WIDEPOINT PERSONAL IDENTITY VERIFICATION

SHARED SERVICE PROVIDER

(WIDEPOINT PIV SSP)

CERTIFICATE PRACTICE STATEMENT

(CPS)

Version 4.2.4

24 July 2020

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

Notice: Operational Research Consultants, Inc. (ORC), a wholly-owned subsidiary of WidePoint Corporation, has changed its legal name to WidePoint Cybersecurity Solutions Corporation, hereafter referred to simply as WidePoint. This is a legal name change only for branding purposes with no change to ownership, corporation type or other status. 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.

TABLE OF CONTENTS

LIST OF TABLES

1 INTRODUCTION

This WidePoint Personal Identity Verification Shared Service Provider Certification Practices Statement, hereafter, referred to as the “WidePoint PIV SSP CPS” is the guiding document for the WidePoint Personal Identity Verification Shared Service Provider Program, hereafter, referred to as the “WidePoint PIV SSP”, The WidePoint PIV SSP operates under the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework (v1.30 dated October 4, 2018) hereafter referred to as “FCPCF” as an authorized component of the Federal Public Key Infrastructure, hereafter, referred to as “FPKI” as governed by the Federal Public Key Infrastructure Policy Authority, hereafter, referred to as “FPKIPA”.

Only Certificate Authorities authorized to operate in accordance with the FPCPF may assert the FPKI Common Policy Certificate Policy Object Identifiers (OIDs) in digital certificates, WidePoint, having completed a compliance audit approved by the FPKIPA, attained an Authority to Operate (ATO) for providing public key certificate services under the FPCPF.

WidePoint PIV SSP public key certificates fall within the following certificate policies:

- A policy for users with software cryptographic modules
- A policy for users with hardware cryptographic modules
- A policy for devices with software cryptographic modules
- A user authentication policy
- A card authentication policy
- A PIV content signing policy
- A Derived-PIV authentication policy
- A Derived-PIV hardware authentication policy

Where a specific policy is not stated, the policies and procedures in this WidePoint PIV SSP CPS apply equally to all policies.

The user policies governing WidePoint PIV SSP certificates apply to Federal employees, contractors, and other affiliated personnel requiring PKI credentials for the purposes of authentication, signature, and confidentiality with federal systems that have not been designated by law as national security systems. The device policy applies to devices operated by or on behalf of federal agencies.

FPCPF requires the use of FIPS 140 validated cryptographic modules by federal employees, contractors and other affiliated personnel for all cryptographic operations and the protection of trusted public keys. Software and hardware cryptographic mechanisms are equally acceptable under the FPCPF. The policies for users with hardware cryptographic modules mandate Level 2 validation.

The WidePoint PIV SSP will provide the following security management services:

- Key generation/storage
- Certificate generation, modification, re-key, 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)

For entities associated with the Federal Common Policy Root CA (FCPCA), the FPCPF requires the use of either 2048 bit RSA keys or 256-bit elliptic curve keys along with the SHA-256 and SHA-384 hash algorithms. WidePoint PIV SSP Certificate Authorities, hereafter, referred to as "WidePoint PIV SSP CAs" are required to use SHA-256 or SHA-384.

FPCPF and this WidePoint PIV SSP CPS are consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 3647 Certificate Policy and Certification Practices Framework.

The terms and provisions of these certificate policies will be interpreted under and governed by applicable Federal law.

1.1 OVERVIEW

1.1.1 CERTIFICATE POLICY

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

1.1.2 RELATIONSHIP BETWEEN THE CP AND THE CPS

This WidePoint PIV SSP CPS is subordinate to the FPCPF, Version 1.31 dated February 8, 2019. The FPCPF states what assurance can be placed in a certificate issued by the WidePoint PIV SSP CAs. This WidePoint PIV SSP CPS states how the WidePoint PIV SSP CA(s) establishes that assurance. The policies and procedures in this WidePoint PIV SSP CPS are applicable to individuals who manage the certificates, who directly use these certificates, and individuals who are responsible for applications or servers that rely on these certificates.

1.1.3 SCOPE

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

1.1.4 INTEROPERATION BETWEEN THE WIDEPOINT PIV SSP AND CAS ISSUING UNDER DIFFERENT POLICIES

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

1.2 DOCUMENT NAME AND IDENTIFICATION

The FPCPF certificate policies are registered with the Computer Security Objects Register (CSOR) at the National Institute of Standards and Technology (NIST). Certificates issued by the WidePoint PIV SSP CAs, in accordance with the FPCPF and this WidePoint PIV SSP CPS, assert at least one of the certificate policies OIDs listed in the table below. The WidePoint PIV SSP and each WidePoint PIV SSP CA issues certificates and complies with this WidePoint PIV SSP CPS and assert at least one of the FPCPF certificate policies as listed in in Table 1 below:

Description	Certificate Policy OID
id-fpki-common-policy	::= {2 16 840 1 101 3 2 1 3 6}
id-fpki-common-hardware	::= {2 16 840 1 101 3 2 1 3 7}
id-fpki-common-devices	::= {2 16 840 1 101 3 2 1 3 8}
id-fpki-common-authentication	::= {2 16 840 1 101 3 2 1 3 13}
id-fpki-common-cardAuth	::= {2 16 840 1 101 3 2 1 3 17}
id-fpki-common-piv-contentSigning	::= {2 16 840 1 101 3 2 1 3 39}
id-fpki-common-derived-pivAuth	::= {2 16 840 1 101 3 2 1 3 40}
id-fpki-common-derived-pivAuth-hardware	::= {2 16 840 1 101 3 2 1 3 41}

Table 1: id-fpki-Common Policy OIDs

Certificates issued to CAs may contain a subset of these OIDs. Certificates issued to users, other than devices, asserting a certificate policy OID to support digitally signed documents or key management, contain either the id-fpki-common-policy or id-fpki-common-hardware. Certificates issued to devices under this policy which use FIPS 140 Level 2 or higher

cryptographic modules include id-fpki-common-devices. Subscriber certificates issued to devices under this policy using software cryptographic modules include id-fpki-common-devices.

This WidePoint PIV SSP CPS includes five (5) certificates specific to FIPS 201 Personal Identity Verification (PIV) for issuance to federal employees and contractors:

- Certificates issued to users supporting authentication but not digital signature, where the corresponding private key is stored on a PIV card, contain id-fpki-common-authentication.
- Certificates issued to users supporting authentication where the private key is stored on a PIV card and can be used without user authentication contain id-fpki-common-cardAuth.
- Certificates issued to users in accordance with NIST SP800-157, supporting authentication but not digital signature, where the corresponding private key is not stored on a PIV card, contain either id-fpki-common-derived-pivAuth-hardware when issued in a manner which meets the requirements for Level 4 authentication as defined by OMB's guidance for E-Authentication; or id-fpki-common-derived-pivAuth for Level 3.
- The id-fpki-common-piv-contentSigning policy is only asserted in certificates issued to devices that sign PIV Card objects in accordance with FIPS 201 or SP800-157.

WidePoint certificates issued under this WidePoint PIV SSP CPS reference the FPCPF by including the appropriate certificate policy OID, identified above, in the *Certificate Policies* field. Additionally, each WidePoint PIV SSP CA that issues certificates will hold a certificate signed by the Federal Common Policy Root CA, hereafter referred to as the "FCPCA" or an Authorized CA that holds a certificate signed by the FCPCA. WidePoint PIV SSP issued certificates containing the FPCPF certificate policy OIDs may not be used except as specifically authorized by this WidePoint PIV SSP CPS and the FPCPF. Unless specifically approved by the FFPKIPA, only the certificate policy OIDs identified above are used in WidePoint PIV SSP certificates.

1.3 PKI PARTICIPANTS

The following are roles relevant to the administration and operation of WidePoint PIV SSP CAs operating under this WidePoint PIV SSP CPS and the FPCPF.

1.3.1 PKI AUTHORITIES

1.3.1.1 FEDERAL CHIEF INFORMATION OFFICERS COUNCIL

The Federal CIO Council comprises the Chief Information Officers of all cabinet level departments and other independent agencies. The Federal CIO Council has established the framework for the interoperable Federal PKI (FPKI) and oversees the operation of the

organizations responsible for governing and promoting its use. In particular, the Common Policy was established under the authority of and with the approval of the Federal CIO Council.

1.3.1.2 FEDERAL PKI POLICY AUTHORITY (FPKIPA)

The Federal PKI Policy Authority (FPKIPA) is a group of U.S. Federal Government Agencies (including cabinet-level Departments) chartered by the Federal CIO Council. The FPKIPA owns the Common Policy and represents the interest of the Federal CIOs. The FPKIPA is responsible for:

- Maintaining the CP
- Approving the CPS for each CA that issues certificates under the Common Policy
- Approving the compliance audit report for each CA issuing certificates under the Common Policy
- Ensuring continued conformance of each CA that issues certificates under the Common Policy with applicable requirements as a condition for allowing continued participation

1.3.1.3 FPKI MANAGEMENT AUTHORITY (FPKIMA)

The FPKIMA is the organization that operates and maintains the Common Policy Root CAs on behalf of the U.S. Government, subject to the direction of the FPKIPA.

1.3.1.4 FPKI MANAGEMENT AUTHORITY PROGRAM MANAGER

The Program Manager is the individual within the FPKI Management Authority who has principal responsibility for overseeing the proper operation of the Common Policy Root CAs including the required repository, and selecting the FPKI Management Authority staff. The Program Manager is selected by the FPKI Management Authority and reports to the FPKIPA. The FPKI Management Authority Program Manager must hold a Top Secret security clearance.

1.3.1.5 POLICY MANAGEMENT AUTHORITY

WidePoint's Chief Security Officer is responsible for maintaining this CPS and for ensuring that all WidePoint PIV SSP components are operated in compliance with this WidePoint PIV SSP CPS. This is referred to as the WidePoint PIV SSP PMA within this WidePoint PIV SSP CPS.

Agencies that contract for the services of the WidePoint PIV SSP under this WidePoint PIV SSP CPS and the Common Policy shall establish a management body to manage any agency-operated components (e.g., RAs or repositories) and resolve name space collisions. This body shall be referred to as an Agency Policy Management Authority, or Agency PMA.

An SSP PMA shall be responsible for notifying its customer Agency PMAs and 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.

An Agency PMA is responsible for ensuring that all Agency-operated PKI components (e.g., CAs, CSSs, CMSs, RAs) are operated in compliance with the Common Policy and This WidePoint PIV SSP CPS, and shall serve as the liaison for that agency to the FPKIPA and the WidePoint PIV SSP PMA.

1.3.1.6 AUTHORIZED WIDEPOINT PIV SSP CAS

A WidePoint PIV SSP CA is the collection of hardware, software and operating personnel that create, sign, and issue public key certificates to subscribers. The WidePoint PIV SSP is authorized by the FPKIPA and may issue certificates that contain FPCPF certificate policies. The WidePoint PIV SSP has been certified by:

- Documenting the specific implemented practices and procedures under which the WidePoint PIV SSP satisfies the requirements of the FPCPF in the WidePoint PIV SSP CPS.
- Successfully completing Security Certification and Accreditation (C&A) in accordance with Federal laws, GSA regulations, and guidelines.

WidePoint is responsible for all aspects of the issuance and management of WidePoint PIV SSP Certificates, including:

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

WidePoint is responsible for ensuring that all work is performed under the supervision of WidePoint or designated Agency personnel, and provides assurance of the trustworthiness and competence of employees and their satisfactory performance of duties relating to provision of the WidePoint PIV SSP services. Each WidePoint PIV SSP CA or employee of WidePoint to whom information may be made available or disclosed is notified in writing by the WidePoint PIV SSP that information so disclosed to the WidePoint PIV SSP or it's employees can be used only for the purposes and to the extent authorized herein.

The WidePoint PIV SSP complies with all applicable Federal and GSA requirements, including those for the prevention and reporting of waste, fraud, and abuse.

1.3.1.7 CERTIFICATE STATUS SERVERS

The WidePoint PIV SSP operates a Certificate Status Server, hereafter referred to as the "WidePoint PIV SSP CSS", using an OCSP responder that provides revocation status and/or certificate validation responses. How to obtain revocation information is provided on the certificate request website. The WidePoint PIV SSP CSS practices conform to the stipulations of the FPCPF and this WidePoint PIV SSP CPS. The WidePoint PIV SSP CSS asserts all the certificate policy OIDs for which it is authoritative. All WidePoint PIV SSP CSS practice updates, as well as any subsequent changes are updated in this WidePoint PIV SSP CPS and submitted to the FPKIPA for conformance assessment. The WidePoint PIV SSP CSS practices include:

- Conformance to the stipulations of the FPCPF and this WidePoint PIV SSP CPS.
- Ensuring that certificate and revocation information is accepted only from valid WidePoint PIV SSP CAs.
- Providing only valid and appropriate responses.
- Asserting all the certificate policy OIDs for which it is authoritative.
- Maintaining evidence of due diligence being exercised in validating certificate status.

1.3.1.8 KEY ESCROW DATABASE (WIDEPOINT KED)

The WidePoint KED is the subsystem that maintains the escrowed private key repository and responds to key registration requests. The WidePoint KED responds to key recovery requests from two or more KRAs or self-recovery by a current subscriber.

1.3.2 REGISTRATION AUTHORITIES

Registration Authorities (RAs) for the WidePoint PIV SSP CAs, are human and non-human entities. WidePoint PIV SSP RAs (human) are approved by a WidePoint PIV SSP Certificate Authority Administrator, hereafter referred to as "WidePoint PIV SSP CAA", or by another WidePoint PIV SSP RA. WidePoint PIV SSP RAs (non-human) are approved via the WidePoint Configuration Control Board (CCB) prior to installation.

For certificates asserting id-fpki-common-hardware, id-fpki-common-authentication, id-fpki-common-cardAuth, and id-fpki-common-derived-pivAuth, and id-fpki-common-derived-pivAuth-hardware, the WidePoint PIV SSP Card Management System, herafter referred to as WidePoint PIV SSP CMSs, are issued a connector certificate for secure authentication to WidePoint PIV SSP CAs. The connector certificate is an administrative certificate issued by the WidePoint PIV

SSP CAs which authorizes WidePoint PIV SSP CMSs to request certificates and certificate revocations of WidePoint PIV SSP CAs.

WidePoint PIV SSP RAs are responsible for:

- Control over the registration process
- The identification and authentication process

1.3.3 KEY RECOVERY AGENT (KRA)

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

1.3.4 KEY RECOVERY REQUESTORS

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

1.3.4.1 SUBSCRIBER

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

1.3.4.2 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 WidePoint SSP. A list of personnel authorized to make such a request is provided to WidePoint by the Customer.

1.3.4.3 External Third-Party Requestor

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

1.3.5 Trusted Agents

A Trusted Agent is a person who satisfies all the trustworthiness requirements for a WidePoint PIV SSP RA and who performs identity proofing as a proxy for the WidePoint PIV SSP RA for WidePoint PIV SSP credentials asserting id-fpki-common-authentication and id-fpki-common-cardAuth. The Trusted Agent records information from applicants and verifies biometrics (e.g., photographs) on presented credentials when the applicant appears in-person before the Trusted Agent. Within the WidePoint PIV SSP, three roles serve as Trusted Agents:

- WidePoint PIV SSP Sponsor
- WidePoint PIV SSP Registrar
- WidePoint PIV SSP Issuer

The responsibilities of these roles are detailed in Section 5.2.1.5.

1.3.6 Subscribers

A subscriber is the End Entity (EE) whose name appears as the subject in a certificate, and who asserts that it uses its key and certificate in accordance with this WidePoint PIV SSP CPS. Subscribers are limited to Federal employees, contractors, affiliated personnel, and devices operated by or on behalf of Federal agencies. CAs are sometimes technically considered "subscribers". However, the term "subscriber" as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information.

WidePoint PIV SSP CMSs are technically subscribers and are responsible for managing smart card token content. WidePoint PIV SSP CMSs are only issued PIV Content Signing certificates and Connector Certificates and are not issued any certificates that express any other FPCPF certificate policy OID. Review of the certificate profile information contained within this WidePoint PIV SSP CPS verifies that only a Content Signing Certificate and a Connector Certificate are issued to a WidePoint PIV SSP CMS.

1.3.6.1 PKI SPONSOR

A WidePoint PIV SSP PKI Sponsor fills the role of a Subscriber for non-human system components (non-FIPS 201) and organizations that are named as public key certificate subjects. The WidePoint PIV SSP PKI Sponsor works with the WidePoint WidePoint PIV SSP RAs and/or LRAs, to register components (routers, firewalls, etc.) in accordance with Section 3.2.3.2, and is responsible for meeting the obligations of Subscribers as defined throughout this document. A WidePoint PIV SSP PKI Sponsor is not considered a trusted role.

1.3.7 RELYING PARTIES

A Relying Party is any entity that wishes to validate the binding of a public key to the name (or role) of a federal employee, contractor, or other affiliated personnel. A Relying Party uses a subscriber's certificate to:

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

At one's own risk, 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.

1.3.8 OTHER PARTICIPANTS

1.3.8.1 CERTIFICATE MANAGEMENT AUTHORITY(S) (CMA)

The WidePoint PIV SSP is responsible for the functions of manufacturing, issuance, suspension, and revocation of all WidePoint PIV SSP certificates.

The WidePoint PIV SSP CAs, RAs and LRAs are considered "Certificate Management Authorities" (CMAs). The term CMA refers to a function assigned to either WidePoint PIV SSP CAs or RAs, or to both CAs and RAs.

Certificate Status Servers (CSSs) such as Online Certificate State Protocol (OCSP) Responders operated by the WidePoint PIV SSP are also considered CMAs. The WidePoint PIV SSP will operate an OCSP Responder in support of the WidePoint PIV SSP.

The WidePoint PIV SSP is responsible for ensuring that all WidePoint PIV SSP CMAs (i.e., the CA, CSSs, RAs, and LRAs) are in compliance with the FPCPF and this WidePoint PIV SSP CPS.

1.3.8.2 LOCAL REGISTRATION AUTHORITIES (LRAS)

WidePoint PIV SSP RAs may delegate the identity proofing tasks to Local Registration Authorities (LRAs) who have been approved by a WidePoint PIV SSP RA. Upon performing their duties, WidePoint PIV SSP LRAs provide verification to the WidePoint PIV SSP RA. If a WidePoint PIV SSP RA delegates duties to one or more WidePoint PIV SSP LRAs, the WidePoint PIV SSP RA informs all other WidePoint PIV SSP RAs. WidePoint PIV SSP LRAs may not designate other LRAs. Approval of certificates may only be approved by WidePoint PIV SSP RA certificate holders of equal or higher levels of assurance. WidePoint PIV SSP LRAs can be WidePoint employees on location at a subscriber's agency or employees of a subscriber's agency.

LRAs are obligated to accurately enter Applicant's information into the system. LRAs may not designate other LRAs under This WidePoint PIV SSP CPS. LRAs under This WidePoint PIV SSP CPS are not authorized to assume any other CA administration functions.

1.3.8.3 SERVICE PROVIDERS

Various service providers support aspects of the WidePoint PIV SSP infrastructure, such as:

- Verizon – ISP
- Sprint – ISP
- Paetech – ISP (phone system only)
- Equinix – Disaster Recovery co-location site
- Fidelity Mechanical Services - HVAC
- Truland Service Corp.- Diesel Generator
- Fannon – Diesel Fuel
- Static Power – Uninterruptable Power Supply (UPS)
- PC Recycler – Electronics recycling and degaussing

WidePoint maintains business relationships, contracts and/or service agreements with these service providers to ensure each respective provider's services are formally defined, and in order to maintain properly functioning equipment and services for the WidePoint PIV SSP infrastructure.

