affiliated with the Sponsoring Organization.
- Respond as required to notices issued by the WidePoint NFI CA.
- Protect the private keys issued to them under the WidePoint NFI CA.
- Provide accurate identification and authentication information during initial and subsequent key recovery requests.
- Determine whether revocation of the public key certificate associated with the recovered key is necessary when notified that their escrowed key has been recovered. Request the revocation, if necessary.

Subscribers who receive certificates from a WidePoint NFI CA shall comply with these CP requirements.

9.6.4 Relying Parties Representations and Warranties

Relying Parties must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each Relying Party for each application and is not controlled by this CP.

Parties who rely upon the certificates issued under this policy should 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.

9.6.5 KED Representations and Warranties

A KED that provides escrowed keys to Requestors under this KRP shall conform to the stipulations of this document. In particular, the following stipulations apply:

- The KED shall operate in accordance with the stipulations of the WidePoint NFI CPS and this CP.
- The KED shall automatically notify the subscribers when their private keys have been escrowed (e.g., a dialog box may appear on a subscriber's screen during the certificate request process).

  > Practice Note: This notification may be part of the subscriber agreement provided during the subscriber registration process.

- The KED shall monitor KRA activity for patterns of potentially anomalous activity as indicators of possible problems in the infrastructure, and initiate inquiries or investigations as appropriate.

9.6.6 KRA Representations and Warranties

WidePoint NFI KRAs who submit requests as described in this CP shall comply with the stipulations of this CP and the applicable WidePoint NFI CPS. In particular, the following stipulations apply:

- WidePoint NFI KRAs shall operate in accordance with the stipulations of this CP and the applicable WidePoint NFI CPS.
- WidePoint NFI KRAs shall protect subscribers' escrowed keys from unauthorized disclosure, including the encrypted files and associated decryption keys.
- WidePoint NFI KRAs shall protect all information associated with key recovery, including the KRA's own key(s), which could be used to recover subscribers' escrowed keys.
- WidePoint NFI KRAs shall release Subscribers' escrowed keys only for properly authenticated and authorized requests from Requestors.
- WidePoint NFI KRAs shall protect all information regarding all occurrences of key recovery.
- WidePoint NFI KRAs shall not communicate any information concerning a key recovery to the Subscriber except when the Subscriber is the Requestor.

9.6.7 Requestor Representations and Warranties

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

- Requestors shall protect Subscribers' recovered key(s) from compromise. Requestors shall 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 shall destroy Subscribers' keys when no longer required (i.e., when the data has been recovered).
- Requestors shall request and use the Subscriber's escrowed key(s) only to recover Subscriber's data they are authorized to access.
- Requestors shall accurately represent themselves to all entities during any key recovery service.
- The Third-Party Requestor shall protect information concerning each key recovery operation.
- The Third-Party Requestor shall communicate information concerning the recovery to the Subscriber when appropriate as determined by the reason for the recovery. The decision to notify the Subscriber shall 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 shall 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 shall sign an acknowledgement of agreement to follow the law and WidePoint policies relating to protection and release of the recovered key.
- Upon receipt of the recovered key(s), the Third-Party Requestor shall sign[2] an attestation to the effect:
  - "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."

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

9.6.8 Representations and Warranties of Affiliated Organizations

Affiliated Organizations shall authorize the affiliation of Subscribers with the organization, and shall inform the Entity CA of any severance of affiliation with any current Subscriber.

9.6.9 Representations and Warranties of Other Participants

No stipulation.

9.7 DISCLAIMERS OF WARRANTIES

WidePoint NFI CAs and KRSs may not disclaim any responsibilities described in this CP.

9.8 LIMITATIONS OF LIABILITY

Nothing in this CP shall create, alter, or eliminate any other obligation, responsibility, or liability that may be imposed on any Program Participant by virtue of any contract or obligation that is otherwise determined by applicable law.

