DigiCert Non-Federal Shared Service Provider PKI

Certification Practice Statement

Version 2.3

April 30, 2020

DigiCert, Inc.
2801 N. Thanksgiving Way
Suite 500
Lehi, UT 84043
USA
Tel: 1-801-877-2100
Fax: 1-801-705-0481
www.digicert.com

DigiCert Non-Federal Shared Service Provider (SSP) Certification Practice Statement

Revision Date: [April 30, 2020]

Important – Acquisition Notice

On October 31, 2017, DigiCert, Inc completed the acquisition of Symantec Corporation's Website Security business unit. As a result, DigiCert is now the registered owner of this CPS document and the PKI Services described within this document.

However, a hybrid of references to both "VeriSign" and "Symantec" and "DigiCert" shall be evident within this document for a period of time until it is operationally practical to complete the re-branding of the Certification Authorities and services. Any references to VeriSign or Symantec as a corporate entity should be strictly considered to be legacy language that solely reflects the history of ownership.

Trademark Notices

DigiCert, Inc.
2801 N. Thanksgiving Way
Suite 500
Lehi, UT 84043
USA
Tel: 1-801-877-2100
Fax: 1-801-705-0481
www.digicert.com
Email: support@digicert.com

TABLE OF CONTENTS

1. INTRODUCTION

Many non-Federal entities, including state and local government agencies and government contractors, have a need for a PKI service that operates at multiple assurance levels and is interoperable with the Federal Government. Many also have a requirement for a smart card token interoperable with the PIV card defined under FIPS 201-2 (referred to as a PIV-interoperable (PIV-I) card). For example, the US Department of Homeland Security is requiring non-Federal first responder organizations to use a PIV-interoperable card. The Non-Federal SSP PKI operates at multiple assurance levels defined by Federal policy and achieve interoperability with the Federal PKI through cross-certification with the Federal Bridge Certification Authority (FBCA).

The intent of PIV-I is to enable issuers to issue cards that are technically interoperable with Federal PIV Card readers and applications, and that may be trusted for particular purposes through a decision of the relying Federal Agency. Reliance on PIV-I Cards is based on compliance with technical specifications and specific trust elements of a PIV-I Card[1] as specified in this CPS.

This Non-Federal SSP PKI Certification Practice Statement (CPS) in conjunction with the DigiCert Certificate Policy for Symantec Trust Network and the Federal Bridge CA Certificate Policy defines the practices that DigiCert will employ in issuing and managing certificates and in maintaining a certificate-based SSP PKI for Non-Federal entities.

Note: all subsequent references to 'SSP' PKI in this document refer to the Non-Federal SSP PKI that DigiCert acquired from Symantec.

1.1 Overview

The Non-Federal SSP PKI service offering provides complete certificate life-cycle support and certificate repository services for non-Federal entities. The Non-Federal SSP PKI operates in the framework and under the DigiCert Certificate Policy for Symantec Trust Network. The architecture and functional solution for the Non-Federal SSP PKI is based on DigiCert's managed PKI service offering, which has been deployed at numerous government agencies, and has previously been approved for cross-certification with the FBCA.

The Non-Federal SSP PKI operates multiple assurance levels defined by the FBCA Certificate Policy:

- Rudimentary Assurance; Little or no confidence in the asserted identity's validity
- Basic Assurance; Some confidence in the asserted identity's validity
- Medium Assurance; Confidence in the asserted identity's validity in a moderate risk environment.
- PIV-I Card Authentication Assurance; Confidence in the asserted identity's validity in a moderate risk environment where use of an activation pin is not practical.
- Medium Hardware, PIV-I Hardware and PIV-I Content Signing; High confidence in the asserted identity's validity.
- Two device certificate policies at the Medium Assurance level are defined to facilitate server to server authentication between FPKI and other PKI domains.

The Non-Federal SSP PKI primary location is at a data center located in [Text Removed]. A disaster recovery site with full backup and data mirroring at the disaster recovery facility in [Text Removed]. All customer transactions are copied between the primary and disaster recovery systems in real-time over a secure VPN connection.

[1] The PIV-I Card requirements rely heavily on relevant specifications from the National Institute of Standards and Technology (NIST).

Authorized DigiCert personnel will perform the CA functions as described in this CPS. The RA functions, including control over the registration process and in-person identity proofing will be performed by government agencies or companies that purchase the Non-Federal SSP PKI services.

End-entities supported by the Non-Federal SSP PKI include, but are not limited to, State/Local employees, contractors and affiliates. The Non-Federal SSP PKI will issue X.509 Version 3 certificates compliant with the certificate profiles listed in Appendix A of this CPS. The certificates can be used by the subscribers and relying parties for both physical and logical access including use in a variety of applications such as secure electronic mail, signature of electronic forms and contract documents, secure document exchange, and secure web access and transmission.

1.1.1 Certification Practices Statement (CPS)

This CPS is the statement of practices that are employed when issuing digital certificates from the DigiCert Non-Federal SSP PKI. This CPS is structured in accordance with RFC 3647 of the Internet Engineering Task Force (IETF).