1.3.9 RELATIONSHIP TO PKI AUTHORITIES FROM CP

The applicable requirements for physical, personnel, and procedural security controls (*X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 5; *WidePoint*

SSP CPS, Section 5), technical security controls (*X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 6; *WidePoint SSP CPS,* Section 6), and Compliance Audit (*X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 8; *WidePoint SSP CPS*,, Section 8) are applied to the PKI Authorities in this CPS as follows:

- CA requirements are applied to the KED
- RA requirements are applied to the KRA and KRA automated systems

1.4 CERTIFICATE USAGE

1.4.1 APPROPRIATE CERTIFICATE USES

The sensitivity of the information processed or protected using certificates issued by the WidePoint PIV SSP will vary significantly. Organizations 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 organization for each application and is not controlled by this WidePoint PIV SSP CPS.

This WidePoint PIV SSP CPS is intended to support the use of validated public keys to access Federal systems that have not been designated national security systems. While a validated public key is not generally sufficient to grant access the key may be sufficient when supplemented by appropriate authorization mechanisms. Credentials issued under this WidePoint PIV SSP CPS may also be used for key establishment. This policy is intended to support applications involving unclassified information, which can include sensitive unclassified data protected pursuant to federal statutes and regulations.

Credentials issued under the id-fpki-common-policy and id-fpki-common-derived-pivAuth policies are intended to meet the requirements for Level 3 authentication, as defined by the OMB E-Authentication Guidance. Credentials issued under the id-fpki-common-hardware, id-fpki-common-authentication, id-fpki-common-derived-pivAuth-hardware, and id-fpki-common-High policies meet the requirements for Level 4 authentication, as defined by the OMB E-Authentication Guidance.

Credentials issued under the id-fpki-common-piv-contentSigning policy are intended to meet the requirements in FIPS 201 and SP 800-157 as the digital signatory of the PIV Card Holder Unique Identifier (CHUID) and associated PIV data objects.

In addition, the FPCPF and this WidePoint PIV SSP CPS may support signature and confidentiality requirements for Federal Government processes.

1.4.2 PROHIBITED CERTIFICATE USES

This WidePoint PIV SSP CPS prohibits the use of any application that does not follow approved standards for the storage and transmittal of cryptographic information. Applicable standards include:

- FIPS 140-2, Security Requirements for Cryptographic Modules

- FIPS 180-4, Secure Hash Algorithm
- FIPS 186-4, Digital Signature Standard
- PKCS #11 Hardware Format
- PKCS #12 Software Format
- X.509 v23 Information Technology – ASN.1 Encoding Rules 1994
- ANSI X9.31 American National Standard for Digital Signature using Reversible Public Key Cryptography for the Financial Service Industry

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

1.5 POLICY ADMINISTRATION

1.5.1 ORGANIZATION ADMINISTERING THE DOCUMENT

The Chief Security Officer of WidePoint administers the WidePoint PIV SSP. The WidePoint Policy Authority is responsible for registration, maintenance, and interpretation of this WidePoint PIV SSP CPS.

WidePoint Policy Authority
South Tower, Suite 210
11250 Waples Mill Road
Fairfax, Virginia 22030

1.5.2 CONTACT PERSON

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

Caroline Godfrey, EVP, Chief Security Officer
South Tower, Suite 210
11250 Waples Mill Road
Fairfax, Virginia 22030
CGodfrey@WidePoint.com

1.5.3 PERSON DETERMINING WIDEPOINT PIV SSP CPS SUITABILITY FOR THE FPCPF

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

The FPKIPA approves the CPS for each CA that issues certificates under the FPCPF.

1.5.4 CPS Approval Procedures

CAs issuing certificates under the FPCPF are required to meet all facets of the policy. The FPKIPA will not issue waivers.

The WidePoint PIV SSP CAs and WidePoint PIV SSP RAs must meet all requirements of this approved WidePoint PIV SSP CPS before commencing operations. The FPKIPA makes the determination that this WidePoint PIV SSP CPS complies with the policy. 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.

In each case, the determination of suitability will be based on an independent compliance auditor's results and recommendations. See Section 8 for further details.

1.6 Definitions and Acronyms

See Section 11 and Section 12.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

The WidePoint PIV SSP maintains a master directory protected by a firewall and accessible through the Internet. Information in WidePoint PIV SSP repositories is protected in accordance with the Privacy Act of 1974 as set forth in WidePoint's Privacy Policy and Procedures documents.

Updating the repository is restricted only to authorized individuals using certificate authenticated access control over SSL. The directory is configured by the WidePoint PIV SSP CAA to recognize WidePoint PIV SSP RAs and CAAs as authorized to make changes. The WidePoint PIV SSP protects any and all repository information not intended for public dissemination or modification.

The WidePoint PIV SSP Repository is responsible for:

- Maintaining a secure system for storing and retrieving certificates.
- Maintaining a current, redacted summary of this WidePoint PIV SSP CPS.
- Maintaining other information relevant to certificates.
- Providing information regarding the status of certificates as valid or invalid that can be determined by a relying party.

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

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

The WidePoint PIV SSP posts WidePoint PIV SSP CRLs at the following location, accessible via HTTP:

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

The WidePoint PIV SSP posts certificates and CRL information in a repository established by the WidePoint PIV SSP. Only publicly available information contained in the certificate(s) is posted in this directory to ensure compliance with the Privacy Act of 1974. WidePoint PIV SSP CAs certificate information access are available via:

- https://orc.widepoint.com/certificates-and-credentials/hspd-12-piv/

The WidePoint PIV SSP certificate repository meets the following obligations:

- To list all un-expired WidePoint PIV SSP CA certificates for relying parties

- To contain an accurate and current CRL for the respective WidePoint PIV SSP CAs for use by relying parties
- To be publicly accessible
- To be available, via certificate-authenticated access control over SSL, for authorized requests coordinated with the WidePoint PIV SSP Point of Contact designated in Section 1.5.2 during normal business hours for the operating organization
- To be maintained in accordance with the practices specified in this WidePoint PIV SSP CPS
- To meet or exceed the requirement of 99% availability for all components within the control of the operating organization

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

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 PUBLICATION OF CERTIFICATES AND CERTIFICATE STATUS

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

- Current, complete, and accurate CRLs
- A copy or link to the current Common Policy
- A summary of this approved CPS

The repository is located at https://orc.widepoint.com/certificates-and-credentials/hspd-12-piv/. WidePoint PIV SSP publicly accessible repository system has been designed and implemented so as to provide 99% availability overall and limit scheduled down-time to 0.5% annually. The WidePoint PIV SSP CSS has also been designed and implemented so as to provide 99% availability overall and limit scheduled down-time to 0.5% annually.

2.2.2 PUBLICATION OF CA INFORMATION

The FPCPF document is publicly available on the FPKIPA website (see https://www.idmanagement.gov/IDM/s/). Only a redacted version of this WidePoint PIV SSP CPS will be publicly available from the WidePoint PIV SSP website (see https://orc.widepoint.com/certificates-and-credentials/hspd-12-piv/). A copy of the current WidePoint PIV SSP annual PKI Compliance Audit Letter will also be posted to the WidePoint PIV SSP website (https://orc.widepoint.com/certificates-and-credentials/hspd-12-piv/).

2.2.3 INTEROPERABILITY

WidePoint PIV SSP CA certificates and CRLs issued under this WidePoint PIV SSP CPS are published as specified. A redacted version of This WidePoint PIV SSP CPS will be updated and published consistent with approved updated versions of the full CPS.

2.2.4 TIME OR FREQUENCY OF PUBLICATION

WidePoint PIV SSP CA certificates are published to a repository at the time of issuance. WidePoint PIV SSP CRL publication is in accordance with Section 4.9. Frequency of WidePoint PIV SSP CRL publication is in accordance with Section 4.9.7.

2.3 ACCESS CONTROLS ON REPOSITORIES

The WidePoint PIV SSP protects CA and Repository information not intended for public dissemination or modification. Access to WidePoint PIV SSP Certificates and status information is in accordance with the FPCPF and this WidePoint PIV SSP CPS. Access controls include:

- Physical access to WidePoint PIV SSP CAs and OCSP server(s) are controlled by job requirements and authentication, as stipulated in Section 5.1.2.
- WidePoint employees are only able to access those resources that they require to accomplish the tasks they are assigned, as stipulated in this WidePoint PIV SSP CPS (access rights are assigned by resource [server, computer, share, volume, printer, etc.]).
- User authentication is via certificate authentication (or UserID and password when appropriate) and data encryption is used, as stipulated in this WidePoint PIV SSP CPS.
- WidePoint employees are assigned access rights before accessing any electronic resources.
- The WidePoint Corporate Security Auditor determines and periodically reviews user access rights.

The WidePoint PIV SSP CAAs and WidePoint PIV SSP System Administrators, hereafter referred to as WidePoint PIV SSP SAs are notified of any changes that affect employee access rights.

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

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

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 TYPES OF NAMES

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

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

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

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

The organizational units department and agency appear when applicable and are used to specify the federal entity that employs the subscriber. At least one of these organizational units must appear in the DN. The additional organizational unit *structuralcontainer* is permitted to support local directory requirements, such as differentiation between human subscribers and devices. This organizational unit may not be employed to further differentiate between subcomponents within an agency.

The distinguished name of the federal employee subscriber will be one of the three following forms:

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

In the first name form, nickname may be the subscriber's first name, a form of the first name, middle name, or pseudonym (e.g., Buck) by which the subscriber is generally known. A generational qualifier, such as "Sr." or "III", may be appended to any of the common name forms specified above.

Distinguished names assigned to federal contractors and other affiliated persons will be within the same directory information tree. The distinguished name of the federal contractor subscribers and affiliate subscribers will take one of the three following forms:

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

For names assigned to federal contractors and other affiliated persons, generational qualifiers may be inserted between lastname and "(affiliate)".

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

Certificates issued under id-fpki-common-authentication include a subject alternative name. The subject alternative name extension includes the pivFASC-N name type. The value for this name is the FASC-N of the subject's PIV card. The subject alternative name extension includes the UUID from the GUID data element of the CHUID. The UUID is included as a URI as specified in section 3 of RFC 4122.

Certificates issued under id-fpki-common-cardAuth include the UUID from the GUID data element of the CHUID. The UUID is included as a URI as specified in section 3 of RFC 4122. Certificates issued under id-fpki-common-cardAuth will not include any other name in the subject alternative name extension but may include a non-NULL name in the subject field. If included, the subject distinguished name shall take one of the following forms:

- C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=structuralcontainer], serialNumber=FASC-N
- dc=gov, dc=org0, [dc=org1], …, [dc=orgN], [ou=structuralcontainer], serialNumber=FASC-N
- dc=mil, dc=org0, [dc=org1], …, [dc=orgN], [ou=structuralcontainer], serialNumber=FASC-N
- C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=structuralcontainer], serialNumber=UUID
- dc=gov, dc=org0, [dc=org1], …, [dc=orgN], [ou=structuralcontainer], serialNumber=UUID
- dc=mil, dc=org0, [dc=org1], …, [dc=orgN], [ou=structuralcontainer], serialNumber=UUID

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

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

Distinguished names based on Internet domain component names shall be in the following directory information trees:

- dc=gov, dc=org0, [dc=org1], …, [dc=orgN], [ou=structuralcontainer]
- dc=mil, dc=org0, [dc=org1], …, [dc=orgN], [ou=structuralcontainer]

The default Internet domain name for the agency [orgN.]…[org0].gov or [orgN.]…[org0].mil, will be used to determine DNs. The first domain component of the DN will either be dc=gov or dc=mil. At a minimum, the org0 domain component must appear in the DN. The org1 to orgN domain components appear, in order, when applicable and are used to specify the federal entity that employs the subscriber.

Distinguished names for federal employee Subscribers will take one of the following forms when their agency's Internet domain name ends in .gov:

- dc=gov, dc=org0, [dc=org1], …, [dc=orgN], [ou=structuralcontainer], cn=<nickname lastname>
- dc=gov, dc=org0, [dc=org1], …, [dc=orgN], [ou=structuralcontainer], cn=<firstname initial. lastname>
- dc=gov, dc=org0, [dc=org1], …, [dc=orgN], [ou=structuralcontainer], cn=<firstname middlename lastname>

Distinguished names for federal employee Subscribers will take one of the following forms when their agency's Internet domain name ends in .mil:

- dc=mil, dc=org0, [dc=org1], …, [dc=orgN], [ou=structuralcontainer], cn=<nickname lastname>
- dc=mil, dc=org0, [dc=org1], …, [dc=orgN], [ou=structuralcontainer], cn=<firstname initial. lastname>
- dc=mil, dc=org0, [dc=org1], …, [dc=orgN], [ou=structuralcontainer], cn=<firstname middlename lastname>

Distinguished names for federal contractors and affiliated persons will take one of the following forms when their agency's Internet domain name ends in .gov:

- dc=gov, dc=org0, [dc=org1], …, [dc=orgN], [ou=structuralcontainer], cn=<nickname lastname> (affiliate)
- dc=gov, dc=org0, [dc=org1], …, [dc=orgN], [ou=structuralcontainer], cn=<firstname initial. lastname> (affiliate)
- dc=gov, dc=org0, [dc=org1], …, [dc=orgN], [ou=structuralcontainer], cn=<firstname middlename lastname> (affiliate)

Distinguished names for federal contractors and affiliated persons will take one of the following forms when their agency's Internet domain name ends in .mil:

- dc=mil, dc=org0, [dc=org1], …, [dc=orgN], [ou=structuralcontainer], cn=<nickname lastname> (affiliate)
- dc=mil, dc=org0, [dc=org1], …, [dc=orgN], [ou=structuralcontainer], cn=<firstname initial. lastname> (affiliate)
- dc=mil, dc=org0, [dc=org1], …, [dc=orgN], [ou=structuralcontainer], cn=<firstname middlename lastname> (affiliate)

For subscriber certificates asserting the following OID, id-fpki-common-piv-contentsigning, the distinguished name will take the following form in the following two cases:

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

Where "ID" equals unique qualifier assigned by organization (e.g. CN=EPA 1 PIV Content Signer; CN=EPA 2 PIV Content Signer).

Devices that are the subject of certificates issued under this policy shall be assigned either a geo political name or an Internet domain component name. Device names shall take one of the following forms where device name is a descriptive name for the device:

- C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=structuralcontainer], cn=<device name>
- dc=gov, dc=org0, [dc=org1], …, [dc=orgN], [ou=structuralcontainer], cn=<device name>
- dc=mil, dc=org0, [dc=org1], …, [dc=orgN], [ou=structuralcontainer], cn=<device name>

For certificates that assert serverAuth in the EKU:

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

This WidePoint PIV SSP CPS does not restrict the directory information tree for names of CAs and CSSs. However, CAs that issue certificates under This WidePoint PIV SSP CPS must have distinguished names. CA and CSS distinguished names may be either a geo-political name or an Internet domain component name. CA and CSS geo-political distinguished names will be composed of any combination of the following attributes:

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

Internet domain component names are composed of the following attributes:

- domain component;
- organizational unit; and
- common name (e.g., SSP<#>.eva.orc.com).

For certificates issued under id-fpki-common-derived-pivAuth-hardware and id-fpki-common-derived-pivAuth, in order to maintain logical access requirements between the PIV Authentication certificate and the Derived PIV Authentication certificate, the primary credential (PIV Authentication) DN string is used for the Derived PIV DN string. During issuance of the Derived PIV, a unique UUID is created and stored in the Subject Alternate Name. This unique UUID is generated independent of the UUID created for the primary credential.

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

Names used in certificates issued by the WidePoint PIV SSP CA(s) identify in a meaningful way the subscriber to which they are assigned.

The common name in the DN represents the subscriber in a way that is easily understandable for humans. For people, this will typically be a legal name, such that the preferred common name form is:

- cn=firstname middle name(initial) lastname

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

The common name used represents the subscriber in a way that is easily understandable for humans. For people, this is typically a legal name. For equipment, this may be a model name and serial number, or an application process (e.g., Organization X Mail List or Organization Y Multifunction Interpreter).

In the case of all Digital Signature and Encryption Certificates asserting FPCPF certificate policy OIDs issued to federal employees naming variations will be one of the following:

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

In the case of all Digital Signature and Encryption Certificates asserting FPCPF certificate policy OIDs issued to federal contractors and other affiliates designated by a sponsoring agency:

- CN = Nickname Smith (affiliate); or

- CN = John J. Smith (affiliate); or
- CN = John Jay Smith (affiliate)

While the WidePoint PIV SSP name in CA certificates is not generally interpreted by relying parties, the FPCPF still requires use of meaningful names by WidePoint PIV SSP CAs issuing under the Common Policy and This WidePoint PIV SSP CPS. If included, the common name will describe the WidePoint PIV SSP CA, as such:

- cn=ORC SSP <CA#>

The subject name in WidePoint PIV CA certificates matches the issuer name in certificates issued by the WidePoint PIV SSP CA, as required by RFC 5280.

3.1.3 Anonymity or Pseudonymity of Subscribers

WidePoint PIV SSP does not issue anonymous or pseudonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting name forms are specified in X.501. Rules for interpreting e-mail addresses are specified in [RFC 5322].

Rules for interpreting the PIV FASC-N name type are specified in [PACS].

3.1.5 Uniqueness of Names

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

The WidePoint PIV SSP ensures the following for subscriber names:

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

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

3.1.6 Recognition, Authentication, and Role of Trademarks

A corporate entity is not guaranteed that its Common Name will contain a trademark if requested. The WidePoint PIV SSP will not issue that name to the rightful owner if it has already issued one sufficient for identification. The WidePoint PIV SSP will not issue a certificate knowing that it infringes the trademark of another.

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

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

In all cases where the subscriber generates key pairs, the subscriber is required to prove, to a WidePoint PIV SSP CA, possession of the private key that corresponds to the public key in the certificate request. Subscribers are required to use a FIPS 140-2 validated cryptographic module for generation of keys. PIV certificates are issued on a PIV card via a Card Management System (CMS).

The subscriber is in possession and control of the private key from time of generation or benign transfer. The WidePoint PIV SSP CAs authenticate the subscriber with a Proof of Possession (POP) test when requesting and retrieving a certificate by requiring the subscriber to perform a private key operation and verifying that the public key presented by the subscriber matches the private key. WidePoint supports multiple enrollment protocols which support POP including:

- KEYGEN/SPAC, CRMF/CMMF, PKCS #10 and CMC

To affect POP, the CA supplies a random challenge string to the browser as part of the KEYGEN tag. The public key generated by the browser and the challenge string supplied by the CA are DER (Distinguished Encoding Rules) encoded together, and the resulting PublicKeyAndChallenge value is then digitally signed with the private key to produce a SignedPublicKeyAndChallenge value. This signed value is then base 64 encoded and sent to the CA as part of the certificate request; the CA verifies the signature using the included public key, thus proving possession by the browser of the private key corresponding to that public key.

The public key and challenge strings are DER encoded as PublicKeyAndChallenge and then digitally signed with the private key to produce a SignedPublicKeyAndChallenge. The SignedPublicKeyAndChallenge is base64 encoded, and the ASCII data is finally submitted to the server as the value of a name-value pair, where the name is specified by the NAME attribute of the KEYGEN tag. When retrieving the completed certificate the browser also checks before importing the certificate into its database, to verify that the public key in the certificate being installed matches the private key it originally generated.

An additional out-of-band check is performed by requiring the requestor to print the base 64 of the DER encoded certificate request and present it in person during the validation process. The RA validates both the person's identity and their possession of a certificate request corresponding to their private key.

For id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-devices, id-fpki-common-piv-contentSigning certificates, id-fpki-common-derived-pivAuth, and id-fpki-common-derived-pivAuth-hardware; the Subscriber generates a key pair (private/public) using the device's associated Cryptographic Service Provider (CSP) and creates a signed PKCS10 object. For id-fpki-common-devices, the key pair is generated in a software CSP, at a minimum. For id-fpki-common-piv-contentSigning, the key pair is generated in a hardware CSP. For id-fpki-common-devices and id-fpki-common-piv-contentSigning, the PKI Sponsor submits the PKCS10 object to the WidePoint PIV SSP PKI CA for certificate processing.

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

3.2.2 AUTHENTICATION OF SPONSORING ORGANIZATION IDENTITY

End entities external to WidePoint requesting Subscriber certificates are authorized by organizations which have established a contractual relationship with WidePoint.