A Relying Party shall have no recourse against WidePoint, the FBCA, the WidePoint NFI CA s, RAs, certificate manufacturing authority or repository for any claim under any theory of liability (including negligence) arising out of reliance upon an certificate, unless such party shall have agreed to provide such recourse under a contract with the relying party. Each Relying Party assumes all risk of such reliance in the absence of such agreement, except that the Subscriber may have liability under applicable law to the Relying Party with respect to a message bearing his digital signature that is authenticated with a certificate.

WidePoint NFI certificates may contain (non-critical field) notice that there is no recourse against the issuer of the certificate except as provided for in this section of the CP, as stipulated in Appendix C, Certificate Profiles, of this Policy.

9.9 INDEMNITIES

No stipulation.

9.10 TERM AND TERMINATION

9.10.1 Term

This CP becomes effective when approved by the WidePoint PKI Policy Authority. This CP has no specified term.

9.10.2 Termination

Termination of this CP is at the discretion of the WidePoint PKI Policy Authority.

9.10.3 Effect of Termination and Survival

The requirements of this CP remain in effect through the end of the archive period for the last certificate issued.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

WidePoint has established appropriate procedures for communications with WidePoint NFI CA customers via contracts and MOAs as applicable.

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.

For all other communications, there is no stipulation.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

The Policy Authority shall review this CP at least once every year. Corrections, updates, or suggested changes to this CP shall be publicly available. Suggested changes to this CP shall be communicated to the Policy Authority and/or Program Manager; such communication must include:

- A description of the change
- A change justification
- Contact information for the person requesting the change

Notice of all proposed changes to this CP under consideration by WidePoint that may materially affect subscribers of this CP (other than editorial or typographical corrections, changes to the contact details, or other such minor changes) will be provided to WidePoint NFI CAs and Relying Parties, and will be posted on the WidePoint NFI web site. The WidePoint NFI CA shall post notice of such proposed changes and shall advise their Subscribers of such proposed changes.

The Policy Authority and/or Program Manager shall assign new OIDs to certificates as needed and maintain control over the numbering sequence of OIDs. WidePoint NFI CAs requiring new OIDs shall submit a request to the Policy Authority and/or Program Manager.

Any interested person may file comments with WidePoint within 45 days of original notice. If the proposed change is modified as a result of such comments, a new notice of the modified proposed change shall be given.

Version control shall be maintained by the Policy Authority using date and consecutive version numbers to identify revised versions of the CP, which will be presented on a Change Control Page at the beginning of the CP.

9.12.2 Notification Mechanism and Period

A copy of this CP is available in electronic form on the Internet at http://www.orc.com/NFI, and via email from the Policy Authority. The WidePoint NFI CA shall also make available copies of this CP both online and in hard copy form.

9.12.3 Circumstances under Which OID Must Be Changed

OIDs will be changed if the Policy Authority determines that a change in the CP requires a change in OIDs.

9.13 DISPUTE RESOLUTION PROVISIONS

In the event of any dispute or disagreement between two or more of the Program Participants (Disputing Parties) arising out of or relating to this CP or the MOA, WidePoint NFI CA CPS, or Agreements related to this CP, which include Subscriber Agreements, the Disputing Parties shall use their best efforts to settle the dispute or disagreement through negotiations in good faith following notice from one Disputing Party to the other(s).

When one of the Disputing Parties is a Federal entity, the dispute arbitrator shall be the WidePoint PKI Policy Authority.

9.14 GOVERNING LAW

The laws of the United States and the Commonwealth of Virginia shall govern the enforceability, construction, interpretation, and validity of this CP.

9.15 COMPLIANCE WITH APPLICABLE LAW

WidePoint NFI CAs 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

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in Section 9.12, Amendments.

9.16.4 Enforcement (Attorney Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 OTHER PROVISIONS

9.17.1 Waivers

No stipulation.

10 CERTIFICATE FORMAT

10.1 Application Certificate

This table is based on Worksheet 7, Certificate Profile for Computing and Communications Devices, of X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program, v1.7, 5 May 2015.