For key recovery, WidePoint would validate a third-party requestor as described in section 1.3.4.2, "Internal Third-Party Requestor".

3.2.3 AUTHENTICATION OF INDIVIDUAL IDENTITY

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

3.2.3.1 AUTHENTICATION OF HUMAN SUBSCRIBERS

Verification of an applicant's identity will be performed prior to certificate issuance and the applicant's identity must be verified no more than 30 days before initial certificate issuance. For medium assurance certificates the applicant's in-person identity verification may be performed by an RA. All applicants for medium hardware assurance certificates are required to appear in person before an RA.

For id-fpki-common-authentication, id-fpki-common-cardAuth, id-fpki-common-policy, and id-fpki-common-hardware, identity-proofing is performed in accordance with section 2.7, PIV Identity Proofing and Registration Requirements, of FIPS 201-2.

Minors and others not competent to perform face-to-face registration alone are not supported under this CPS. At a minimum, authentication procedures for WidePoint PIV SSP certificate Federal employee applicants must include the following steps:

1) Verify that a request for certificate issuance to the applicant was submitted by agency management.

2) Verify Applicant's employment through use of official agency records.

3) Establish applicant's identity by in-person proofing before an RA, based on either of the following processes:

   A) Process #1:

      i) The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and

      ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and

      iii) The credential presented in Step 3) a) i) above is verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid). Typically this is accomplished by querying a database maintained by the organization that issued the credential, but other equivalent methods may be used.

   B) Process #2:

      i) The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and

      ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and

      iii) The applicant presents current corroborating information (e.g., current credit card bill or recent utility bill) to the RA. The identifying information (e.g., name and address) on the credential presented in Step 3) b) i) above is verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid).

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

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

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

1) Verify that a request for certificate issuance to the applicant was submitted by an authorized sponsoring agency employee (e.g., contracting officer or contracting officer's technical representative).

2) Verify sponsoring agency employee's identity and employment through either one of the following methods:

A) A digitally signed request from the sponsoring agency employee, verified by a currently valid employee signature certificate issued by a WidePoint PIV SSP CA, may be accepted as proof of both employment and identity,

B) Authentication of the sponsoring agency employee with a valid employee PIV-authentication certificate issued by the agency may be accepted as proof of both employment and identity, or

C) In-person identity proofing of the sponsoring agency employee may be established before the registration authority as specified in employee authentication above and employment validated through use of the official agency records.

3) Establish applicant's identity by in-person proofing before the registration authority, based on either of the following processes:

A) Process #1:

i) The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and

ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and

iii) The credential presented in Step 3) a) i) above shall be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid). Typically this is accomplished by querying official records maintained by the organization that issued the credential.

B) Process #2:

i) The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and

ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and

iii) The applicant presents current corroborating information (e.g., current credit card bill or recent utility bill) to the RA. The identifying information (e.g., name and address) on the credential presented in Step 3) b) i) above shall be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid).

4) Record and maintain a biometric of the applicant (e.g., a photograph or fingerprint) by the RA or CA. (Handwritten signatures and other behavioral characteristics are not accepted as biometrics for the purposes of this policy.) This establishes an audit trail for dispute resolution.

In all cases, a RA records the following information:

- The Identity of the person performing the validation process

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

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

- Name of document presented for identity proofing
- For PIV certificates the identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 1615-0047, Employment Eligibility Verification.
- Issuing authority
- Date of issuance
- 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
- The WidePoint PIV SSP name, including subcontractors, if any
- All associated error messages and codes
- Date/time of process completion
- Names (IDs) of WidePoint PKI processes, including subcontractors' processes, if any.

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

3.2.3.2 AUTHENTICATION OF DEVICES

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

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

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

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

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

Note: FQDNs shall be listed in id-fpki-common-devices Subscriber Certificates using dNSNames in the subjectAltName extension or in Subordinate CA Certificates via dNSNames in permittedSubtrees within the Name Constraints extension.

WidePoint does not issue certificates containing wildcard characters (*).

All requests for device certificates shall be digitally signed by the sponsor.

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

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

In person or supervised remote registration by the PKI Sponsor, with the identity of the PKI Sponsor confirmed in accordance with the requirements of Section 4.1.1.3.

3.2.3.3 AUTHENTICATION OF DERIVED PIV CREDENTIALS

This section applies to certificates asserting id-fpki-common-derived-pivAuth-hardware and id-fpki-common-derived-pivAuth. An RA or CAA verifies that the request for certificate issuance to the PIV Cardholder has been submitted by an authorized agency employee.

The PIV Cardholder presents his/her PIV Card for validation. The PIV Cardholder is prompted to activate the card to demonstrate they are in possession of the corresponding private key. The PIV Cardholder activates the card using either their PIN or their biometric. Using standards-compliant PKI path validation, the WidePoint PIV SSP validates the PIV card confirming that it is neither expired nor revoked, and that it is from a trusted source. For certificates asserting id-fpki-common-derived-pivAuth-hardware, the foregoing occurs with the PIV Cardholder in the presence of the WidePoint PIV SSP RA or WidePoint PIV SSP CAA.

WidePoint maintains a copy of the PIV Cardholder's PIV Authentication certificate.

For certificates asserting id-fpki-common-derived-pivAuth-hardware, applicants must appear at the WidePoint PIV SSP RA in person to present the PIV Card and perform the PKI-AUTH authentication mechanism. The WidePoint PIV SSP RA performs a 1:1 comparison of the PIV Cardholder, in accordance with [SP 800-76], against biometric data stored on the PIV Card. The WidePoint PIV SSP RA records and maintains the biometric sample used to validate the PIV Cardholder. In cases where 1:1 biometric comparison is not possible, then the PIV Cardholder presents a government-issued form of identification. The WidePoint PIV SSP RA examines this additional credential for biometric data (e.g., a photograph on the credential itself) which can be linked to the PIV Cardholder. If validation is successful using the additional credential, then the process documentation for the issuance of the certificate includes the identity of the WidePoint PIV SSP RA, a signed declaration by the WidePoint PIV SSP RA that he/she verified the identity of the PIV Cardholder as required by This WidePoint PIV SSP CPS using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury), a unique identifying number from the second form of identification or a facsimile of the ID, a biometric of the PIV Cardholder, and the date and time of the verification.

Seven days after issuing the Derived credential, the WidePoint PIV SSP checks the revocation status of the PIV Authentication certificate (using the OCSP/CRL URL within the PIV Authentication certificate) which was recorded during the Derived PIV enrollment. This step can detect use of a compromised PIV Card to obtain a derived credential.

3.2.3.4 AUTHENTICATION OF THIRD-PARTY KEY RECOVERY REQUESTOR

This section addresses the key recovery use case in which the requestor is other than the Subscriber associated with the private key. Widepoint SSP KRAs will verify the identity of the Requestor prior to initiating the key recovery request. WidePoint ensures that a Requestor establishes their identity to a KRA. In cases where an electronic request is made, a KRA will

verify the digital signature on the request and ensure that the request is signed using a certificate at least to the specified assurance level of the key being recovered, prior to initiating the key recovery request. In all cases where a digitally signed, electronic request is made, a KRA will authenticate the identity of the Requestor by validating their digital signatures. In cases where digital authentication is not possible, a KRA will perform in-person identity authentication, as specified in Section 3.1.

3.2.3.5 Authentication of Key Recovery Agent

The KRA authenticates using their PIV Authentication certificate.

3.2.4 Non-verified Subscriber Information

The WidePoint PIV SSP does not include information in certificates that has not been verified.

3.2.5 Validation of Authority

3.2.5.1 Issuance

Before issuing certificates that assert organizational authority, The WidePoint PIV SSP validates the individual's authority to act in the name of the organization. This validation is performed by having the applicant complete and submit a "Proof of Organizational Affiliation" letter, made available to applicants on the WidePoint PIV SSP website. The WidePoint PIV SSP uses Proof of Organizational Affiliation letters for applicants attempting to obtain:

- Component/ Server certificates
- VPN IPsec Component Certificates

In accordance with Section 3.2.3.2, all requests for device certificates in the name of an organization, shall be digitally signed by the sponsor. In addition, the CPS shall specify a process by which an organization identifies the individuals who may request certificates that assert organizational authority. If an organization specifies, in writing, the individuals who may request a certificate, then the CA shall not accept any certificate requests that are outside this specification. The CA shall provide an Applicant with a list of the organization's authorized certificate requesters upon the Applicant's verified written request.

3.2.5.2 Key Recovery

3.2.5.2.1 Requestor Authorization Validation

For key recovery, the KRA validates the authorization of the Requestor as described in section 1.3.4.2, "Internal Third-Party Requestor".

3.2.5.2.2 KRA Authorization Validation

When successfully authenticated, a KRA is authorized to obtain keys for an identified Subscriber's organization based on assigned scope and role.

3.2.6 CRITERIA FOR INTEROPERATION

The FPKIPA determines the interoperability criteria for CAs operating under the FPCPF.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY

3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

WidePoint PIV SSP Certificate re-keying (signing and encryption) is accomplished through the limitation on certificate renewal. The minimum in-person registration requirement for all WidePoint PIV SSP certificate re-keying described, with the exception of CA certificates, is once every 9 years from the time of initial registration (i.e., after two 3-year re-keys). WidePoint PIV SSP subscribers must identify themselves for the purpose of re-keying through use of their current signature key, except that identity will be established through initial registration process, described in Section 3.2.3.1, at least once every nine years from the time of initial registration.

For device certificates, identity may be established through the use of the device's current signature key, the signature key of the device's human PKI Sponsor, except that identity shall be established through the initial registration process at least once every nine years from the time of initial registration.

In addition, for re-key of subscriber certificates issued under id-fpki-common-derived-pivAuth-hardware, identity is established via mutual authentication between WidePoint and the cryptographic module containing the current key, if the new key will be stored in the same cryptographic module as the current key. The Subscriber's identity must be established through the initial registration process if the new key will be stored in a different cryptographic module than the current key. An WidePoint PIV SSP RA or WidePoint PIV SSP CAA verifies that the request for certificate re-issuance to the PIV Cardholder has been submitted by an authorized agency employee.

WidePoint PIV SSP CA certificate re-key follows the same procedure as is performed for initial WidePoint PIV SSP CA certificate generation.

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

3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

After a certificate has been revoked or expired, the applicant is required to go through the initial registration process as described in Section 3.2.3.1.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Certificate revocation requests may be made using the same practices as certificate issuance requests. In addition, certificate revocation requests may be made electronically using e-mail digitally signed by a certificate of equal or greater level of assurance than that of the certificate for which the request is made. In either case, the request must include the reason for revocation. See Section 4.9 for details on certificate revocation procedures. Subscribers who are in possession of their private keys may also revoke their own certificates at any time by following the instructions provided via the WidePoint PIV SSP website (https://orc.widepoint.com/certificate-revocation/).

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

A WidePoint PIV SSP certificate revocation request that is submitted electronically may be authenticated on the basis of a digital signature using the certificate's associated key pair. The identity of the person submitting a revocation request in any other manner is authenticated in accordance with Section 4.9 of This WidePoint PIV SSP CPS. Revocation requests authenticated on the basis of the SSP Certificate's associated key pair are always accepted as valid. Other revocation request authentication mechanisms for non-PIV certificates include a request in writing signed by the subscriber and sent via U.S. Postal Service first-class mail. WidePoint PIV SSP RAs verify the authentication mechanism and balances the need to prevent unauthorized revocation requests against the need to quickly revoke certificates.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 WHO CAN SUBMIT A CERTIFICATE APPLICATION

4.1.1.1 CA CERTIFICATES

The WidePoint PIV SSP does not issue CA certificates outside of the WidePoint PIV SSP.

4.1.1.2 USER CERTIFICATES

Applications for Subscriber certificates are submitted by the applicant (or PKI sponsor) or an authorized representative of the applicant's organization.

4.1.1.3 DEVICE CERTIFICATES

Some computing and communications components (web servers, routers, firewalls, etc.) may be named as certificate subjects. In such cases, the component must have a human PKI Sponsor. The PKI Sponsor is responsible for providing to the CAA, or approved RAs, through an application form, correct information regarding:

- Equipment identification
- Equipment public keys
- Equipment authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the WidePoint PIV SSP to communicate with the PKI sponsor when required

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

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

In person registration by the PKI Sponsor, with the identity of the PKI Sponsor confirmed in accordance with the requirements of Section 3.2.3.1.

4.1.1.4 Code Signing Certificates

Not applicable. The WidePoint PIV SSP does not support the issuance of code-signing certificates.

4.1.1.5 Key Recovery Applications

Subscribers may request recovery of their own escrowed encryption keys as verified in-person at a WidePoint KRA workstation. Additionally, internal third-party requestors (as described in Section 1.3.4.2 and permitted by WidePoint policy) and external third-party requestors (as described in Section 1.3.4.3) who are empowered with a court order from a competent court (such as a DoD investigator who has authorization to access the Subscriber's communication, or a duly authorized law enforcement or court official who has court authorization to access a Subscriber's communication) may also request recovery of escrowed keys.

4.1.2 Enrollment Process and Responsibilities

All WidePoint PIV SSP electronic transmissions and communications supporting application and issuance processes are authenticated and protected from modification using SSL. Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair are used. Out-of-band communications protect the confidentiality and integrity of the data by sealing all data and only sending via trusted carriers (e.g. U.S. Postal Service, FedEx, UPS). It is the responsibility of the Subscriber to provide the WidePoint PIV SSP with accurate information on their certificate applications.

4.1.2.1 WidePoint PIV SSP CMS Certificate Enrollment

For id-fpki-common-hardware, id-fpki-common-authentication, and id-fpki-common-cardAuth, an authorized agency official notifies a WidePoint PIV SSP Sponsor that an agency employee or contractor is authorized to be issued a PIV Card. The WidePoint PIV SSP Sponsor then creates an applicant record in the card management system using employment information maintained by the agency. The WidePoint PIV SSP Sponsor notifies the WidePoint PIV SSP Registrar that the applicant is ready for enrollment.

The applicant meets in-person with the WidePoint PIV SSP Registrar at a designated WidePoint PIV SSP workstation. The WidePoint PIV SSP Registrar accesses the card management system using their PIV Card. As stipulated in Section 3.2, the WidePoint PIV SSP Registrar validates the applicant's identity. The WidePoint PIV SSP Registrar captures the applicant's biometrics (fingerprints and facial image). The WidePoint PIV SSP Registrar confirms the applicant's NACI status, and updates the applicant's record to either "Approved" or "Waiting for response". The WidePoint PIV SSP Registrar approves card issuance within the system, and notifies a WidePoint PIV SSP Issuer that a card can be issued to the applicant.

4.1.2.2 DEVICE CERTIFICATES

Some computing and communications components (e.g., web servers, routers, firewalls, etc.) may be named as certificate subjects. In such cases, the component must have a human PKI Sponsor. The PKI Sponsor is responsible for providing to the WidePoint PIV SSP CAA, or an authorized WidePoint PIV SSP RA, through an application form, correct information regarding:

- Equipment identification
- Equipment public keys
- Equipment authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable WidePoint to communicate with the PKI sponsor when required

A WidePoint PIV SSP RA reviews the information submitted for the device, and validates the identity of the PKI Sponsor in accordance with Section 3.2.

4.1.2.3 DERIVED CERTIFICATE ENROLLMENT

For id-fpki-common-derived-pivAuth, the Subscriber presents id-fpki-common-authentication to the WidePoint PIV SSP Derived Credential Enrollment, hereafter referred to as the “WidePoint PIV SSP DCE”, site using their PIV Card. The site challenges the Subscriber for their PIN in order to access the PIV Authentication certificate on the card. Upon receipt of the correct PIN, the site reads the card and populates a Certificate Status Request form based on the data read, and generates a Quick Response (QR) Code. The Subscriber scans the QR code using a WidePoint Certificate on Device ® mobile app. A mobile enrollment code is generated. The Subscriber validates the CSR by entering the mobile enrollment code at the WidePoint PIV SSP DCE site.

4.1.3 KEY ESCROW PROCESS AND RESPONSIBILITIES

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

keys are protected by the KEK, which is a 24-byte AES key. All cryptographic operations occur in the HSM. The private key is encrypted in the HSM with the KEK for secure storage in the database.

4.1.4 KEY RECOVERY PROCESS AND RESPONSIBILITIES

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

A third-party requestor would submit a request to a designated WidePoint SSP KRA, digitally-signing the request using an associated PKI-issued authentication or signature certificate of assurance level equal to or greater than that of the escrowed key. Written requests signed by hand and witnessed by a KRA or notarized may be accepted on a case-by-case basis.

4.1.4.1 KEY RECOVERY THROUGH KRA

All copies of escrowed keys are protected using two-person control procedures during recovery and delivery to the authenticated and authorized third-party requestor; and during operation and maintenance of the WidePoint SSP KED function.

4.1.4.2 AUTOMATED SELF-RECOVERY

Automated self-recovery is not supported.

4.1.4.3 KEY HISTORY RECOVERY TO HARDWARE TOKEN

The WidePoint SSP CMS, when issuing a new PIV Card to a Subscriber, will recover previous key management keys stored in escrow for that user and inject them into the archive key management slots designated of the PIV Card for the Subscriber.

4.2 CERTIFICATE APPLICATION PROCESSING

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

4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

The applicant's identity will be established in-person. Information provided is checked to ensure its legitimacy. Federal Government-issued Photo I.D Credentials are required. The applicant's identity must be personally verified prior to the certificate being issued. The applicant will appear personally before either:

- An authorized WidePoint PIV SSP RA or LRA
- A Trusted Agent approved by the WidePoint PIV SSP or appointed in writing by name by the WidePoint PIV SSP

The WidePoint PIV SSP RA, LRA or Trusted Agent will verify:

- That the applicant is a duly authorized representative of the Sponsoring Organization as an employee, partner, member, agent, or other association, in good standing.
- The Sponsoring Organization's identity as specified in Section 3.2.3.1.

The process documentation and authentication requirements will include the following:

- Identity of the person performing the identification.
- A signed declaration by that person that he or she verified the identity of the subscriber as required by the applicable certificate policy which may be met by establishing how the applicant is known to the verifier as required by this certificate policy.
- A unique identifying number from the ID of the verifier and from the ID of the applicant.
- The date and time of the verification.
- A declaration of identity signed by the applicant using a handwritten signature. This will be performed in the presence of the person performing the identity authentication.

The applicant will personally appear before one of the required identity verifiers at any time prior to application of a WidePoint PIV SSP CA's signature to the applicant's certificate. Alternatively, when private keys are delivered to subscribers via hardware tokens, the subscribers will personally appear before the WidePoint PIV SSP RA, LRA or Trusted Agent to obtain their tokens or token activation data.

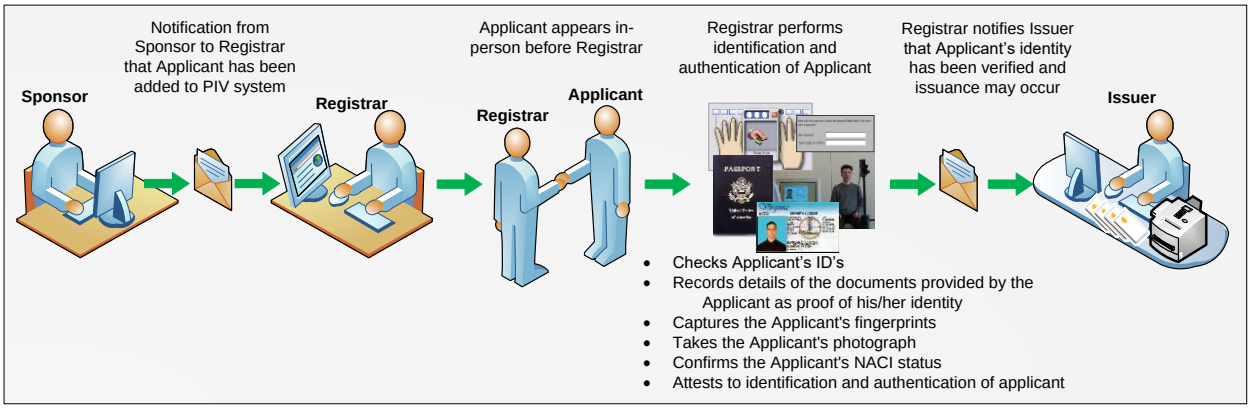

Figure 1-PIV Identification and Authentication Process Flow

The WidePoint PIV SSP RA or LRA will archive a copy of all information used in the verification process. In all cases, the agency/organization records the following information:

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

The following elements are present 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
- The WidePoint PIV SSP name, including subcontractors, if any
- All associated error messages and codes
- Date/time of process completion
- Names (IDs) of WidePoint PIV SSP processes, including subcontractors' processes, if any.