Field	Criticality Flag	Value	Comments
Certificate			
tbsCertificate			Fields to be signed.
version		2	Integer value of "2" for version 3 certificate.
serialNumber		INTEGER	Unique positive integer.
signature			
AlgorithmIdentifier			Must match Algorithm Identifier in signatureAlgorithm field. The parameters field is only populated when the algorithm is RSA.
algorithm		1.2.840.113549.1.1.11	sha256WithRSAEncryption
parameters		NULL	For all RSA algorithms except id-RSASSA-PSS
issuer			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue			
validity			
notBefore			
Time			
utcTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime		YYYYMMDDHHMMSSZ	Use for dates after 2049.
notAfter			
Time			
utcTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime		YYYYMMDDHHMMSSZ	Use for dates after 2049.
subject			
Name			X.500 Distinguished name of the owner of the subject public key in the certificate.
RDNSequence			
RelativeDistinguishedName			

Field	Criticality Flag	Value	Comments
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue			
subjectPublicKeyInfo			
algorithm			
AlgorithmIdentifier			Public key algorithm associated with the public key.
algorithm		1.2.840.113549.1.1.1	RSA
parameters		NULL	
subjectPublicKey		BIT STRING	
required extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	
keyUsage	TRUE		
digitalSignature		1	
nonrepudiation		0	
keyEncipherment		1	
dataEncipherment		0	
keyAgreement		0	
keyCertSign		0	
cRLSign		0	
encipherOnly		0	
decipherOnly		0	
certificatePolicies	FALSE		
PolicyInformation			
policyIdentifier		1.3.6.1.4.1.3922.1.1.1.37	
cRLDistributionPoints	FALSE		
DistributionPoint			
distributionPoint			
DistributionPointName			
fullName			
GeneralNames			
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			

Field	Criticality Flag	Value	Comments
AttributeType		OID	
AttributeValue			
uniformResourceIdentifier		ldap://… or http://...	
authorityInfoAccess	FALSE		
AccessDescription			
accessMethod		Id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	
accessLocation			
GeneralName			
uniformResourceIdentifier		ldap://… or http://...	
extKeyUsage	BOOLEAN		This extension MUST appear in certificates issued after June 30, 2019. The extension should be non-critical and shall not include the anyExtendedKeyUsage value. The values listed below for keyPurposeID are recommended for inclusion. Additional keyPurposeIDs, consistent with signing purposes, may be specified. Note: For certificates issued prior to June 30, 2019, anyExtendedKeyUsage may be present or the entire extension may be absent.
keyPurposeId	FALSE	1.3.6.1.5.5.7.3.1	Server authentication
		1.3.6.1.5.5.7.3.2	client authentication
subjectAltName	FALSE		
GeneralNames			
GeneralName			
dNSName		IA5String	For devices, this field contains the DNS name of the subject.
iPAddress		IA5String	For devices, this field contains the IP address of the subject.

10.2 Domain Controller Certificate

This table is based on Worksheet 7, Certificate Profile for Computing and Communications Devices, of X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program, v1.7, 5 May 2015.

Field	Criticality Flag	Value	Comments
Certificate			
tbsCertificate			Fields to be signed.
version		2	Integer value of "2" for version 3 certificate.
serialNumber		INTEGER	Unique positive integer.

Field	Criticality Flag	Value	Comments
signature			
AlgorithmIdentifier			Must match Algorithm Identifier in signatureAlgorithm field. The parameters field is only populated when the algorithm is RSA.
algorithm		1.2.840.113549.1.1.11	sha256WithRSAEncryption
parameters		NULL	For all RSA algorithms except id-RSASSA-PSS
issuer			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue			
validity			
notBefore			
Time			
utcTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime		YYYYMMDDHHMMSSZ	Use for dates after 2049.
notAfter			
Time			
utcTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime		YYYYMMDDHHMMSSZ	Use for dates after 2049.
subject			
Name			X.500 Distinguished name of the owner of the subject public key in the certificate.
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue			
subjectPublicKeyInfo			
algorithm			
AlgorithmIdentifier			Public key algorithm associated with the public key.
algorithm		1.2.840.113549.1.1.1	RSA
parameters		NULL	
subjectPublicKey		BIT STRING	
required extensions			
authorityKeyIdentifier	FALSE		

Field	Criticality Flag	Value	Comments
keyIdentifier		OCTET STRING	
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	
keyUsage	TRUE		
digitalSignature		1	
nonrepudiation		0	
keyEncipherment		1	
dataEncipherment		0	
keyAgreement		0	
keyCertSign		0	
cRLSign		0	
encipherOnly		0	
decipherOnly		0	
certificatePolicies	FALSE		
PolicyInformation			
policyIdentifier		1.3.6.1.4.1.3922.1.1.1.37	
cRLDistributionPoints	FALSE		
DistributionPoint			
distributionPoint			
DistributionPointName			
fullName			
GeneralNames			
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue			
uniformResourceIdentifier		ldap://… or http://...	
authorityInfoAccess	FALSE		
AccessDescription			
accessMethod		(1.3.6.1.5.5.7.48.1)	
accessLocation			
GeneralName			
uniformResourceIdentifier		http://...	
accessMethod		(1.3.6.1.5.5.7.48.2)	
accessLocation			
GeneralName			

Field	Criticality Flag	Value	Comments
uniformResourceIdentifier		ldap://… or http://...	
extKeyUsage	BOOLEAN		This extension MUST appear in certificates issued after June 30, 2019. The extension should be non-critical and shall not include the anyExtendedKeyUsage value. The values listed below for keyPurposeID are recommended for inclusion. Additional keyPurposeIDs, consistent with signing purposes, may be specified. Note: For certificates issued prior to June 30, 2019, anyExtendedKeyUsage may be present or the entire extension may be absent
keyPurposeId	FALSE	1.3.6.1.5.5.7.3.1	Server authentication
		1.3.6.1.5.5.7.3.2	client authentication
subjectAltName	FALSE		
GeneralNames			
GeneralName			
dNSName		IA5String	For devices, this field contains the DNS name of the subject.
dSObjectGuid		GUID	For devices, this field contains the GUID of the subject.
CertificateTemplateName	FALSE	DomainController	

11 BIBLIOGRAPHY

Refer to Appendix C, Applicable Federal and GSA Regulations.

12 ACRONYMS AND ABBREVIATIONS

AIS	Automated Information System
CA	Certification Authority
CARL	Certificate Authority Revocation List
CIAO	Critical Infrastructure Assurance Office
CM	Configuration Management
CMA	Certificate Manufacturing Authority
COMSEC	Communications Security
COOP	Continuity of Operations Plan
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Object Registry
DCID	Director of Central Intelligence Directive
DES	Data Encryption Standard
DITSCAP	Department of Defense Information Technology Security Certification and Accreditation Process
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
EO	Executive Order
ERC	Enhanced Reliability Check
FAR	Federal Acquisition Regulations
FBCA	Federal Bridge Certification Authority

FBCA Operational Authority	Federal Bridge Certification Authority Operational Authority
FCPF	Federal Common Policy Framework
FedCIRC	Federal Computer Incident Response Capability
FED-STD	Federal Standard
FIPS	Federal Information Processing Standards
FIPS PUB	(US) Federal Information Processing Standard Publication
FISCAM	Federal Information System Controls Audit Manual
FPCPF	Federal PKI Common Policy Framework
FPKI	Federal Public Key Infrastructure
FPKI-Prof	Federal PKI X.509 Certificate and CRL Extensions Profile
FPKISC	Federal PKI Steering Committee
FPKIPA	Federal PKI Policy Authority
GAO	(US) General Accounting Office
GPEA	Government Paperwork Elimination Act of 1998
HAG	High Assurance Guard
IATO	Interim Authority to Operate
IAW	In Accordance With
IETF	Internet Engineering Task Force
IS	Information System
ISO	International Organization for Standardization
ISSM	Information System Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology

ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector
ITU-TSS	International Telecommunications Union – Telecommunications System Sector
LAN	Local Area Network
LRA	Local Registration Authority
MOA	Memorandum of Agreement (as used in the context of this CP, between an Agency and the Federal PKI Policy Authority allowing interoperation between the FBCA and Agency Principal CA)
NAC	National Agency Check
NACIC	National Agency Check with Inquiries Credit
NIACAP	National Information Assurance Certification and Accreditation Process
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OID	Object Identifier
OMB	(US) Office of Management and Budget
OPM	(US) Office of Personnel Management
PCCIP	President’s Commission on Critical Infrastructure Protection
PDD	Presidential Decision Directive
PIN	Personal Identification Number
PIV-I	Personal Identity Verification - Interoperable
PMO	Program Management Office
PKCS	Public Key Certificate Standard

PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PMA	Policy Management Authority
PPP	Privacy Practices and Procedures
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SBU	Sensitive But Unclassified
~~SHA-1~~	~~Secure Hash Algorithm, Version 1~~
SHS	Secure Hash Standard
S/MIME	Secure Multipurpose Internet Mail Extension
SO	System Owner
SPM	Security Program Manager
SSL	Secure Sockets Layer
SSP	System Security Plan
TAISS	Telecommunications and Automated Information Systems Security
TSDM	Trusted Software Development Methodology
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
U.S.C.	United States Code
WAN	Wide Area Network
WWW	World Wide Web

13 GLOSSARY

Access
Ability to make use of any information system (IS) resource.

Access Control
Process of granting access to information system resources only to authorized users, programs, processes, or other systems.

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.

Activation Data
Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).

Agency
Any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Executive Branch of the Federal Government.

Agency CA
A CA that acts on behalf of an Agency, and is under the operational control of an Agency.

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.

Archive
Long-term, physically separate storage.

Attribute Authority
An entity recognized by the Federal PKI Policy Authority or comparable Agency 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.

Audit Data
Chronological record of system activities (i.e., audit trail) to enable the reconstruction and examination of the sequence of events and changes in an event.

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.

Backup

Copy of files and programs made to facilitate recovery if necessary.

Binding

Process of associating two related elements of information.

Biometric

A physical or behavioral characteristic of a human being.

CA Facility

The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.

Certificate

A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. As used in this CP, the term "Certificate" refers to certificates that expressly reference the OID of this CP in the "Certificate Policies" field of an X.509 v.3 certificate.

Certificate Management Authority (CMA)

An entity that is delegated or outsourced the task of actually manufacturing the certificate on behalf of a WidePoint NFI CA.

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.

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 Authority

A trusted entity that provides online verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.

Certification
The technical evaluation, made as part of and in support of the accreditation process that establishes the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements.

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.

Certification Authority Software
Key Management and cryptographic software used to manage certificates issued to Subscribers.

Certification Practice 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).

Client (application)
A system entity, usually a computer process acting on behalf of a human user, which makes use of a service provided by a server.

Common Criteria
A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.

Component Private Key
Private key associated with a function of the certificate issuing equipment, as opposed to being associated with an operator or administrator.

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.

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.

Critical Infrastructure

Those physical and cyber-based systems essential to the minimum operations of the economy and government, including but not limited to telecommunications, energy, banking and finance, transportation, water systems, and emergency services, both governmental and private.

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.

Cryptoperiod

Time span during which each key setting remains in effect.

Custodial Subscriber Key

Custodial Subscriber Key Stores hold keys for a number Stores of Subscriber certificates in one location.

Data Encryption Standard (DES)

NIST data encryption standard adopted by the US government as FIPS PUB 46, which allows only hardware implementations of the data encryption algorithm.

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.

Employee

Any person employed by an Agency as defined above.

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

The process of transforming text into an unintelligible form, in such a way that the original data either cannot be obtained, or can be obtained only by using a decryption process.

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.

Federal Bridge Certification Authority (FBCA)

The Federal Bridge Certification Authority consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certificate Practice Statements) that are used to provide peer-to-peer interoperability among Agency Principal Certification Authorities.