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

- The assurance level of the new certificate will be the same or lower than the certificate used as the authentication credential.
- The DN of the new certificate will be identical to the DN of the certificate used as the authentication credential.
- Information in the new certificate that could be used for authorization will be identical to that of the certificate used as the authentication credential.
- The expiration date of the new certificate will be no later than the next required in-person authentication date associated with the certificate used as the authentication credential.
- The validity period of the new certificate will not be greater than the maximum validity period requirements of the FPCPF for that particular type of certificate.
- The in-person authentication date associated with the new certificate will be no later than the in-person authentication date associated with the certificate used for authentication.

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

4.2.1.1 AUTHENTICATION OF DEVICE IDENTITY CERTIFICATES

Some computing and communications devices (web servers, routers, firewalls, etc.) may be named as certificate subjects. In such cases, the device must have a human PKI Sponsor as described in Section 4.1.1.3. The PKI Sponsor is responsible for providing to an approved WidePoint PIV SSP RA, through an application form, correct information regarding:

- Equipment identification

- Equipment public keys
- Equipment authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the WidePoint PIV SSP to communicate with the PKI sponsor when required

A WidePoint PIV SSP RA will authenticate the validity of any authorizations to be asserted in the certificate, and will verify source and integrity of the data collected to an assurance level commensurate with the certificate level being requested. Authentication and integrity checking is accomplished by one of the following methods:

- Verification of digitally signed messages sent from PKI sponsors (using certificates of equivalent or greater assurance than that being requested).
- In person registration by the PKI Sponsor, with the identity of the PKI Sponsor confirmed in accordance with the requirements of Section 4.1.1.3.

4.2.1.2 DERIVED PIV CERTIFICATES

For id-fpki-common-derived-pivAuth, a WidePoint PIV SSP RA accesses the WidePoint PIV SSP DCE site using a WidePoint PIV SSP certificate of equal or greater assurance than the certificate to be issued to the Subscriber. The WidePoint PIV SSP RA validates the information provided as described in Section 3.2.3.3.

4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

Upon successful completion of the subscriber identification and authentication process, the WidePoint PIV SSP creates the requested SSP Certificate, notifies the applicant thereof, and makes the WidePoint PIV SSP Certificate available to the applicant. If the applicant provided an e-mail address, the WidePoint PIV SSP sends the notification message via e-mail. If no e-mail address was provided, the WidePoint PIV SSP sends the notification to the U.S. postal address provided.

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

4.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS

The entire process from applicant appearing before one of the required identity verifiers to certificate issuance will take no more than 30 days.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

For issuance of id-fpki-common-authentication and id-fpki-common-cardAuth certificates, interaction with the CA at the time of certificate issuance is conducted by the WidePoint PIV SSP Issuer using their WidePoint PIV SSP Issuer PIV card to authenticate to the WidePoint PIV SSP PIV card issuing station, as shown in Figure 2, below . The WidePoint PIV SSP PIV card issuing station authenticates to the WidePoint PIV SSP CA via the WidePoint PIV SSP CMS, which securely connects to the WidePoint PIV SSP CA. Upon receiving approval from a PIV Registrar who has conducted in-person identity verification, the PIV Issuer will:

- Verify the identity of the applicant via in-person identity-proofing and verify the integrity of the information in the certificate request,
- Print the PIV card

The applicant, via the WidePoint PIV SSP PIV card issuing/activation station, will then activate the PIV card via biometric 1:1 authentication, which was captured during registration. The applicant generates a PIN for the PIV card. A request is then generated to the WidePoint PIV SSP CA to build and sign a certificate, if all certificate requirements have been met. Once the certificates have been written to the PIV card, the applicant, now a Subscriber, formally acknowledges their obligations as described in Section 9.6.3, via the WidePoint PIV SSP PIV card issuing/activation station using his/her PIV card and associated PIN.

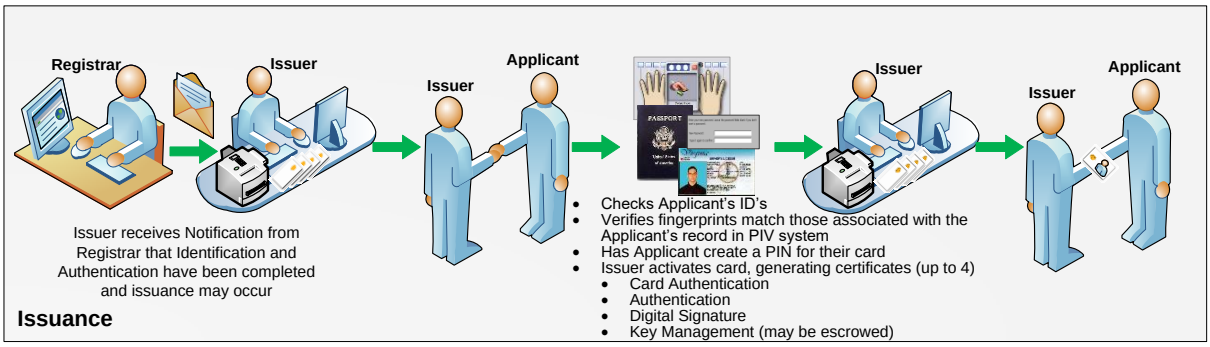

Figure 2-PIV Card Issuance Process

For id-fpki-common-devices, id-fpki-common-piv-contentSigning, id-fpki-common-derived-pivAuth, id-fpki-common-derived-pivAuth-hardware, upon successful completion of the subscriber identification and authentication process in accordance with Section 3.2.3, Authentication of Individual Identity, of This WidePoint PIV SSP CPS, WidePoint creates the requested certificate, notifies the applicant thereof, and, after ensuring that the Subscriber has formally acknowledged his/her obligations in accordance with Section 9.6.4, Subscriber Representations and Warranties, makes the certificate available to the applicant.

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

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

4.3.2 NOTIFICATION TO SUBSCRIBER BY THE CA OF ISSUANCE OF CERTIFICATE

If the applicant provided an e-mail address, the WidePoint PIV SSP sends the notification message via e-mail. If no e-mail address was provided, the WidePoint PIV SSP sends the notification to the U.S. postal address provided.

The notification informs the applicant of the creation of a certificate, states a URL for use by the applicant for retrieving the certificate, contain a unique serial number, and reaffirms the subscriber's responsibilities as explained in the application process. For device certificates, the notification is sent to the human PKI Sponsor associated with the device certificate. The notification also obligates the subscriber to:

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

Upon issuance of a WidePoint PIV SSP Certificate, the WidePoint PIV SSP warrants to all program participants that:

- The WidePoint PIV SSP has issued, and manages, the certificate in accordance with the requirements in This WidePoint PIV SSP CPS.
- WidePoint PIV SSP has complied with all requirements in this WidePoint PIV SSP CPS when identifying the subscriber and issuing the certificate.
- There are no misrepresentations of fact in the WidePoint PIV SSP issued certificate known to the WidePoint PIV SSP and that the WidePoint PIV SSP has verified the information in the issued certificate.
- Information provided by the subscriber for inclusion in the WidePoint PIV SSP issued certificate has been accurately transcribed to the certificate.
- The WidePoint PIV SSP issued certificate meets the material requirements of this WidePoint PIV SSP CPS.

For id-fpki-common-derived-pivAuth, e-mail notification is sent from the The WidePoint PIV SSP DCE site.

4.4 CERTIFICATE ACCEPTANCE

As described in this WidePoint PIV SSP CPS, a condition to issuing a certificate that asserts FPCPF certificate policy OIDs is that the subscriber will indicate acceptance or rejection of the certificate to the WidePoint PIV SSP and acknowledge the subscriber obligations. By accepting the WidePoint PIV SSP issued certificate, the subscriber is warranting that all information and representations made by the subscriber that are included in the WidePoint PIV SSP issued certificate are true.

The WidePoint PIV SSP notifies the certificate applicant of certificate issuance through e-mail. The notification includes the URL that the applicant uses to receive the approved certificate. The WidePoint PIV SSP verifies possession of the subscriber's private key at the time the applicant accepts the issued certificate.

The notification informs the subscriber of the creation of the certificate, contents of the certificate and reaffirms the subscriber's responsibilities as explained in the application process. The notification informs the subscriber if the private key has been escrowed.

The subscriber agreement includes the following subscriber obligations. The subscriber will:

- Accurately represent themselves in all communications with the WidePoint PIV SSP.
- Protect their private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements, and local procedures.
- Notify the WidePoint PIV SSP, in a timely manner, of the suspicion that their private keys are compromised or lost. Such notification will be made directly or indirectly through mechanisms consistent with this WidePoint PIV SSP CPS.
- Abide by all the terms, conditions, and restrictions levied upon the use of their private keys and certificates.
- Formally accept the certificate at the designated WidePoint PIV SSP web page during certificate retrieval. (Failure to do so will result in revocation of the certificate.)

The subscriber has already agreed to the obligations during the request phase (as stipulated in the Subscriber Agreement), and the certificate can only be accepted during a Proof of Possession (POP) of private key test. The WidePoint PIV SSP logs the acceptance of the certificate.

A subscriber who does not provide this verification notice within 30 calendar days of receiving notification that his or her approved certificate is available for downloading, or who is found to have acted in a manner counter to these obligations will have his or her certificate revoked, and will forfeit all claims he or she may have against the WidePoint PIV SSP in the event of a dispute arising from the failure to fulfill the obligations above.

4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

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

To affect POP a WidePoint PIV SSP CA supplies a random challenge string to the browser as part of the KEYGEN tag. The public key generated by the browser and the challenge string supplied by the WidePoint PIV SSP CA are DER (Distinguished Encoding Rules) encoded together, and the resulting PublicKeyAndChallenge value is then digitally signed with the private key to produce a SignedPublicKeyAndChallenge value. This signed value is then base 64 encoded and sent to the WidePoint PIV SSP CA as part of the certificate request; the WidePoint PIV SSP CA verifies the signature using the included public key, thus proving possession by the browser of the private key corresponding to that public key.

The public key and challenge strings are DER encoded as PublicKeyAndChallenge and then digitally signed with the private key to produce a SignedPublicKeyAndChallenge. The SignedPublicKeyAndChallenge is base64 encoded, and the ASCII data is finally submitted to the server as the value of a name-value pair, where the name is specified by the NAME-attribute of the KEYGEN tag. When retrieving the completed certificate the browser also checks before importing the certificate into its database, to verify that the public key in the certificate being installed matches the private key it originally generated.

For id-fpki-common-derived-pivAuth, the Subscriber launches the WidePoint Certificate on Device ® mobile app and clicks on the download certificate button.

Failure to object to a properly requested certificate or its contents constitutes acceptance of the certificate.

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

4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA

WidePoint PIV SSP PKI CA certificates are published to the appropriate repositories.

Subscriber certificates are not published.

4.4.3 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

WidePoint PIV SSP CAs do not issue certificates to other entities.

4.5 KEY PAIR AND CERTIFICATE USAGE

The WidePoint PIV SSP certifies keys for use in signing or encrypting, but not both. The use of a specific key is determined by the key usage extension. The key usage extension is included in all certificates and is always marked critical in order to limit the use of a public key certificate for its intended purpose, as stipulated in the X.509 Certificate and CRL Extensions Profile [CCP-PROF].

4.5.1 SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE

Subscriber responsibilities relating to use of the subscriber's private key and certificate are stipulated in section 9.6.4, “Subscriber Representations and Warranties”.

4.5.2 RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE

WidePoint PIV SSP CAs issue CRLs specifying the current status of all unexpired certificates (except for OCSP responder certificates which include the id-pkix-ocsp-nocheck extension). It is recommended that relying parties process and comply with this information whenever using Common Policy certificates in a transaction.

4.6 CERTIFICATE RENEWAL

The WidePoint PIV SSP does not renew certificates, and therefore does not accept requests for renewal. Any use of the term “renewal” within this WidePoint PIV SSP CPS refers to rekeying. At the end of the life of a certificate, the WidePoint PIV SSP provides subscribers with the ability to obtain a new certificate via rekey, with a different public key and new serial number (and, when applicable, on a new card) while retaining the rest of the subscriber’s information from the expiring certificate (e.g. name, email address, etc.). The process for rekeying a Subscriber’s certificate is described in Section 3.3.1, above. Although true renewal is not available under this WidePoint PIV SSP CPS, the WidePoint PIV SSP does use the term “Renewal” when interacting with Subscribers for simplification of Customer understanding.

4.6.1 CIRCUMSTANCE FOR CERTIFICATE RENEWAL

Renewal does not apply within the WidePoint PIV SSP. See Section 4.6.

4.6.2 WHO MAY REQUEST RENEWAL

Renewal does not apply within the WidePoint PIV SSP. See Section 4.6.

4.6.3 PROCESSING CERTIFICATE RENEWAL REQUESTS

Renewal does not apply within the WidePoint PIV SSP. See Section 4.6.

4.6.4 Notification of New Certificate Issuance to Subscriber

Renewal does not apply within the WidePoint PIV SSP. See Section 4.6.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Renewal does not apply within the WidePoint PIV SSP. See Section 4.6.

4.6.6 Publication of the Renewal Certificate by the CA

Renewal does not apply within the WidePoint PIV SSP. See Section 4.6.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Renewal does not apply within the WidePoint PIV SSP. See Section 4.6.

4.7 Certificate Re-Key

The minimum requirement for all WidePoint PIV SSP certificate re-keying, with the exception of WidePoint PIV SSP CA certificates, is once every three (3) years from the time of initial registration. WidePoint PIV SSP subscribers will identify themselves for the purpose of re-keying through use of their current signature key, except that identity will be established through the initial registration process described in Section 3.2.3.1.

4.7.1 Circumstance for Certificate Re-key

A revoked certificate will not be re-keyed.

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

4.7.2 Who May Request Certification of a New Public Key

The Subscriber or an approved WidePoint PIV SSP RA may request the re-key of a Subscriber certificate. In the case of device certificates, the human PKI sponsor of the device may request certification of a new public key for the device. An approved WidePoint PIV SSP RA will take the appropriate actions.

4.7.3 Processing Certificate Re-keying Requests

The re-key process will be in accordance with the certificate issuance process described in Section 3.2. Identity validation may be in accordance with Section 3.3. The Subscriber or an RA may request the modification of a Subscriber certificate. The WidePoint PIV SSP CA or an RA will validate any changes in the subscriber authorizations reflected in the certificate. For

device certificates, the human PKI Sponsor of the device may request certificate modification for the device.

4.7.4 Notification of New Certificate Issuance to Subscriber

The WidePoint PIV SSP will notify subscribers of new certificate issuance in accordance with the notification processes specified in Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

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

4.7.6 Publication of the Re-keyed Certificate by the CA

When a WidePoint PIV SSP CA private signature key is updated, and thus generates a new public key, the WidePoint PIV SSP notifies all WidePoint PIV SSP CAAs, RAs, and subscribers who rely on the WidePoint PIV SSP CA's certificate that it has been changed.

See also section 4.4.2, "Publication of the Certificate by the CA".

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

When a WidePoint PIV SSP CA private signature key is updated, and thus generates a new public key, the WidePoint PIV SSP notifies all WidePoint PIV SSP CAAs, RAs, LRAs, and subscribers that rely on the WidePoint PIV SSP CA's certificate that it has been changed.

4.8 Certificate Modification

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

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

When a WidePoint PIV SSP CA updates its private signature key and thus generates a new public key, the WidePoint PIV SSP will obtain a new certificate from the Common Policy CA.

4.8.1 Circumstance for Certificate Modification

A WidePoint PIV SSP CA may modify a WidePoint PIV SSP CA or OCSP responder certificate whose characteristics have changed (e.g. assert new policy OID). The new certificate will have a different subject public key.

A WidePoint PIV SSP certificate may be modified if some of the information other than the DN, such as the e-mail address or authorizations, has changed.

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

4.8.2 Who May Request Certificate Modification

The Subscriber or an approved WidePoint PIV SSP RA with a valid certificate may request the modification of a Subscriber certificate. The WidePoint PIV SSP CA or RA will validate any changes in the subscriber authorizations reflected in the certificate. For device certificates, the human PKI Sponsor of the device may request certificate modification.

4.8.3 Processing Certificate Modification Requests

The certificate modification process will be in accordance with the certificate issuance process described in Section 3.2. Identity validation must be in accordance with this CPS. In addition, a WidePoint PIV SSP CA or RA validates any changes in the subscriber authorizations reflected in the certificate. Proof of all subject information changes must be provided to an approved WidePoint PIV SSP RA or other designated agent and verified before the modified certificate is issued. The approved WidePoint PIV SSP RA exercises due diligence in validating the requested change of information and/or authorizations (e.g. applicant/subscriber's Common Name, Affiliation, and/or email address). If an individual's name changes (e.g., due to marriage), then proof of the name change must be provided to the approved WidePoint PIV SSP RA or other designated agent in order for a certificate with the new name to be issued. If the subscriber's authorizations have decreased, the existing certificate will be revoked and the subscriber will be required to obtain a new certificate following the initial registration process of new subscribers.

4.8.4 Notification of New Certificate Issuance to Subscriber

The WidePoint PIV SSP CAs will notify subscribers of new certificate issuance in accordance with the notification processes specified in Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

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

4.8.6 Publication of the Modified Certificate by a WidePoint PIV SSP CA

The WidePoint PIV SSP makes no stipulation regarding publication of subscriber certificates, except as noted in Section 9.4.3.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

The WidePoint PIV SSP makes no stipulation regarding notification of certificate issuance by WidePoint PIV SSP CAs to other entities, except as noted in Section 2.2.

4.9 Certificate Revocation and Suspension

Revocation requests must be authenticated. The individual making the request will either digitally sign requests for certificate revocation, or the individual will present the request in person to an RA.

WidePoint PIV SSP CAs operating under this WidePoint PIV SSP CPS will issue CRLs covering all unexpired certificates issued under this WidePoint PIV SSP CPS, except for OCSP responder certificates that include the id-pkix-ocsp-nocheck extension.

WidePoint PIV SSP CAs operating under This WidePoint PIV SSP CPS will make public a description of how to obtain revocation information for the certificates the WidePoint PIV SSP publishes, and an explanation of the consequences of using dated revocation information. This information, as noted in Section 4.9.6 of this WidePoint PIV SSP CPS and the Summary made publicly available. This information is also given to subscribers during certificate request or issuance, and is readily available to any potential relying party.

Certificate suspension for WidePoint PIV SSP CA certificates is not allowed.

The FPKIPA will be notified at least two weeks prior to the revocation of any WidePoint PIV SSP CA certificate, whenever possible. For emergency revocation, the WidePoint PIV SSP shall follow the notification procedures in Section 5.7.

4.9.1 Circumstances for Revocation

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

A Subscriber or a Sponsoring Organization (where applicable), is responsible for promptly requesting revocation of a WidePoint PIV SSP issued certificate:

- When the private key, or the media holding the private key, associated with the WidePoint PIV SSP issued certificate is, or is suspected of having been, compromised
- When the individual named in the certificate no longer represents, or is no longer affiliated with, the Sponsoring Organization.
- If the WidePoint PIV SSP learns, or reasonably suspects, that the subscriber's private key has been compromised or the subscriber has failed to meet their responsibilities.
- If the WidePoint PIV SSP determines that the issued certificate was not properly issued in accordance with this WidePoint PIV SSP CPS.
- If the certificate holder requests that the certificate be revoked.
- If the certificate holder can be shown to have violated the subscriber obligations, including payment of any required fees.
- If the certificate holder is no longer authorized to hold the certificate (e.g. termination of employment or change in responsibilities).
- If the information in the certificate is no longer accurate so that identifying information needs to be changed (e.g. change of name or privilege attributes asserted in the subscriber's certificate are reduced). This includes evidence that a wild card certificate has been issued with a name where the PKI Sponsor does not exercise control of the entire name space associated with the wild card certificate.
- The subscriber's employer or organization requests revocation.
- The certificate was obtained by fraud or mistake.
- The certificate was not correctly requested, issued or accepted.
- The certificate contains incorrect information, is defective or creates a possibility of incorrect reliance or usage.
- Certificate private key compromise is suspected.
- The certificate holder fails to make a payment or other contractual obligations related to the certificate.

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

The WidePoint PIV SSP provides for the revocation of certificates when requested, at any time for any reason. If the Government provides RA functions, or if the WidePoint PIV SSP has delegated revocation functions to subcontractor RAs, all information is transmitted via a network

between the WidePoint PIV SSP and/or subcontractors and/or government RAs using mutual authentication.

Whenever any of the above circumstances are reported, the appropriate authority will review the circumstances and make a revocation decision. The revocation decision shall be made based on appropriate criteria, to include:

- The nature of the alleged problem;
- The number of Certificate Problem Reports received about a particular Certificate or Subscriber; and
- Relevant legislation

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

4.9.2 WHO CAN REQUEST REVOCATION

WidePoint may summarily revoke certificates issued by a WidePoint CA at its discretion. A written notice and brief explanation for the revocation will subsequently be provided to the subscriber. The RA can request the revocation of a subscriber's certificate on behalf of any authorized party, as specified herein. A subscriber may request revocation of their WidePoint PIV SSP issued certificate at any time for any reason. A Sponsoring Organization may request revocation of a WidePoint PIV SSP issued certificate to its authorized representatives (agency employees and/or contractors) at any time for any reason. If the Government provided RA functions, or if the WidePoint PIV SSP has delegated revocation functions to subcontractor RAs, all information is transmitted via a network between WidePoint and/or subcontractors and/or government RAs using mutual authentication.

The WidePoint PIV SSP provides Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to WidePoint PIV SSP certificates via the "revocation' page of the WidePoint PIV SSP website, located at https://orc.widepoint.com/certificate-revocation/.

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

4.9.3 PROCEDURE FOR REVOCATION REQUEST

When a revocation request with a stated reason from revocation comes from an agency designated person authorized to request revocation of certificates for their agency and is digitally or manually signed with identity credentials at least to the same assurance level as the certificate to be revoked, the WidePoint PIV SSP will revoke the certificate immediately.

If a WidePoint PIV SSP CMA or RA is making the request, the reason for the revocation request is documented. If a WidePoint PIV SSP LRA is requesting the revocation, the reason will be

sent to a WidePoint PIV SSP RA via a digitally signed e-mail message for revocation, who investigates the request, document the reason for the revocation request and archive. Upon disposition, the WidePoint PIV SSP CMA or RA sends the reason for revocation and confirm that it was vetted to the WidePoint PIV SSP RA via a digitally signed e-mail message for revocation.

Where subscribers use hardware tokens, revocation is optional if all the following conditions are met:

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

In all other cases, revocation of the certificates is mandatory. Even where all the above conditions have been met, revocation of the associated certificates will be executed.

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

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

If a WidePoint PIV SSP CMA is choosing to revoke a certificate because of sufficient evidence of noncompliance with this WidePoint PIV SSP CPS, a WidePoint PIV SSP RA documents the reason for certificate revocation and notifies the subscriber of the revocation.

Subscribers leaving the organizations that sponsored their participation in the PKI will surrender to their organization's PKI POC (through any accountable mechanism, defined in the RPS) all cryptographic hardware tokens that were issued, under the sponsoring organization, prior to leaving the organization. The PKI POC will zeroize as described in Section 6.2.7 or destroy the token promptly upon surrender and will protect the token from malicious use from the time of surrender. In all cases, whether software or hardware tokens are involved, the organization will promptly notify a WidePoint PIV SSP RA to revoke the certificate and attest to the disposition of the token, via a digitally signed e-mail.

4.9.4 REVOCATION REQUEST GRACE PERIOD

WidePoint PIV SSP issued certificates are revoked upon request as soon as the need can be verified. There is no grace period. The subscriber, or sponsoring organization, must request revocation from the WidePoint PIV SSP as soon as the need for revocation has been determined.

4.9.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

WidePoint PIV SSP CAs will revoke certificates as quickly as practical upon receipt of a proper revocation request. WidePoint PIV SSP RAs receive revocation requests via email request or revocation letters on company letter head. Once a WidePoint PIV SSP RA receives a revocation request email from an WidePoint PIV SSP RA the revocation is conducted immediately. Revocation requests will be processed before the next CRL is published, excepting those requests received within two hours of CRL issuance. Revocation requests received within two hours of CRL issuance will be processed before the following CRL is published.

WidePoint PIV SSP issued certificates are revoked upon request as soon as the need can be verified. There is no grace period. The subscriber, or sponsoring organization, must request revocation from WidePoint PIV SSP as soon as the need for revocation has been determined.

4.9.6 REVOCATION CHECKING REQUIREMENTS FOR RELYING PARTIES

The WidePoint PIV SSP makes no stipulation regarding Relying Parties' checking of revocation information.

Practice note: 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

The WidePoint PIV SSP CAs issue CRLs every 6 hours with a validity period of 48 hours. The WidePoint PIV SSP CAs are configured to ensure the frequency of the nextUpdate, where the parameters for 6-hour frequency and 48-hour validity are maintained. New CRLs are issued four times per day even if there are no changes or updates to be made, and certificate status information is published not later than the next scheduled update.

When a revocation request is granted for the reason of key compromise, the revocation information will be posted on the next CRL, except that, if the revocation request is made within 2 hours of the next schedule CRL, the revocation information may be posted on the very next CRL. All superseded CRLs are removed from the repository upon posting of the latest CRL.

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

WidePoint PIV SSP CRLs may be obtained from:

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

Each WidePoint PIV SSP CRL is published no later than the time specified in the "nextUpdate" field of the previously issued CRL for the same scope.

4.9.8 MAXIMUM LATENCY FOR CRLS

WidePoint PIV SSP CRLs will be posted upon generation, but within no more than 4 hours after generation. Furthermore, each CRL will be published no later than the time specified in the nextUpdate field of the previously issued CRL for the same scope.

4.9.9 ON-LINE REVOCATION/ STATUS CHECKING AVAILABILITY

The WidePoint PIV SSP validates online and near-real-time the status (Valid, Invalid or Suspended) and signature of any WidePoint PIV SSP issued certificate that asserts the certificate policies as defined in Section 1.2. This is indicated in an Certificate Validation Request message through the WidePoint PIV SSP CSS. The WidePoint PIV SSP CSS returns in the Certificate Status Response message a signed message..

The WidePoint PIV SSP CSS is located at:

- http://ssp.eva.orc.com/.

The WidePoint PIV SSP supports online status checking via OCSP [RFC 6960] for end entity certificates issued that assert any certificate policy OID stipulated in this WidePoint PIV SSP CPS, see Section 1.2. Status information maintained by the WidePoint PIV SSP CSS is configured to be updated and available to relying parties within 18 hours.

However, because some relying parties cannot accommodate on-line communications, WidePoint PIV SSP CAs make current and accurate CRLs available, as stated in Section 4.9.7.

For the status of Subscriber Certificates:

- The WidePoint PIV SSP updates information provided via an Online Certificate Status Protocol at least every 18 hours. OCSP responses from this service have a maximum expiration time of ten days.

If the WidePoint PIV SSP CSS receives a request for status of a certificate that has not been issued, then the WidePoint PIV SSP CSS does not respond with a "good" status. The WidePoint PIV SSP monitors the responder for such requests as part of its security response procedures.

The WidePoint PIV SSP operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

The WidePoint PIV SSP CSS maintains an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the WidePoint PIV SSP.

The WidePoint PIV SSP maintains a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

In addition, for id-fpki-common-devices certificates, WidePoint PIV SSP CSS responses must be signed either:

- By the WidePoint PIV SSP CA that issued the certificates whose revocation status is being checked, or
- By a delegated OCSP Responder using a certificate signed by the CA that issued the certificate whose revocation status is being checked.

In the latter case, the OCSP signing Certificate shall contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC2560.

4.9.10 On-line Revocation Checking Requirements

Any delegated OCSP responder used for verifying certificates asserting a certificate policy OID from this WidePoint PIV SSP CPS are required to meet the certificate profile stipulated in the X.509 Certificate and CRL Extensions Profile [CCP-PROF] (refer to sample profile below) and ensure that:

- Certificates indicated as being valid have a chain of valid certificates (valid as defined by [X.509]) linking back to the FCPCA.
- Each certificate in the certificate chain used to validate the certificate whose status is being requested is checked for revocation, such that the relying party need not check more than one responder to validate a subscriber certificate.
- Certificate status responses provide authentication and integrity services commensurate with the assurance level of the certificate being verified.
- It is made clear in the certificate status response the attributes (other than certificate subject name [e.g., citizenship, clearance authorizations, etc.]) being authenticated by the responder.
- Accurate and up-to-date CRLs, from the WidePoint PIV SSP CAs, are used to provide the revocation status.
- Revocation status responses provide authentication and integrity services commensurate with the assurance level of the certificate being checked.

Table 4 presents a sample WidePoint PIV SSP CSS OCSP Responder Self-Signed Certificate.

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Sha256WithRSAEncryption { 1 2 840 113549 1 1 11}
Issuer Distinguished Name	cn=<Host URL | IP Address | Host Name>, ou=<OCSP Responder Name>, o=<Organization>, c=US | *optional:*

Field	Value
	e=admin@mail.com, l=locality, s=state |
Validity Period	Not more than 6 years from date of issue in Generalized Time format
Subject Distinguished Name	cn=<Host URL | IP Address | Host Name>, ou=<OCSP Responder Name>, o=<Organization>, c=US | *optional: e=admin@mail.com, l=locality, s=state* |
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 11}
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	Sha256WithRSAEncryption {1 2 840 113549 1 1 11}
Extensions	Not Present

Table 2: Sample OCSP Responder Self-Signed Certificate

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

4.9.11 Other Forms of Revocation Advertisements Available

WidePoint PIV SSP does not make available any other methods to publicize revoked certificates.

4.9.12 Special Requirements Related To Key Compromise

If a WidePoint PIV SSP certificate is revoked because of suspicion of private key compromise, the following additional requirements apply in addition to requirements specified above.

If a WidePoint PIV SSP CA certificate is revoked, a CRL will be issued within 18 hours of notification.

The WidePoint PIV SSP issues new CRLs with date of compromise and notifies, through website posting, any relying parties that download the CRL that a certificate has been revoked because of key compromise, and the date that the suspected compromise occurred.

If the compromised certificate was a WidePoint PIV SSP RA certificate, the WidePoint PIV SSP RA revalidates any subscriber certificates validated after the date of the suspected compromise, and revokes any certificates not revalidated.

The WidePoint PIV SSP has the ability to transition any reason code to compromise. The process to transition to compromise is a manual process that requires a WidePoint PIV SSP CAA accompanied by a WidePoint PIV SSP SA acting directly on the internal database managing the respective WidePoint PIV SSP CA.

4.9.13 CIRCUMSTANCES FOR SUSPENSION

At no time does the WidePoint PIV SSP suspend a WidePoint PIV SSP CA certificate.

4.9.14 WHO CAN REQUEST SUSPENSION

Not Applicable

4.9.15 PROCEDURE FOR SUSPENSION REQUEST

Not Applicable

4.9.16 LIMITS ON SUSPENSION PERIOD

Not Applicable

4.10 CERTIFICATE STATUS SERVICES

4.10.1 OPERATIONAL CHARACTERISTICS

The WidePoint PIV SSP CSS provides OCSP responses to validation requests and is responsible for:

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

The WidePoint PIV SSP CAA administers the WidePoint PIV SSP CSS.

4.10.2 SERVICE AVAILABILITY

The WidePoint PIV SSP makes no stipulations regarding service availability, except those detailed in Section 4.9.7 and Section 4.9.9.

4.10.3 OPTIONAL FEATURES

None.

4.11 End of Subscription

The WidePoint PIV SSP makes no stipulation regarding subscription, other than a subscription ends when the certificate expires or is revoked.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

WidePoint PIV SSP CA private keys are never escrowed.

Under no circumstances is a signature key escrowed..

For PIV Cards, encryption keys are escrowed within the card management system. Replacement cards issued to a Subscriber may include encryption keys previously issued to the Subscriber. These keys are stored in a key history container.

Escrowed keys are protected at no less than the level of security in which they were generated, delivered, and protected by the subscriber.

Under no circumstances is a subscriber signature key allowed to be held in trust by a third party.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

WidePoint PIV SSP does not support key escrow and recovery using key encapsulation techniques.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

WidePoint PIV SSP CA equipment is dedicated to the CA function. WidePoint PIV SSP RA workstations are dedicated to the use of issuing certificates.

The WidePoint PIV SSP CA, RA, CMS, and CSS equipment consists of equipment dedicated to the WidePoint PIV SSP CA, RA, CMS, and CSS functions, and do not perform non-related functions. The equipment includes, but is not limited to, the system running the WidePoint PIV SSP CA, RA, CMS, and CSS software, hardware cryptographic modules, and databases and directories located on the equipment. In addition, databases and directories located on the equipment are not accessible to the subscribers and Relying Parties.

Unauthorized use of WidePoint PIV SSP CA, RA, CMS, and CSS equipment is forbidden. Physical security controls are implemented that protect the hardware and software from unauthorized use. WidePoint PIV SSP CA equipment is protected from unauthorized access while the cryptographic module is installed and activated via multi-party control. The WidePoint PIV SSP implements multi-level physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. Cryptographic modules and the WidePoint PIV SSP CA cryptographic tokens are protected against theft, loss, and unauthorized use through multi-level physical security and multi-party management.

<REDACTED>

5.1.1 SITE LOCATION AND CONSTRUCTION

<REDACTED>

5.1.2 PHYSICAL ACCESS

Physical access to WidePoint PIV SSP CA, RA and CSS hardware, including the firewall server, and any external cryptographic hardware tokens, is limited to those personnel performing one of the roles identified in Section 5.2. Access to any media containing WidePoint PIV SSP CA, RA or CSS information is also physically protected and access restricted to authorized personnel.

<REDACTED>

5.1.2.1 PHYSICAL ACCESS FOR CA EQUIPMENT

<REDACTED>

5.1.2.2 PHYSICAL ACCESS FOR RA EQUIPMENT

<REDACTED>

5.1.2.3 Physical Access for CSS Equipment

<REDACTED>

5.1.3 Power and Air Conditioning

<REDACTED>

5.1.4 Water Exposure

<REDACTED>

5.1.5 Fire Prevention and Protection

<REDACTED>

5.1.6 Media Storage

<REDACTED>

5.1.7 Waste Disposal

<REDACTED>

5.1.8 Off-Site Backup

<REDACTED>

5.2 Procedural Controls

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles have proven to be diligent and trustworthy as described in the next section. The functions performed in these roles form the basis of trust in the entire PKI. The WidePoint PIV SSP uses two (2) approaches to increase the likelihood that these roles can be successfully carried out. The first approach is to ensure that the persons filling the roles are trustworthy and properly trained. The second is to distribute the functions of the role among several people, so that any malicious activity requires collusion.

The trusted roles are the WidePoint PIV SSP CAA, the SA, RA, and the CSS Administrator. Multiple trusted individuals are employed in a separation of responsibilities. However, the

WidePoint PIV SSP CAA and CSS Administrator roles are combined in one role for the WidePoint PIV SSP. For the purposes of this document the WidePoint PIV SSP CAA and the CSS Administrator roles are designated as WidePoint PIV SSP CAA.

The WidePoint PIV SSP maintains lists, including names, organizations, and contact information, of those company individuals who act in trusted roles, and makes them available during compliance audits. Separation of duties complies with Section 5.2.4 and the requirements of two-person control as stipulated in Section 5.2.2, regardless of the titles and number of Trusted Roles.

5.2.1.1 ADMINISTRATOR

The WidePoint PIV SSP refers to the role of Administrator as a Certificate Authority Administrator (CAA). Any WidePoint PIV SSP CAA who operates a WidePoint PIV SSP CA that asserts a certificate policy OID defined in this document is subject to the stipulations of this WidePoint PIV SSP CPS.

The WidePoint PIV SSP CAA(s) names are logged and made available during compliance audits.

<REDACTED>

5.2.1.2 OFFICER

The WidePoint PIV SSP refers to the role of Officer as a Registration Authority (RA). WidePoint PIV SSP RAs, at the discretion of WidePoint PIV SSP CAAs, can assume the responsibility of issuing and revoking certificates.

<REDACTED>

5.2.1.3 AUDITOR

The WidePoint Corporate Security Auditor is a distinct individual who is not in the direct reporting chain of the Information Technology or Operations departments and does not perform any additional trusted roles.

<REDACTED>

5.2.1.4 OPERATOR

The WidePoint PIV SSP refers to the Operator as the System Administrator (SA).

<REDACTED>

5.2.1.5 TRUSTED AGENTS

In keeping with the goal of maintaining the trustworthiness of WidePoint PIV SSP issued certificates, a separation of roles has been implemented for the operation of the WidePoint PIV SSP card workstation(s). No one (1) person can single-handedly produce a PIV Card. The separation of roles is further enforced by technical controls within the card management application. The roles of WidePoint PIV SSP Sponsor, Registrar, and Issuer are mutually exclusive. Appointment letters for each of these roles are issued to individuals holding their respective role and each of the appointment letters lists the obligations incurred by individuals serving in these roles.

Operational Role Name	Operational Role Definition
WidePoint PIV SSP Sponsor	The individual who confirms authorization for a PIV Card to be issued to the PIV Applicant. The PIV Sponsor adds the pre-registration information to the card management system for the Applicant.
WidePoint PIV SSP Registrar	The individual responsible for identity-proofing the PIV Applicant and ensuring the successful completion of the background checks. The PIV Registrar provides the final approval for the issuance of a PIV Card to the Applicant.
WidePoint PIV SSP Issuer	The individual that performs credential personalization and issues the identity credential to the PIV Applicant after all identity-proofing, background checks, and related approvals have been completed. The PIV Issuer is also responsible for maintaining records and controls for PIV Card stock to ensure that stock is used only to issue valid credentials.

Table 3: PIV Roles

5.2.2 NUMBER OF PERSONS REQUIRED PER TASK

The WidePoint PIV SSP implements commercially reasonable practices that 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. Trusted roles include:

<REDACTED>

Two or more persons are required for the following tasks:

<REDACTED>

Where multi-party control is required, at least one of the participants must be an Administrator. All participants must serve in a trusted role, as defined in Section 5.2.1.

<REDACTED>

5.2.3 Identification and Authentication for Each Role

<REDACTED>

5.2.4 Roles Requiring Separation of Duties

The WidePoint PIV SSP implements commercially reasonable practices that ensure that one person acting alone cannot circumvent safeguards. To increase the likelihood that these roles can be successfully carried out, the functions of WidePoint PIV SSP CAAs, SAs, and RAs are distributed among more than one (1) person, so that any malicious activity would require collusion.

Under no circumstances will the incumbent of these roles perform their own auditing function. No individual is assigned more than one (1) trusted role and no individual is permitted to have more than one identity. For administration of WidePoint PIV SSP CA applications, this is enforced by requiring the WidePoint PIV SSP CAA to log into the operating system, the WidePoint PIV SSP SA then elevates to root privileges, and the WidePoint PIV SSP CAA authenticates to the WidePoint PIV SSP CA application by presenting a certificate and private key password.