Federal Bridge Certification Authority Membrane

The Federal Bridge Certification Authority Membrane consists of a collection of Public Key Infrastructure components including a variety of Certification Authority PKI products, Databases, CA specific Directories, Border Directory, Firewalls, Routers, Randomizers, etc.

FBCA Operational Authority

The Federal Bridge Certification Authority Operational 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 Federal PKI Policy Authority is a Federal Government body responsible for setting, implementing, and administering policy decisions regarding interagency PKI interoperability that uses the FBCA.

Federal Information Processing Standards (FIPS)

These are Federal standards that prescribe specific performance requirements, practices, formats, communications protocols, etc. for hardware, software, data, telecommunications operation, etc. Federal agencies are expected to apply these standards as specified unless a waiver has been granted in accordance to agency waiver procedures.

Firewall

Gateway that limits access between networks in accordance with local security policy.

Government

The U.S. Federal Government and its authorized agencies and entities.

Hardware Token

A sequence of bits or characters, contained in a device such as a smart card, a metal key, or some other physical token, that enables recognition of an entity by a system through personal, equipment, or organizational characters or codes; and the process used to verify the identity of a user and the user's eligibility to access an information system.

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.

Individual Accountability

The principle that requires individual users be held accountable for their actions through technical controls, which associate the identity of the user with the time, method, and degree of access to a system.

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.

Information Technology (IT)

Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services, and related resources.

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. 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.

Interim Authority to Operate (IATO)

When a system does not meet the requirements for accreditation, but the criticality of the system mandates that it become operational, temporary authority to operate may be granted. IATO is contingent upon the implementation of proposed solutions and security actions according to an agreed upon schedule within a specified time period.

Intermediate CA

A CA that is subordinate to another CA, and has a CA subordinate to itself.

Key Changeover

The procedure used by an Authority to replace its own private key (e.g., due to compromise) and replace current valid certificates issued with old key.

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.

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.

Least Privilege

The principle that requires that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks in order to limit the damage that can be caused by accident, error, or unauthorized use.

Legal Non-Repudiation

How well possession or control of the private signature key can be established. See Non-Repudiation.

Life Cycle

Stages through which an information system passes, typically characterized as initiation, development, operation, and termination.

Local Registration Authority (LRA)

A Registration Authority with responsibility for a local community.

Memorandum of Agreement (MOA)

Agreement between the Federal PKI Policy Authority and an Agency allowing interoperability between the Agency Principal CA 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).

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.

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 four 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 CP.

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 Federal PKI Policy Authority.

Principal CA

The Principal CA is a CA designated by an Agency to interoperate with the FBCA. An Agency 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 Agency policy.

Privacy Practices and Procedures (PPP)

A written statement describing policies and procedures for the protection of individual information covered by the Privacy Act as required by OMB Circular A-130 for every computer system maintaining a system of records on behalf of the Federal Government.

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 a WidePoint NFI 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 Agency 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 Management
The total process of identifying, controlling, and eliminating, or minimizing certain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation, and test, security evaluation of safeguards, and overall security review**.**

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.

Router
A special-purpose computer (or software package) that handles the connection between two or more networks. Routers spend all their time looking at the destination addresses of the packets passing through them and deciding on which route to send them.

Rules of Behavior
Rules that have been established and implemented concerning the use of, security in, and acceptable level of risk for the system.

Secret Key
A “shared secret” used in symmetric cryptography, wherein users are authenticated based on a password, Personal Identification Number (PIN), or other information shared between the user and the remote host or server. A single key is shared between two parties: the sender, to encrypt a transmission, and the recipient, to decrypt the transmission, with the shared key being generated with an algorithm agreed to beforehand by the transacting parties.

Sensitivity
The level of protection that information requires. An information

technology environment consists of the system, data, and applications, which must be examined individually and in total. All systems and applications require some level of protection for confidentiality, integrity, and availability, which is determined by an evaluation of the sensitivity and criticality of the information processed, the relationship of the system to the organization's mission, and the economic value of the system components.