<REDACTED>

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

All personnel performing one of the roles identified in Section 5.2.1 are required to have a personal security investigation that has been favorably adjudicated in order to be assigned to sensitive positions. An active secret clearance is sufficient to meet this requirement. For individuals who do not have an active clearance, the WidePoint PIV SSP requests the individual to provide references and sign a background verification disclosure and authorization and release. All personnel in a trusted role go through a background check, performed by a qualified investigator, as described in Section 5.3.2.

WidePoint PIV SSP CAAs, RAs, SAs, and WidePoint Corporate Security Auditors will:

- Be of unquestionable loyalty, trustworthiness, and integrity.
- Have demonstrated security consciousness and awareness in all daily activities.

- Have a strong background in information technology resource administration and technical administration in computer operations, system software, and/or application software totaling 12 months.
- Not be assigned other duties that would interfere with their CAA, RA, or SA duties and responsibilities.
- Not knowingly have been previously relieved of a past assignment for reasons of negligence or non-performance of duties.
- Be U.S. citizens.
- Have demonstrated financial stability.
- Have valid personal security investigations favorably adjudicated and be assigned to sensitive positions.
- Have received proper training in the performance of roles and duties. WidePoint PIV SSP RAs and LRAs are trained in the verification policies and practices of this WidePoint PIV SSP CPS and are trained in the performance of WidePoint PIV SSP RA and LRA duties, respectively.

In addition, WidePoint PIV SSP CAAs and RAs have a technical understanding of WidePoint PIV SSP CA systems and the responsibilities of the WidePoint PIV SSP RA within that system.

WidePoint PIV SSP CAAs, RAs, SAs, and WidePoint Corporate Security Auditors will go through a thorough background check performed by a qualified investigator, including, but not limited to:

- Criminal history check that shows no misdemeanor or felony convictions.
- Civil lawsuit history checks and a social security number trace to confirm valid number.
- Personal, financial, and work/job reference checks which show that the subject of the check is competent, reliable, and trustworthy.
- Financial status check showing that the subject of the check has not committed any fraud or is otherwise financially trustworthy.
- Education verification of highest or most relevant degree.
- DMV records will demonstrate no pattern of violations.
- A residence check to demonstrate that the person is a trustworthy neighbor.

An active secret clearance is sufficient to meet this requirement. The results of these checks will not be released except as required by the FPCPF.

5.3.2 BACKGROUND CHECK PROCEDURES

WidePoint PIV SSP CAAs, RAs, SAs, and WidePoint Corporate Security Auditors will either hold a US security clearance or go through a thorough background check covering:

- Criminal history check that shows no misdemeanor or felony convictions.
- Civil lawsuit history checks and a social security number trace to confirm valid number.
- Personal, financial, and work/job reference checks which show that the subject of the check is competent, reliable and trustworthy.
- Financial status check showing that the subject of the check has not committed any fraud or is otherwise financially trustworthy.
- Education verification of highest or most relevant degree.
- DMV records will demonstrate no pattern of violations.
- A residence check to demonstrate that the person is a trustworthy neighbor.
- Social Security trace will show that the person has a valid social security number.

The period of investigation must cover at least the last five (5) years for each area, excepting the residence check which must cover at least the last three (3) years. Regardless of the date of award, the highest educational degree must be verified.

An active secret clearance will be sufficient to meet this requirement. The results of these checks will not be released except as required by Section 9.4.4.

Re-screening is performed when required, as determined by the requirements of the initial investigation (e.g. Secret, 10 years; Confidential, 15 years). The WidePoint Facility Security Officer is responsible for maintaining and stewardship of clearance data.

5.3.3 TRAINING REQUIREMENTS

All personnel, and contractors located or working on-site or accessing U.S. Government IT resources receive information systems security awareness training annually. Additionally, periodic refresher training is provided to all personnel. The training program covers the requirements of the Computer Security Act of 1987, Public Law 100-235, which are adequately detailed in the Office of Personnel Management Computer Security Awareness Training materials
<REDACTED>

5.3.4 Retraining Frequency and Requirements

Those involved in filling trusted roles are made aware of changes in an WidePoint -authorized CA operation by way of notifications and training resulting from any changes to WidePoint PIV SSP CAs or CSSs operation. Any significant changes to the operation require retraining which must be documented. WidePoint PIV SSP maintains a file of signed and dated statements from the WidePoint PIV SSP personnel listing their names, roles, re-training received, and date training completed.

5.3.5 Job Rotation Frequency and Sequence

WidePoint ensures the continuity and integrity of the WidePoint PIV SSP services.

5.3.6 Sanctions for Unauthorized Actions

Any unauthorized actions resulting in irreparable damage to the WidePoint PIV SSP systems such as compromising any private key will be prosecuted to the fullest extent of the law. The responsible individuals may be prosecuted to the maximum of extent that the law affords, both criminal and civil.

Any unauthorized actions by a WidePoint PIV SSP RA will result in the immediate revocation of the RA certificate and the removal of that individual from the RA role. Certificates issued by that RA might also be revoked. The RA may be prosecuted for any damages caused to the WidePoint PIV SSP system.

Any unauthorized actions by an RA or LRA will result in the immediate revocation of the RA/ LRA certificate and the removal of that individual from the RA/ LRA role. Certificates validated by that RA/ LRA might also be revoked. The RA/ LRA may be prosecuted for any damages caused to the WidePoint PIV SSP system.

5.3.7 Independent Contractor Requirements

Any company subcontracting to provide services for any WidePoint PIV SSP CMA role with regards to the WidePoint PIV SSP system is required to establish procedures, which are reviewed and approved by WidePoint. The subcontractor will require all employees delivering such services to be in accordance with this WidePoint PIV SSP CPS and the FPCPF, and subject to the compliance audit requirements of this WidePoint PIV SSP CPS.

5.3.8 Documentation Supplied to Personnel

Operations and maintenance documentation is supplied to authorized individuals performing the roles of WidePoint PIV SSP CAAs and SAs. Operations manuals for WidePoint PIV SSP systems and administration are written and managed for each logical instance of the WidePoint PIV SSP system and each physical instance of an WidePoint PIV SSP system.

Documentation is provided to personnel as required for fulfilling the requirements of each role.

5.4 AUDIT LOGGING PROCEDURES

<REDACTED>

5.5 RECORDS ARCHIVAL

<REDACTED>

5.6 KEY CHANGEOVER

<REDACTED>

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

Compromise or disaster notification and recovery procedures are employed by WidePoint to ensure a secure state.

<REDACTED>

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

<REDACTED>

5.7.3 ENTITY (CA) PRIVATE KEY COMPROMISE PROCEDURES

<REDACTED>

5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

The WidePoint PIV SSP maintains a Disaster Recovery Plan (DRP). <REDACTED>

5.8 AUTHORITY TERMINATION

<REDACTED>

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

CA key pair generation is created with a verifiable audit trail that the security requirements for procedures were followed. The generation process follows established Certification Authority processes, a written script and is video recorded. The process is detailed enough to show that appropriate role separation was used.

6.1.1.1 CA KEY PAIR GENERATION

WidePoint PIV SSP CA certificate-signing keys are generated in FIPS 140-2 Level 3 validated cryptographic Hardware Security Modules (HSM) under multi-party control.

WidePoint PIV SSP CA key pair generation is created with a verifiable audit trail that the security requirements for procedures were followed. All WidePoint PIV SSP CA key pair generation is captured with video recording for verifiable proof that the documented procedure is followed. The documentation of the procedure details that appropriate role separation is used, and the video provides proof. The key generation procedures are witnessed by WidePoint PIV SSP personnel other than those performing the trusted roles for the key generation. All persons in attendance during the key generation procedure sign a key generation attendance sheet. The attendance sheet is placed in the program binder located in the WidePoint Corporate Security Auditor safe drawer in the WidePoint PIV SSP SNOC. Key generation procedures and artifacts are made available to the independent third-party auditor during annual audits.

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

<REDACTED>

6.1.1.3 CSS KEY PAIR GENERATION

The WidePoint PIV SSP CSS (OCSP responder) certificate signing keys will be generated in a FIPS 140-2 Level 2 (or higher) validated cryptographic HSM in accordance with FIPS 186-2 (specific make/model HSM are: Thales [nCipher], NetHSM 500, Validation #770). All WidePoint PIV SSP CAs and CSSs (OCSP responder) employ products operating in the “FIPS mode.”

6.1.1.4 PIV CONTENT SIGNING KEY PAIR GENERATION

For WidePoint PIV SSP CMS which issues PIV Content-Signing certificates, the keys will be generated using a FIPS 140-2 (or higher) HSM for the CMS. The WidePoint PIV SSP does not support issuance of id-fpki-common-High.

The HSM key generation occurs when the WidePoint PIV SSP issues a CSR command to the HSM. This causes the HSM to generate the private key within its FIPS 140-2 Level 2 or higher environment. Procedure documentation for accomplishing generation of PIV Content-signing key pair is maintained on a certificate-enabled internal wiki page.

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER

The WidePoint PIV SSP subscriber's private key for id-fpki-common-hardware, id-fpki-common-authentication, and id-fpki-common-cardAuth is generated directly on the subscriber's token; or, in the case of id-fpki-common-hardware key management certificates, in a key generator which benignly transfers the key to the subscriber's token. The subscriber is in possession and control of the private key at the time of generation for id-fpki-common-policy, id-fpki-common-devices, id-fpki-common-derived-pivAuth, and id-fpki-common-derived-pivAuth-hardware.

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

As part of the certificate application process, the subscriber's public key is transferred to <REDACTED>

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

The WidePoint PIV SSP supports delivery of its CA and trust anchor public keys (including the FCPCA trust anchor) via a web interface to a protected server using SSL. The public key is stored such that it is unalterable and not subject to substitution. Relying Parties must contact the help desk to receive the official certificate hashes to compare them with the certificates downloaded from the site.

<REDACTED>

6.1.5 KEY SIZES

Digital Signature certificates asserting the FPCPF certificate policy OIDs that have an expiration date after December 30, 2008 will use a 2048-bit modulus. Digital Signature Standard (DSS) and Elliptic Curve are not supported.

<REDACTED>

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

Public key parameters for use with the RSA algorithm defined in PKCS#-1 are generated and checked in accordance with PKCS#-1.

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

The WidePoint PIV SSP certifies keys for use in signing or encrypting, but not both. The use of a specific key is determined by the key usage extension. The key usage extension is included in all certificates and is always marked critical in order to limit the use of public key certificate for its intended purpose, as stipulated in the X.509 Certificate and CRL Extensions Profile [CCP-PROF].

WidePoint PIV SSP user certificates that assert id-fpki-common-authentication, id-fpki-common-derived-pivAuth-hardware, id-fpki-common-derived-pivAuth, or id-fpki-common-cardAuth only assert the digitalSignature bit. Other WidePoint PIV SSP user certificates used for digital signatures assert both the digitalSignature and nonRepudiation bits. WidePoint PIV SSP certificates that contain RSA public keys that are to be used for key transport assert the keyEncipherment bit. Public keys that are bound into WidePoint PIV SSP CA certificates are used only for signing certificates and status information (e.g., CRLs). WidePoint PIV SSP CA certificates whose subject public key is used to verify other certificates asserts the keyCertSign bit. WidePoint PIV SSP CA certificates whose subject public key is used to verify CRLs asserts the cRLSign bit. WidePoint PIV SSP CA certificates whose subject public key is used to verify Online Certificate Status Protocol (OCSP) responses asserts the digitalSignature and/or nonRepudiation bits. WidePoint PIV SSP device certificates used for digital signatures [including authentication] assert the digitalSignature bit. WidePoint PIV SSP device certificates that contain RSA public keys that are used for key transport assert the keyEncipherment bit. WidePoint PIV SSP device certificates used for both digital signatures and key management assert the digitalSignature bit and the keyEncipherment bit. WidePoint PIV SSP device certificates do not assert the nonRepudiation bit. The dataEncipherment, encipherOnly, and decipherOnly bits are not asserted in certificates issued under the WidePoint PIV SSP program.

For End Entity certificates issued after June 30, 2019, the Extended Key Usage extension will always be present and shall not contain *anyExtendedKeyUsage* {2.5.29.37.0}. Extended Key Usage OIDs shall be consistent with key usage bits asserted.

If a certificate is used for authentication of ephemeral keys, the Key Usage bit in the certificate must assert the DigitalSignature bit and may or may not assert Key Encryption and Key Agreement depending on the public key in the SPKI of the certificate.

WidePoint PIV SSP signing certificates issued for id-fpki-common-piv-contentSigning include an extended key usage of id-PIV-content-signing (see [CCP-PROF]).

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

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

Subscribers will use cryptographic modules that have been validated to meet at least the criteria specified for FIPS 140 Level 1 for all cryptographic operations. FIPS 140 Level 2 must be used to receive a Medium Hardware Assurance certificate, including PIV.

<REDACTED>

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

<REDACTED>

6.2.3 Private Key Escrow

Under no circumstances is a WidePoint PIV SSP CA signature key used to sign certificates or CRLs escrowed.

Human subscriber key management keys are escrowed to provide key recovery as described in Section 4.12.1. If a device has a separate key management key certificate, the key management private key may be escrowed.

Under no circumstances will a signature key be escrowed.

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Private Signature Key

The WidePoint PIV SSP may back up CA private keys on a separate cryptographic module in order to alleviate the need to re-key in the case of cryptographic module failure. At least one copy of the private signature key will be stored off-site. The backup module is an HSM that meets FIPS 140 Level 3 requirements and Level 3 key management requirements. In the event a WidePoint PIV SSP CA private key requires back-up, the procedure is performed under the same multi-person control as the generation of the original signature key. The module is under the protection of WidePoint PIV SSP CAAs and SAs and under lock and key at all times, in accordance with this WidePoint PIV SSP CPS. When the WidePoint PIV SSP re-keys, the private key in the backup module is zeroed or otherwise destroyed.

6.2.4.2 BACKUP OF SUBSCRIBER PRIVATE SIGNATURE KEY

Backup copies must be stored in an encrypted form and protected by a password from unauthorized access. The Subscriber (PKI Sponsor for Component) is responsible for ensuring that all copies of private keys, including those that might be embedded in component backups, are protected. This includes protecting any workstation on which any of its private keys reside. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module.

For id-fpki-common-hardware, id-fpki-common-authentication, id-fpki-common-derived-pivAuth-hardware, and id-fpki-common-cardAuth, private signing keys are generated on the token and are not backed up or copied.

6.2.4.3 BACKUP OF SUBSCRIBER PRIVATE KEY MANAGEMENT KEY

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

6.2.4.4 BACKUP OF CSS PRIVATE KEY

<REDACTED>

6.2.4.5 BACKUP OF DEVICE PRIVATE KEY

For device certificates, the WidePoint PIV SSP recommends to the component PKI Sponsors to make a single backup copy of the component private keys to support backup in cases where component malfunction results in key corruption and will provide recommended procedures. The PKI Sponsors will also be advised that backup private key must be stored on a removable media and cannot be kept online. Backed up device private keys must 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.

6.2.4.6 BACKUP OF COMMON PIV CONTENT SIGNING KEY

All key transfers must be done from an approved cryptographic module, and the key must be encrypted during the transfer. The WidePoint PIV SSP PIV Content Signing private signature keys are backed up under multi-person control. At least one copy of the private signature key is stored at the WidePoint PIV SSP DR facility. All copies of the WidePoint PIV SSP PIV Content Signing private signature key are accounted for and protected in the same manner as the original. The Subscriber (PKI Sponsor) is responsible for ensuring that all copies of private keys, including those that might be embedded in component backups, are protected, including protecting any workstation on which any of its private keys reside.

6.2.5 PRIVATE KEY ARCHIVAL

Under no circumstances are WidePoint PIV SSP CA private signature keys, subscriber private signatures keys, non-repudiation signature or authentication keys archived. Archival or long-term back-up of confidentiality keys is recommended if any information encrypted with those keys is archived in its encrypted state.

Escrowed keys are stored in a protected WidePoint PIV SSP KED, in accordance with this CPS. The WidePoint PIV SSP KED consists of equipment dedicated to the key recovery and archival functions.

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

WidePoint PIV SSP CA private keys may be exported from the cryptographic module only to perform WidePoint PIV SSP CA key backup procedures, as described in Section 6.2.4.1. At no time will a WidePoint PIV SSP CA private key exist in plaintext outside the cryptographic module.

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

6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

The WidePoint PIV SSP makes no stipulations regarding private key storage on cryptographic modules beyond that specified in FIPS 140.

6.2.8 METHOD OF ACTIVATING PRIVATE KEY

A passphrase/PIN/biometric will be used to activate the private key for WidePoint PIV SSP RA, LRA, subscriber medium assurance and medium hardware assurance (e.g. PIV). Passwords will be generated by the subscriber and entered at the time of key generation (at the WidePoint PIV SSP RA/LRA workstation in the case of medium hardware assurance) and managed according to the FIPS 140-2 guidance for strong passwords in accordance with the subscriber obligation agreement. Entry of activation data will be protected from disclosure.
<REDACTED>

6.2.9 METHOD OF DEACTIVATING PRIVATE KEY

<REDACTED>

6.2.10 Method of Destroying Private Key

<REDACTED>

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Archival of public keys is achieved via certificate archival.

6.3.2 Certificate Operational Periods and Key Usage Periods

The maximum validity period of a WidePoint PIV SSP CA signature certificate is 10 years. A WidePoint PIV SSP CA private key will be used for signing subscriber certificates for no more than four years.

<REDACTED>

6.3.3 Restrictions on CA Private Key Usage

The private key used by WidePoint PIV SSP CAs for issuing certificates is used only for signing such WidePoint PIV SSP certificates and, optionally, CRLs or other validation services responses.

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

The private key used by each WidePoint PIV SSP RA in connection with the issuance of WidePoint PIV SSP certificates is used only for communications relating to the approval, issuance, or revocation of such certificates.

Under no circumstances will the WidePoint PIV SSP 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

<REDACTED>

6.4.2 Activation Data Protection

<REDACTED>

6.4.3 Other Aspects of Activation Data

If during the life of the PIV card the card becomes locked due to failed PIN attempts, the PIN may be reset. To complete a PIN reset the cardholder must appear in-person to a WidePoint PIV SSP Registration/Issuance/Activation workstation and perform a 1:1 biometric match of the PIV cardholder against the biometric included in the PIV card prior to releasing the unlocked PIV card back to the cardholder. This biometric 1:1 match can only be conducted by a trusted agent of the WidePoint PIV SSP.

6.5 Computer Security Controls

<REDACTED>

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

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

Security management control includes the execution of tools and procedures to ensure that the operational system and network adhere to configured security. These tools and procedures include checking the integrity of the security software, firmware, and hardware to ensure their correct operation.

<REDACTED>

6.6.2 Security Management Controls

<REDACTED>

6.6.3 OBJECT REUSE

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 are documented in WidePoint's Policies and Procedures, and the WidePoint System Security Plan.

6.6.4 LIFE CYCLE SECURITY CONTROLS

<REDACTED>

6.7 NETWORK SECURITY CONTROLS

<REDACTED>

6.8 TIME-STAMPING

The WidePoint PIV SSP system provides time stamps for use in audit record generation. The WidePoint PIV SSP maintains an internal time service <REDACTED>

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

WidePoint PIV SSP issued certificates contain public keys used for authenticating the sender and receiver of an electronic message and verifying the integrity of such messages, i.e., public keys used for digital signature verification.

WidePoint PIV SSP issues and maintains certificates that conform to the ITU-T Recommendation X.509, *"The Directory: Authentication Framework,"* June 1997.

All WidePoint PIV SSP issue certificates include a FPCPF certificate policy OID as specified in Section 1.2 within the appropriate field, and contain the required certificate fields according to the X.509 Certificate and CRL Extensions Profile [CCP-PROF] and this WidePoint PIV SSP CPS.

Complete certificate profile information, including key generation methods, for WidePoint certificates can be found in the X.509 Certificate and CRL Extensions Profile for the Common Policy [CCP-PROF] and the applicable WidePoint PIV SSP CA build document.

7.1.1 VERSION NUMBER(S)

WidePoint PIV SSP CAs are configured to issue X.509 v3 certificates (populate version field with integer 2).

7.1.2 CERTIFICATE EXTENSIONS

WidePoint PIV SSP certificate profiles are in accordance with the requirements of the certificate profiles described in the X.509 Certificate and CRL Extensions Profile [CCP-PROF] and the applicable WidePoint PIV SSP CA build document.

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

7.1.3 ALGORITHM OBJECT IDENTIFIERS

WidePoint PIV SSP CAs are configured to issue certificates that use the following OIDs for signatures.

Sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

WidePoint PIV SSP issued certificates use the following OIDs for identifying the algorithm for which the subject key was generated.

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

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

The WidePoint PIV SSP does not generate elliptic curve public keys or implement RSA with PSS padding.

7.1.4 NAME FORMS

X.500 Distinguished Names (DNs) are used by all WidePoint PIV SSP CAs in the issuer and subject fields of the certificates, with the attribute type as further constrained by RFC 5280.

X.500 Directories use the DN for lookups. All Relying Parties will have the ability to process DNs. If communities request to use other names, for example certificates used to implement a hardware protocol, where device addresses are most useful and certificate lookup is not performed, WidePoint will define alternate name forms to be included in the subjectAltName extension and provide the alternative name form to the Policy Authority. Any name form, defining General Name [ISO9594-8] is used, in accordance with the required profile as specified in Section 3.1.

The subject field in certificates issued under id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-authentication, id-fpki-common-derived-pivAuth-hardware, id-fpki-common-derived-pivAuth, id-fpki-common-piv-contentSigning, and id-fpki-common-devices is populated with an X.500 distinguished name as specified in Section 3.1.

The issuer fields of certificates are populated with a non-empty X.500 Distinguished Name as specified in Section 3.1.

The subject alternative name extension is present and includes the pivFASC-N name type in certificates issued under id-fpki-common-authentication and id-fpki-common-cardAuth.

The subject alternative name extension is present and includes a UUID, encoded as a URI, in certificates issued under id-fpi-common-authentication, id-fpki-common-cardAuth, id-fpki-common-derived-pivAuth-hardware, and id-fpki-common-derived-pivAuth.

7.1.5 NAME CONSTRAINTS

The WidePoint PIV SSP CAs may assert name constraints in CA certificates.

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIERS

WidePoint PIV SSP issued certificates assert the certificate policy OID appropriate to the level of assurance with which it was issued. WidePoint PIV SSP issued certificates issued under this

WidePoint PIV SSP CPS assert at least one of the following OIDs in the certificate policies extension, as appropriate:

- id-fpki-common-policy ::= {2 16 840 1 101 3 2 1 3 6}
- id-fpki-common-hardware ::= {2 16 840 1 101 3 2 1 3 7}
- id-fpki-common-devices ::= {2 16 840 1 101 3 2 1 3 8}
- id-fpki-common-authentication ::= {2 16 840 1 101 3 2 1 3 13}
- id-fpki-common-derived-pivAuth ::= {2 16 840 1 101 3 2 1 3 40}
- id-fpki-common-derived-pivAuth-hardware ::= {2 16 840 1 101 3 2 1 3 41}
- id-fpki-common-cardAuth ::= {2 16 840 1 101 3 2 1 3 17}
- id-fpki-common-piv-contentSigning ::= {2 16 840 1 101 3 2 1 3 39}

WidePoint PIV SSP issued certificates that assert the id-fpki-common-piv-contentSigning policy OID will not express any other certificate policy OIDs.

7.1.7 Usage of Policy Constraints Extension

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

7.1.8 Policy Qualifiers Syntax and Semantics

The certificates issued under this WidePoint PIV SSP CPS do not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

WidePoint PIV SSP CAs are configured to not set the certificate policies extension to be critical. Relying Parties whose client software does not process this extension operate in this regard at their own risk. Processing semantics for the critical certificate policy extension used by WidePoint conforms to X.509 Certificate and CRL Extensions Profile [CCP-PROF].

7.1.10 Inhibit Any Policy Extension

WidePoint PIV SSP 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.

*Note: The recommended criticality setting is different from RFC 5280.

7.2 CRL Profile

WidePoint PIV SSP CRL profiles addressing the use of each extension are provided in and conform to the X.509 Certificate and CRL Extensions Profile [CCP-PROF] and the applicable WidePoint PIV SSP CA build document.

7.2.1 Version Number(s)

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

7.2.2 CRL and CRL Entry Extensions

Detailed CRL profiles covering the use of each extension are available and described in the X.509 Certificate and CRL Extensions Profile [CCP-PROF] and are in accordance with the CRL profile of that document. WidePoint PIV SSP CAs support CRL Distribution Points (CRL DP) in all Subscriber certificates.

7.3 OCSP Profile

WidePoint PIV SSP CSSs sign responses using algorithms designated for CRL signing, as shown below. OCSP requests are not required to be signed (refer to RFC6960 for detailed syntax). OCSP requests and responses contain the following formats as shown in Table 7 below.

Field	Expected Value
Version	V3 (2)
Requester Name	Not Required
Request List	List of certificates – generally this should be the list of two certificates: WidePoint PIV SSP CA certificate and end entity certificate
Signature	Not Required
Extensions	Not Required

Table 4: OCSP Request Format

Table 8 lists which fields are populated by a WidePoint OCSP Responder:

Field	Expected Value
Response Status	Successful | Malformed Request | Internal Error | Try Later
Response Type	id-pkix-ocsp-basic {1 3 6 1 5 5 7 48 1 1}
Version	V1 (0)
Responder ID	Hash of Responder public key
Produced At	Generalized Time
List of Responses	Each response will contain certificate id; certificate status1, thisUpdate, nextUpdate2,
Extension	
Nonce	Will be present if nonce extension is present in the request
Signature Algorithm	Sha256WithRSAEncryption {1 2 840 113549 1 1 11}
Signature	Present
Certificates	Applicable certificates issued to the OCSP Responder

Table 5: OCSP Response Format

7.3.1 VERSION NUMBER(S)

WidePoint PIV SSP CSSs operated under this WidePoint PIV SSP CPS uses OCSP Version 1.

7.3.2 OCSP EXTENSIONS

Critical OCSP extensions are not used.

1 If the certificate is revoked, the OCSP Responder will provide revocation time and revocation reason from CRL entry and CRL entry extension.
2 The OCSP Responder will use thisUpdate and nextUpdate from CA CRL.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The WidePoint PIV SSP is subject to an annual review by the FPKIPA to ensure that WidePoint PIV SSP policies and operations remain compliant with the FPCPF.

The WidePoint PIV SSP conducts an annual compliance audit, or earlier if requested, to ensure that the requirements of this WidePoint PIV SSP CPS are being implemented and enforced. The WidePoint PIV SSP PMA is responsible for ensuring audits are conducted for all WidePoint PIV SSP functions regardless of how or by whom the WidePoint PIV SSP components are managed and operated. No particular assessment methodology is required.

8.1 FREQUENCY OF AUDIT OR ASSESSMENT

The WidePoint PIV SSP systems are periodically, but at a minimum annually, independently audited for conformance to the appropriate policies and procedures, as well as the “Compliance Audit Requirements” document. The WidePoint PIV SSP operates primary and secondary (backup) secure data centers in conformance with FISMA and commercial practices. The WidePoint PIV SSP systems conform to FISMA requirements, as stipulated for Moderate systems.

The WidePoint PIV SSP has developed certification, accreditation, and security assessment policies and procedures that are at a minimum reviewed and updated annually, in accordance with NIST SP 800-53.

Security controls are reviewed, at a minimum, annually and updated accordingly for the purpose of determining the extent to which controls are correctly implemented and operating, and meeting the system’s security needs.

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

The WidePoint PIV SSP is subject to an annual review by the FPKIPA to ensure that WidePoint PIV SSP policies and operations remain compliant with the FPCPF.

8.2 IDENTITY/ QUALIFICATIONS OF ASSESSOR

The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the WidePoint PIV SSP CPS and the FPCPF. The compliance auditor must perform such compliance audits as a regular ongoing business activity. In addition to the previous requirements, the auditor must be a certified information system auditor (CISA) or IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

An independent, third-party auditing firm audits the WidePoint PIV SSP annually, in accordance with FISMA for compliance. WidePoint has an independent internal department that performs weekly procedures in order to attest to WidePoint compliance with This WidePoint PIV SSP CPS. Audit and inspection is accomplished in accordance with the NIST SP 800-53.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The compliance auditor either will be a private firm that is independent from the entities (CA and RAs) being audited, or it will be sufficiently organizationally separated from those entities to provide an unbiased, independent evaluation. An example of the latter situation may be an Agency inspector general. To insure independence and objectivity, the compliance auditor may not have served in developing or maintaining the WidePoint PIV SSP SNOC Facility or this WidePoint PIV SSP CPS. The FPKIPA will determine whether a compliance auditor meets this requirement.

The Agency PMA is responsible for identifying and engaging a qualified auditor of agency operations implementing aspects of this WidePoint PIV SSP CPS and providing the WidePoint PIV SSP with a copy of the audit report letter as evidence of completion of an annual audit.

The WidePoint PIV SSP relies upon the combined efforts of an independent external IT auditor, which is an entity separate from WidePoint, and an internal audit capability that is sufficiently organizationally separated from those entities operating WidePoint PIV SSP CAs, so as to provide an unbiased, independent evaluation. The WidePoint PIV SSP performs internal audits of WidePoint PIV SSP CSS and RA facilities, as defined herein.

8.4 TOPICS COVERED BY ASSESSMENT

The purpose of WidePoint PIV SSP compliance audits is to verify that the WidePoint PIV SSP and its recognized trusted roles comply with all the requirements of the current versions of the CP and This WidePoint PIV SSP CPS. All aspects of the WidePoint PIV SSP operation are subject to compliance audit inspections. Components other than WidePoint PIV SSP CAs may be audited fully or by using a representative sample. If the auditor uses statistical sampling, all WidePoint PIV SSP components, WidePoint PIV SSP component managers and operators must be considered in the sample. The samples must vary on an annual basis.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

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

1) The compliance auditor will note the discrepancy.
2) The compliance auditor will notify the parties, identified in Section 8.6, of the discrepancy and determine what further notifications or actions are necessary.
3) WidePoint will propose a remedy, including expected time for completion, to the FPKIPA and each WidePoint PIV SSP Agency PMA.

Any remedy may include permanent or temporary WidePoint PIV SSP cessation or termination of WidePoint PIV SSP operation to revoke a certificate issued by the CA, or take other actions deemed appropriate. However, several factors must be considered in this decision, including the severity of the discrepancy and the risks it imposes, and the disruption to the certificate using community.

Remedies will be defined by the FPKIPA and communicated to WidePoint as soon as possible to limit the risks created. The FPKIPA and WidePoint will determine a time for completion. The implementation of remedies will be coordinated between the FPKIPA-affected Agency and WidePoint, and subsequently communicated to the FPKIPA. A special audit may be required to confirm the implementation and effectiveness of the remedy.

8.6 COMMUNICATION OF RESULTS

On an annual basis, an Auditor Letter of Compliance, prepared in accordance with the FPKI Annual Review Requirements document, on behalf of an Agency PMA and its management, and operation of WidePoint PIV SSP RA and/or LRA equipment and systems on-site at the Agency's facility must be provided to the WidePoint PIV SSP.

On an annual basis, WidePoint PIV SSP submits an annual review package to the FPKIPA. This package is prepared in accordance with the FPKI Compliance Audit Requirements document and includes an assertion from WidePoint PIV SSP that all PKI components have been audited – including any components that may be separately managed and operated. The report shall identify the versions of the FPCPF CP and this WidePoint PIV SSP CPS used in the assessment. Additionally, where necessary, the results will be communicated as set forth in Section 8.5 above.

Required remedies will be defined and communicated by the auditor to the WidePoint PIV SSP as soon as possible to limit the risks created. A special audit may be required to confirm the implementation and effectiveness of the remedy.

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

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

Fees are either published on the WidePoint PIV SSP website or established contractually.

9.1.1 CERTIFICATE ISSUANCE OR RENEWAL FEES

A fee per validity year, unless otherwise negotiated, is levied by WidePoint PIV SSP to issue certificates that FPCPF certificate policies as described in Section 1.2. Likewise, a fee per each additional year, unless otherwise negotiated, is levied by WidePoint to renew a WidePoint PIV SSP certificate. A fee per encryption certificate is levied for the escrowing of encryption keys.

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

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

9.1.2 CERTIFICATE ACCESS FEES

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

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEES

WidePoint does not charge additional fees for access to CRLs and OCSP status information.

9.1.4 FEES FOR OTHER SERVICES

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

9.1.5 Refund Policy

Refunds may be negotiated on a case-by-case basis. As described in Section 4.4.1, the subscriber is in possession and control of the private key at the time of issuance. Once issuance has occurred, there will be no refund.

9.2 Financial Responsibility

WidePoint PIV SSP does not limit the use of certificates issued by CAs under this WidePoint PIV SSP CPS. Rather, entities, acting as relying parties, must determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction.

9.2.1 Insurance Coverage

WidePoint maintains reasonable levels of business insurance.

9.2.2 Other Assets

Not applicable.

9.2.3 Insurance or Warranty Coverage for End-Entities

Not applicable.

9.3 Confidentiality of Business Information

WidePoint PIV SSP CA information not requiring protection is made publicly available. Public access to WidePoint PIV SSP organizational information will be determined at the sole discretion of WidePoint PIV SSP.

9.3.1 Scope of Confidential Information

The WidePoint PIV SSP will keep the following information confidential at all times:

- Private signing and client authentication keys
- Personal or non-public information about Subscribers
- WidePoint security mechanisms

9.3.2 Information not within the Scope of Confidential Information

Information deemed not within the scope of confidential information will include:

- Information included in WidePoint PIV SSP issued certificates
- WidePoint PIV SSP CA public certificates
- Information contained in the WidePoint PIV SSP CPS summary document
- Any certificate status or certificate revocation reason code

9.3.3 Responsibility to Protect Confidential Information

Except as required to support the audits performed by the WidePoint PIV SSP independent external auditor, confidential information will not be released to third parties unless required by law or requested by a court with jurisdiction over the WidePoint PIV SSP.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The WidePoint PIV SSP conducts a Privacy Threshold Analysis in compliance with FISMA and NIST SP 800-53. The WidePoint PIV SSP protects all Subscriber identifying information. All Subscriber identifying information will be maintained in accordance with applicable laws.

9.4.2 Information Treated as Private

Information requested from individuals during the certificate issuance process other than that information which is specifically included in the certificate, is withheld from release. This information may include personal information as described in Section 3.1 and is subject to the Privacy Act. All information in the WidePoint PIV SSP record (not repository) is handled as SBU, and access will be restricted to those with official needs. The contents of the archives maintained by WidePoint PIV SSP CAs operating under the CP and This WidePoint PIV SSP CPS will not be released except as required by law.

Collection of PII is limited to the minimum necessary to validate the identity of the subscriber. This may include attributes that correlate identity evidence to authoritative sources. The WidePoint PIV SSP RA will provide explicit notice to the subscriber regarding the purpose for collecting and maintaining a record of the PII necessary for identity proofing and the consequences for not providing the information. PII collected for identity proofing purposes shall not be used for any other purpose.

WidePoint PIV SSP issued certificate private keys are considered sensitive and access will be restricted to the certificate owner, except as stipulated with regard to escrow and/or recovery of encryption certificates. Private keys protected by the WidePoint PIV SSP will be held in strictest confidence. Under no circumstances will any private key appear unencrypted outside WidePoint PIV SSP hardware. Private keys held in escrow by the WidePoint PIV SSP will be released only to a trusted authority in accordance with this WidePoint PIV SSP CPS, or law enforcement official, in accordance with U.S. law, the FPCPF, and this CPS.

WidePoint PIV SSP audit logs and transaction records as a whole are considered sensitive and will not be made available publicly.

9.4.3 Information not Deemed Private

No sensitive information will be held in certificates, as certificate information is publicly available in repositories. Information not considered sensitive includes the subscriber's name, electronic mail address, certificate public key, and certificate validity period. However, certificates which contain the FASC-N in the subject alternative name extension will not be made publicly available.

9.4.4 Responsibility to Protect Private Information

The WidePoint PIV SSP will not disclose certificate-related information to any third party unless authorized by the FPKIPA or Agency PMA, required by law, government rule or regulation, or order of a court of competent jurisdiction. The WidePoint PIV SSP will authenticate any request for release of information. Sensitive But Unclassified (SBU) information pertaining to the WidePoint PIV SSP program will be securely stored at either WidePoint's facility or WidePoint's off-site location. This does not prevent the WidePoint PIV SSP from disclosing the certificate and certificate status information (e.g., CRL, OCSP Requests and Responses, etc.).

9.4.5 Notice and Consent to Use Private Information

The WidePoint PIV SSP PMA or Agency PMA is not required to provide any notice or obtain the consent of the subscriber or Authorized Agency Personnel in order to release private information in accordance with other stipulations of Section 9.4. All notices will be in accordance with the applicable laws.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

9.4.7 Other Information Disclosure Circumstances

None.

9.5 Intellectual Property Rights

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

- Certificates and CRLs are the property of the WidePoint PIV SSP. Permission is granted to reproduce and distribute certificates issued by the WidePoint PIV SSP on a nonexclusive, royalty-free basis, provided that they are reproduced and distributed in full. WidePoint PIV SSP CA certificates and CRLs will not be published in any publicly accessible repository or directory without the express written permission of WidePoint PIV SSP.
- This WidePoint PIV SSP CPS is the sole property of the Widepoint Corporation.
- Private keys are the personal property of the subscribers who rightfully use or are capable of using them (or their employer or principal), regardless of the physical medium within which they are stored and protected.
- Public keys are the personal property of subscribers (or their employer or principal), regardless of the physical medium within which they are stored and protected.
- WidePoint PIV SSP Certificates, including WidePoint PIV SSP public keys, are the property of WidePoint. WidePoint licenses relying parties to use such keys only in conjunction with FIPS 140-2 validated encryption modules.

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

9.6 Representations and Warranties

Agencies contracting with the WidePoint PIV SSP for services and certificates under this WidePoint PIV SSP CPS are required to ensure that their respective Agency Policy Management Authorities perform the following:

- Review periodic compliance audits to ensure that RAs and other components operated by the agency are operating in compliance with this WidePoint PIV SSP CPS; and
- Review name space control procedures to ensure that distinguished names are uniquely assigned within their agency.

9.6.1 CA Representations and Warranties

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

The WidePoint PIV SSP warrants that any RA, LRA, or designated authority will operate in accordance with the applicable sections of this WidePoint PIV SSP CPS.

Subscriber (applicant) Agencies warrant that:

- Procedures are implemented in accordance with the FPCPF and this WidePoint PIV SSP CPS.
- Sanctions are accomplished in accordance with this WidePoint PIV SSP CPS.
- Operate in accordance with the applicable sections of this WidePoint PIV SSP CPS.
- Meet the personnel and training requirements stipulated in this WidePoint PIV SSP CPS.
- Will cooperate and assist the WidePoint PIV SSP in monitoring and auditing that authorized staff members are operating in accordance with the applicable sections of this WidePoint PIV SSP CPS.
- Network security controls to the equipment are in accordance with the applicable sections of This WidePoint PIV SSP CPS.

9.6.2 KED Representations and Warranties

The WidePoint KED conforms to the stipulations of this document.

9.6.3 RA Representations and Warranties

WidePoint PIV SSP RAs are obligated to accurately represent the information prepared for the WidePoint PIV SSP and to process requests and responses in a timely and secure manner. WidePoint PIV SSP RAs may designate WidePoint PIV SSP LRAs; however, LRAs may not designate other WidePoint PIV SSP LRAs under this WidePoint PIV SSP CPS. A WidePoint PIV SSP RA that performs registration functions as described in this WidePoint PIV SSP CPS must comply with the stipulations of the FPCPF, and this WidePoint PIV SSP CPS, which has been approved by the FPKIPA for use. WidePoint PIV SSP RAs under this WidePoint PIV SSP CPS are not authorized to assume any other WidePoint PIV SSP administration functions.