Separation of Duties

Principle by which roles and responsibilities are divided among individuals so that a single individual cannot subvert a critical process.

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).

Suspend (a certificate)

To temporarily suspend the operational period of a Certificate for a specified time period or from a specified time forward.

Symmetric Key

A key that can be used to encrypt and decrypt the same data.

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.

System Security Plan (SSP)

Documentation of the management, technical, and operational security controls of a Federal automated information system as required by OMB Circular A-130.

Technical non-repudiation

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. See Non-Repudiation

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.

Token

Object that a user possesses for the purpose of I&A. Tokens are characterized as “memory tokens” and “smart tokens.” Memory tokens store but do not process information. Special reader/writer devices control the reading and writing of data to and from the token. Smart tokens incorporate one or more integrated circuit into the token. Smart tokens are typically ‘unlocked’ through the use of a PIN or password.

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 Agency in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.

Trusted Certificate

A certificate that is trusted by the Relying Party on the basis of secure 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.

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.

Valid Certificate

A certificate that (1) a WidePoint NFI CA has issued, (2) the Subscriber listed in it has accepted, (3) has not expired, and (4) has not been revoked. Thus, a certificate is not “valid” until it is both issued by a WidePoint NFI CA and has been accepted by the Subscriber.

Vulnerability Assessment

An analysis of flaws or weaknesses in security procedures, technical controls, physical controls or other controls that may allow harm to occur to an automated information system.

Zeroize

A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data.

APPENDIX A. PIV-INTEROPERABLE SMART CARD DEFINITION

The following requirements shall apply to PIV-I Cards:

1. To ensure interoperability with Federal systems, PIV-I Cards shall 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. PIV-I Cards shall conform to [NIST SP 800-73].
3. The mandatory X.509 Certificate for Authentication shall be issued under a policy that is cross certified with the FBCA PIV-I Hardware policy OID.
4. All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile].
5. PIV-I Cards shall 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. PIV-I Cards shall contain an electronic representation (as specified in SP 800-73 and SP 800-76) of the Cardholder 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 PIV-I Cards.
8. Visual distinction of a 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 a PIV-I Card shall not be placed entirely within Zone 11, Agency Seal, as defined by [FIPS 201].
9. The PIV-I Card physical topography shall include, 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. PIV-I Cards shall have an expiration date not to exceed 5 years of issuance.
11. Expiration of the PIV-I Card should not be later than expiration of PIV-I Content Signing certificate on the card.
12. The digital signature certificate that is used to sign objects on the PIV-I Card (e.g., CHUID, Security Object) shall contain a policy OID that has been mapped to the FBCA PIV-I Content Signing policy OID. The PIV-I Content Signing certificate shall conform to [PIV-I Profile].

13. The PIV-I Content Signing certificate and corresponding private key shall be managed within a trusted Card Management System as defined by Appendix B.
14. At issuance, the RA shall activate and release the PIV-I Card to the subscriber only after a successful 1:1 biometric match of the applicant against the biometrics collected in Section 3.2.3.1.
15. 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 shall perform a challenge response protocol using cryptographic keys stored on the card in accordance with [SP800-73]. When cards are personalized, card management keys shall be set to be specific to each PIV-I Card. That is, each PIV-I Card shall contain a unique card management key. Card management keys shall 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

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

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

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.

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

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

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

A formal configuration management methodology shall be used for installation and ongoing maintenance of the CMS. Any modifications and upgrades to the CMS shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the CMS.

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

All Trusted Roles who operate a CMS shall 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

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.
CCP-PROF	X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers Program
FBCA CP	X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA) / Version 2.32 / 4 April 2018
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
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
GSA IT Security Policy	GSA Order CIO P 2100.1D, GSA Information Technology (IT) Security Policy, June 27, 2007
GSA IT Sec 06-30	IT Procedural Guide: Managing Enterprise Risk (Security Categorization, Risk Assessment, and Certification and Accreditation)
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.
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-PROF	X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards, April 23, 2010.

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

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.