A WidePoint PIV SSP RA supporting the WidePoint PIV SSP, and this WidePoint PIV SSP CPS, is obligated to conform to the stipulations of this document, including:

- Maintaining its operations in conformance to the stipulations of this WidePoint PIV SSP CPS.
- Including only valid and appropriate information in certificate requests, and maintaining evidence that due diligence was exercised in validating the information contained in the certificate.
- Confirming that issuance occurs no later than 30 days after verification of identity (as stipulated in section 4.2.3, “Time to Process Certificate Applications”).
- Ensuring that obligations are imposed on subscribers in accordance with Section 9.6.3, and that Subscribers are informed of the consequences of not complying with those obligations.

When validating subscriber requests for certificates issued under this WidePoint PIV SSP CPS, an RA accepts the following obligations:

- To validate the accuracy of all information contained in the subscriber’s certificate request.
- To validate that the named subscriber actually requested the certificate.
- To verify to the WidePoint PIV SSP RA that the certificate request originated from the named subscriber and that the information contained in the certificate request is accurate.
- To use the WidePoint PIV SSP RA certificate only for purposes associated with the WidePoint PIV SSP RA function.
- To use private keys only on the machines that are protected and managed using commercial best practices.
- To request revocation and verify reissue requirements of a subscriber’s certificate upon notification of changes to information contained in the certificate.
- To request revocation of the certificates of subscribers found to have acted in a manner counter to subscriber obligations.
- To inform subscribers and the WidePoint PIV SSP RA of any changes in the WidePoint PIV SSP RA’s status.
- To protect the WidePoint PIV SSP RA certificate private keys from unauthorized access.

- To immediately revoke his/her own RA certificate and report to the WidePoint PIV SSP RA if private key compromise is suspected.

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

9.6.4 SUBSCRIBER REPRESENTATIONS AND WARRANTIES

Each subscriber (or human PKI Sponsor for device certificates) obtaining a certificate from the WidePoint PIV SSP is required to sign (either digitally sign or wet signature) a document containing the requirements he/she must meet pertaining to the protection of the private key and use of the certificate, before being issued the certificate. Wherever possible, subscriber documents will be digitally signed.

When requesting and using a certificate issued under this WidePoint PIV SSP CPS, a subscriber (or human PKI Sponsor for device certificates) accepts the following obligations:

- To accurately represent themselves in all communications with the WidePoint PIV SSP .
- To protect the certificate private key from unauthorized access in accordance with Section 6.2, as stipulated in their certificate acceptance agreements, and local procedures.
- To immediately report to a WidePoint PIV SSP RA or LRA and request certificate revocation if private key compromise is suspected.
- To use the certificate only for authorized applications which have met the requirements of the Common Policy and this WidePoint PIV SSP CPS.
- To use the certificate only for the purpose for which it was issued, as indicated in the key usage extension.
- To use private keys only on the machines that are protected and managed using commercial best practices.
- To report any changes to information contained in the certificate to the appropriate WidePoint PIV SSP RA or LRA for certificate reissue processing.
- To determine whether revocation of the pubic key certificate associated with a recovered key is necessary, when notified that his or her escrowed key has been recovered. The Subscriber requests the revocation, if necessary.
- Abide by all the terms, conditions, and restrictions levied upon the use of their private keys and certificates.

These obligations are provided to the subscriber during the registration process in the form of a Subscriber Agreement that the subscriber must read and agree to prior to completing

registration. Theft, compromise or misuse of the private key may cause the subscriber, relying party and their organization legal consequences.

If the human PKI Sponsor for a device is not physically located near the sponsored device, and/or does not have sufficient administrative privileges on the sponsored device to protect the device's private key and ensure that the device's certificate is only used for authorized purposes, the device PKI Sponsor may delegate these responsibilities to an authorized administrator for the device. The delegation must be documented and signed by both the device PKI Sponsor and the authorized administrator for the device. Delegation does not relieve the device PKI Sponsor of his or her accountability for these responsibilities. In the case where a human PKI Sponsor changes, either the departing or new PKI Sponsor must notify the WidePoint PIV SSP via digitally signed email of the change, listing the status of each certificate under his/her sponsorship.

9.6.5 KRA Representations and Warranties

WidePoint SSP KRAs will comply with the following stipulations:

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

9.6.6 Requestor Representations and Warranties

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

- Requestors will protect Subscribers' recovered key(s) from compromise. Requestors must use a combination of computer security, cryptographic, network security,

physical security, personnel security, and procedural security controls to protect their keys and recovered Subscribers' keys.

- Third-party Requestors will destroy Subscribers' keys when no longer required (i.e., when the data has been recovered).
- Requestors will request and use the Subscriber's escrowed key(s) only to recover Subscriber's data they are authorized to access.
- Requestors will accurately represent themselves to all entities during any key recovery service.
- The Third-Party Requestor will protect information concerning each key recovery operation.
- The Third-Party Requestor will communicate information concerning the recovery to the Subscriber when appropriate as determined by the reason for the recovery. The decision to notify the Subscriber will be based on the law and the Issuing Organization's policies and procedures for third party information access.
- In the event that the Third-Party Requestor notifies the Subscriber of a key recovery, the Requestor will consult with the Subscriber to determine whether or not the recovery circumstances warrant revoking the associated public key certificate.
- As a condition of receiving a recovered key, a Requestor will sign an acknowledgement of agreement to follow the law and the Issuing Organization's policies relating to protection and release of the recovered key.
- Upon receipt of the recovered key(s), the Third-Party Requestor will sign[3] 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 *[Issuing Organization]* policies, applicable laws and Federal regulations concerning the protection of the recovered key and any data recovered using the key."

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

9.6.7 Relying Party Representations and Warranties

This WidePoint PIV SSP CPS does not specify the steps which a relying party should take to determine whether to rely upon a certificate. The relying party decides, pursuant to its own policies, what steps to take. The WidePoint PIV SSP merely provides the tools (i.e., certificates and CRLs) needed to perform the trust path creation and certificate validation which the relying party may wish to employ in its determination.

9.6.8 Repository Representations and Warranties

The WidePoint PIV SSP warrants that procedures are implemented in accordance with the FPCPF and this WidePoint PIV SSP CPS, and that any certificates issued that assert the certificate policy OIDs identified in Section 1.2 are issued in accordance with the stipulations of the FPCPF and this WidePoint PIV SSP CPS.

The WidePoint PIV SSP warrants that RAs or Trusted Agents operate in accordance with the applicable sections of the FPCPF and this WidePoint PIV SSP CPS.

The certificate repository meets the following obligations:

- To list all un-expired certificates for the WidePoint PIV SSP to relying parties.
- To contain an accurate and current CRL for the WidePoint PIV SSP for use by relying parties.
- To be publicly accessible through a web server gateway using HTTPS and FIPS 140-2 approved encryption.
- To be physically accessible, via certificate authenticated access control over SSL, for authorized requests coordinated with the WidePoint PIV SSP point of contact during normal business hours for the operating organization.
- To be maintained in accordance with the practices specified in this WidePoint PIV SSP CPS.
- To meet or exceed the requirement of 99% availability for all components within the control of the operating organization. NOTE: Communication failures as a result of Internet problems external to the operating organization will not count against this availability requirement.

The WidePoint PIV SSP maintains a copy of at least all certificates and CRLs it issues and provides this information to the US Government for archiving. The WidePoint PIV SSP provides this information on a certificate accessed web server posted no later than 10 days after the end of the collection of the data. If desired, the archive information can be delivered to the US Government on CDROM or other FPKIPA approved media.

9.7 DISCLAIMERS OF WARRANTIES

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

The WidePoint PIV SSP disclaims all warranties and obligations of any type other than those listed herein; in the Common Policy; or in the FPKI KRP.

9.8 LIMITATIONS OF LIABILITY

9.8.1 LOSS LIMITATION

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

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

9.8.2 U.S. FEDERAL GOVERNMENT LIABILITY

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

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

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

9.9 INDEMNITIES

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

9.10 TERM AND TERMINATION

9.10.1 TERM

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

9.10.2 TERMINATION

This WidePoint PIV SSP CPS will survive any termination of the WidePoint PIV SSP. The requirements of This WidePoint PIV SSP CPS remain in effect through the end of the archive period for the last certificate issued. Termination of the FPCPF is at the discretion of the FPKIPA.

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

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

Intellectual property rights will survive This WidePoint PIV SSP CPS, in accordance with the IP laws of the United States. The requirements of This WidePoint PIV SSP CPS remain in effect through the end of the archive period for the last certificate issued.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

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

Any planned changes to the WidePoint PIV SSP that has the potential to affect the FPKI operational environment shall be communicated to the FPKIPA 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 must be provided to the FPKIPA within 24 hours following implementation.

9.12 AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENT

The FPKIPA will review the FPCPF at least once every year. Corrections, updates, or changes to the FPCPF CP will be made publicly available either by posting a copy of the FPCPF CP or a link to the FPCPF CP's location on the WidePoint PIV SSP website.

WidePoint will update this WidePoint PIV SSP CPS is accordance with changes to the Common Policy. A redacted version of the WidePoint PIV SSP CPS will be made available via the WidePoint PIV SSP website.

9.12.2 NOTIFICATION MECHANISM AND PERIOD

WidePoint PIV SSP will publish information (including the currently approved CPS, with sensitive data redacted) on a web site.

9.12.3 CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED

The certificate policy OIDs will only change if the FPKIPA determines that a change in the FPCPF CP reduces the level of assurance provided.

9.13 DISPUTE RESOLUTION PROVISIONS

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

With respect to Subscriber or Relying Party Agreements or Obligations made by an entity by purchasing the services associated with this WidePoint PIV SSP CPS, disputes as to operational or policy issues will use the procedure set forth in the Shared Service Provider Roadmap.

9.14 GOVERNING LAW

The laws of the United States of America will govern the enforceability, construction, interpretation, and validity of This WidePoint PIV SSP CPS with respect to the Common Policy

9.15 COMPLIANCE WITH APPLICABLE LAW

Operation of the WidePoint PIV SSP CA(s) is required to comply with applicable law.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 ENTIRE AGREEMENT

None.

9.16.2 ASSIGNMENT

None.

9.16.3 SEVERABILITY

All contracts negotiated, for the purpose of providing WidePoint PIV SSP services under the FPCPF, will contain clauses that ensure continuity and stability of the WidePoint PIV SSP operation.

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

9.16.4 ENFORCEMENT (ATTORNEY'S FEES AND WAIVER OF RIGHTS)

Failure by any person to enforce a provision of this WidePoint PIV SSP CPS will not be deemed a waiver of future enforcement of that or any other provision.

9.16.5 FORCE MAJEURE

The WidePoint PIV SSP will not be responsible for any breach of warranty, delay, or failure in performance under this WidePoint PIV SSP CPS that results from events beyond its control including, but not limited to, acts of God, acts of war, epidemics, power outages, fire, earthquakes, and other disasters.

9.17 OTHER PROVISIONS

None.

10 BIBLIOGRAPHY

The following documents were used in part to either directly or indirectly develop This WidePoint PIV SSP CPS:

Common Name or Acronym	Information and Location
ABADSG	Digital Signature Guidelines, 1996-08-01. http://www.abanet.org/scitech/ec/isc/dsgfree.html.
AUDIT	FPKI Annual Review Requirements https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/annual-review-requirements.pdf
CIMC	Certificate Issuing and Management Components Family of Protection Profiles, version 1.0, October 31, 2001.
FIPS 140-2	Security Requirements for Cryptographic Modules May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
FIPS 186-2	Digital Signature Standard, January 27, 2000. http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf
FIPS 201	Personal Identity Verification (PIV) of Federal Employees and Contractors https://csrc.nist.gov/publications/detail/fips/201/2/final
FOIACT	5 U.S.C. 552, Freedom of Information Act. http://www4.law.cornell.edu/uscode/5/552.html
FPKI-Prof	Federal PKI X.509 Certificate and CRL Extensions Profile
ISO9594-8	Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 1997.
ITMRA	40 U.S.C. 1452, Information Technology Management Reform Act of 1996. http://www4.law.cornell.edu/uscode/40/1452.html
NAG69C	Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999.
NIST SP 800-73	Interfaces for Personal Identity Verification (4 Parts) http://csrc.nist.gov/publications/PubsSPs.html
NIST SP 800-76	Biometric Data Specification for Personal Identity Verification https://csrc.nist.gov/publications/detail/sp/800-76/2/final
NIST SP 800-78	Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV) http://csrc.nist.gov/publications/nistpubs/800-78-2/sp800-78-2.pdf

Common Name or Acronym	Information and Location
NIST SP 800-157	Guidelines for Derived Personal Identity Verification (PIV) Credentials http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf
NSD42	National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990. http://snyside.sunnyside.com/cpsr/privacy/computersecurity/nsd42.txt (redacted version)
NS4005	NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997.
NS4009	NSTISSI 4009, National Information Systems Security Glossary, January 1999.
PIV Profile	X.509 Certificate and CertificateRevocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program / Version 1.9 / May 9, 2018 Reference Link: https://www.idmanagement.gov/fpki/#certificate-policies
PKCS#12	Personal Information Exchange Syntax Standard, April 1997. ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf
RFC 2510	Certificate Management Protocol, Adams and Farrell, March 1999.
RFC 3647	Certificate Policy and Certification Practices Framework, Chokhani and Ford, Sabett, Merrill, and Wu, November 2003.
SSP 800-89	Recommendation for Obtaining Assurance for Digital Signature Applications, NIST Special Publication 800-89 http://csrc.nist.gov/publications/nistpubs/
SSP 800-56A	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, NIST Special Publication 800-56A http://csrc.nist.gov/publications/nistpubs/

11 ACRONYMS AND ABBREVIATIONS

AID	Application Identifier
CA	Certification Authority
CARL	Certificate Authority Revocation List
CCB	Configuration Control Board
CMS	Card Management System
COMSEC	Communications Security
CP	Certificate Policy; also Common Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Object Registry
DOD	Department of Defense
DN	Distinguished Name
DPCI	Derived PIV Credential Issuer
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ERC	Enhanced Reliability Check
FAR	Federal Acquisition Regulations
FBCA	Federal Bridge Certification Authority
FQDN	Fully Qualified Domain Name
FPCPF	U.S. Federal PKI Common Policy Framework
FPKI MA	Federal Public Key Infrastructure Management Authority
FED-STD	Federal Standard
FIPS PUB	(US) Federal Information Processing Standard Publication
FPKI	Federal Public Key Infrastructure
FPKI-E	Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile
FPKISC	Federal PKI Steering Committee

FPKIPA	Federal PKI Policy Authority
GPEA	Government Paperwork Elimination Act of 1998
GSA	General Services Administration
HTTP	HyperText Transfer Protocol
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector
ITU-TSS	International Telecommunications Union – Telecommunications System Sector
LDAP	Lightweight Directory Access Protocol
NII	National Information Infrastructure
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
POC	Point of Contact
RA	Registration Authority
RFC	Request For Comments

RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA-1	Secure Hash Algorithm, Version 1
S/MIME	Secure Multipurpose Internet Mail Extension
SNOC	Secure Network Operations Center
SSL	Secure Sockets Layer
TSDM	Trusted Software Development Methodology
UPN	User Principal Name
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
U.S.C.	United States Code
UUID	Universally Unique Identifier (defined by RFC 4122)
WWW	World Wide Web

12 GLOSSARY

Term	Definition
Access	Ability to make use of any information system (IS) resource. [NS4009]
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Affiliated Organization	Organizations that authorize affiliation with Subscribers of PIV certificates.
Applicant	The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]
Archive	Long-term, physically separate storage.
Attribute Authority	An entity, recognized by the FPKIPA or comparable Entity body as having the authority to verify the association of attributes to an identity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of

	information. [NS4009]
Backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
Binding	Process of associating two related elements of information. [NS4009]
Biometric	A physical or behavioral characteristic of a human being.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]. As used in this WidePoint PIV SSP CPS, the term “Certificate” refers to certificates that expressly reference the OID(s) of this WidePoint PIV SSP CPS in the “Certificate Policies” field of an X.509 v.3 certificate.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs.
Certification Authority Revocation List (CARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates, that have been revoked.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.
Certification Authority Software	Key Management and cryptographic software used to manage certificates issued to subscribers.
Certificate Policy (CP)	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

Certification 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).
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 that it has issued that are revoked prior to their stated expiration date.
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
Client (application)	A system entity, usually a computer process acting on behalf of a human user that makes use of a service provided by a server.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by the National Institute of Standards and Technology.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
Cross-Certificate	A certificate used to establish a trust relationship between two Certification Authorities.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]
Crypto period	Time span during which each key setting remains in effect. [NS4009]
Data Integrity	Assurance that the data are unchanged from creation to reception.

Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.
Dual Use Certificate	A certificate that is intended for use with both digital signature and data encryption services.
Duration	A field within a certificate which is composed of two subfields; "date of issue" and "date of next issue".
E-commerce	The use of network technology (especially the internet) to buy or sell goods and services.
Encrypted Network	A network that is protected from outside access by NSA-approved high-grade (Type I) cryptography. Examples are SIPRNET and TOP SECRET networks.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
End-entity	Relying Parties and Subscribers
Entity	For the purposes of this document, "Entity" refers to an organization, corporation, community of interest, or government agency with operational control of a CA.
Entity CA	A CA that acts on behalf of an Entity, and is under the operational control of an Entity. The Entity may be an organization, corporation, or community of interest. For the Federal Government, an Entity may be any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Federal Government.
FBCA Management Authority (FPKI MA)	The Federal Public Key Infrastructure Management Authority is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the Federal Bridge Certification Authority.
Federal Public Key Infrastructure Policy Authority (FPKI PA)	The FPKIPA is a federal government body responsible for setting, implementing, and administering policy decisions regarding inter-Entity PKI interoperability that uses the FBCA.
Firewall	Gateway that limits access between networks in accordance with

	local security policy. [NS4009]
High Assurance Guard (HAG)	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.
Information System Security Officer (ISSO)	Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, from design through disposal. [NS4009]
Inside threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]
Key Exchange	The process of exchanging public keys in order to establish secure communications.
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Key Pair	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.
Key Recovery Policy (KRP)	A key recovery policy is a specialized form of administrative policy tuned to the protection and recovery of key management private keys (i.e. decryption keys) held in escrow. A key recovery policy addresses all aspects associated with the storage and recovery of

	key management certificates.
Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community.
Mission Support Information	Information that is important to the support of deployed and contingency forces.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
Naming Authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
National Security System	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI they are used to uniquely identify each of the 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 WidePoint PIV SSP CPS.
Policy Management Authority (PMA)	Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies. For the FBCA, the PMA is the FPKIPA.
Principal CA	The Principal CA is a CA designated by an Entity to interoperate with the FBCA. An Entity may designate multiple Principal CAs to interoperate with the FBCA.
Privacy	Restricting access to Subscriber or Relying Party information in accordance with Federal law and Entity policy.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.
Relying Party	A person or Entity who has received information that includes a certificate and a digital signature verifiable with reference to a

	public key listed in the certificate, and is in a position to rely on them.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A database containing information and data relating to certificates as specified in This WidePoint PIV SSP CPS; may also be referred to as a directory.
Responsible Individual	A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Server	A system entity that provides a service in response to requests from clients.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).
Subscriber	A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device.
Superior CA	In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).
System Equipment	A comprehensive accounting of all system hardware and software

Configuration	types and settings.
System High	The highest security level supported by an information system. [NS4009]
Technical non-repudiation	The contribution public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
Trust List	Collection of trusted certificates used by Relying Parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of an Entity in confirming Subscriber identification during the registration process. Trusted Agents do not have automated 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. [NS4009]
Update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.