This CPS describes the practices for the creation and management of X.509 Version 3 public-key certificates for use in applications requiring communication between networked computer-based systems used by non-Federal entities which meets Federal information assurance levels and is cross certified with the FBCA to enable interoperability with Federal entities. These applications include but are not limited to: electronic mail; transmission of unclassified information; signature of electronic forms; contract formation signatures; and authentication of infrastructure components such as web servers, firewall and directories. The intended network for these network security applications is the Internet. This CPS describes the rights and obligations of persons and entities authorized under this CPS and the CP to fulfill any of the following roles: Certification Authority, Registration Authority, Trusted Agent, Repository, and the end-entity roles of Subscriber and Relying Party.

This Non-Federal SSP CPS defines the policies and procedures that will be followed for the creation and management of X.509 Version 3 public-key certificates for use in applications requiring communication between networked computer-based systems used by non-Federal entities which meets Federal information assurance levels and is cross certified with the FBCA to enable interoperability with Federal entities. These applications include but are not limited to: electronic mail; transmission of unclassified information; signature of electronic forms; contract formation signatures; and authentication of infrastructure components such as web servers, firewall and directories. The intended network for these network security applications is the Internet.

1.2 Document Name and Identification

This CPS describes the practices for Non-Federal SSP PKI services delivered in accordance with the DigiCert Certificate Policy for Symantec Trust Network. This CPS identifies distinct certificate policies for Non-Federal SSP PKI users and devices within the Symantec Trust Network Classes 1, 2 and 3. The Non-Federal SSP PKI Policy Object Identifiers are subordinate to the Symantec Trust Network (STN) Policy Object Identifiers as shown below:

STN Policy Object Identifiers	Non-Federal SSP PKI Policy Object Identifiers:
2.16.840.1.113733.1.7.23.1 STN Class 1	2.16.840.1.113733.1.7.23.1.1.2 SSP Rudimentary
2.16.840.1.113733.1.7.23.2 STN Class 2	2.16.840.1.113733.1.7.23.2.1.2 SSP Basic
2.16.840.1.113733.1.7.23.3 STN Class 3	2.16.840.1.113733.1.7.23.3.1.6 SSP Medium 2.16.840.1.113733.1.7.23.3.1.7 SSP MediumHardware 2.16.840.1.113733.1.7.23.3.1.8 SSP mediumDevices 2.16.840.1.113733.1.7.23.3.1.36 SSP mediumDevicesHardware

	2.16.840.1.113733.1.7.23.3.1.13 SSP Auth (no longer issued, found in legacy certificates only) 2.16.840.1.113733.1.7.23.3.1.14 SSP Medium CBP 2.16.840.1.113733.1.7.23.3.1.15 SSP MediumHardware CBP 2.16.840.1.113733.1.7.23.3.1.17 SSP PIV-I cardAuth 2.16.840.1.113733.1.7.23.3.1.18 SSP PIV-I Hardware 2.16.840.1.113733.1.7.23.3.1.20 SSP PIV-I contentSigning

Certificates issued by the Non-Federal SSP PKI service will assert at least one of the following Policy Object Identifiers:

- *id-stn-ssp-rudimentary* ::= {2 16 840 1 113733 1 7 23 1 1 2}

  Maps to FBCA rudimentaryAssurance. For users with software cryptographic modules. Uses: email address authentication, email encryption.

- *id-stn-ssp-basic* ::= {2 16 840 1 113733 1 7 23 2 1 2}

  Maps to FBCA basicAssurance. For users with software cryptographic modules. Uses: low risk activities related to digital signature, client authentication, and encryption.

- *id-stn-ssp-medium* ::= {2 16 840 1 113733 1 7 23 3 1 6}

  Maps to FBCA mediumAssurance. For users with software cryptographic modules. Uses: digital signature, client authentication, encryption. Mutually exclusive of id-stn-ssp-mediumHardware.

- *id-stn-ssp-medium-CBP* ::= {2 16 840 1 113733 1 7 23 3 1 14}

  Maps to FBCA medium-CBP. Identical to requirements defined for the *id-stn-ssp-medium* with the exception of the citizenship requirements in section 5.3.1.

- *id-stn-ssp-mediumHardware* ::= {2 16 840 1 113733 1 23 3 1 7}

  Maps to FBCA mediumHardware. For users with hardware cryptographic modules (e.g., smart card). Uses: digital signature, client authentication, encryption. Mutually exclusive of id-stn-ssp-medium.

- *id-stn-ssp-mediumHardware-CBP* ::= {2 16 840 1 113733 1 23 3 1 15}

  Maps to FBCA mediumHardware-CBP. Identical to requirements defined for the *id-stn-ssp-mediumHardware* with the exception of the citizenship requirements in section 5.3.1.

- *id-stn-ssp-mediumDevices* ::= {2 16 840 1 113733 1 7 23 7 3 1 8}

  For devices (non-person entity) only; requires a human sponsor. Uses: device authentication, encryption.

- *id-stn-ssp-mediumDevicesHardware* ::= {2 16 840 1 113733 1 7 23 7 3 1 36}

  For devices (non-person entity) only; requires a human sponsor. Uses: device authentication, encryption.

- *id-stn-ssp-authentication* ::= {2 16 840 1 113733 1 7 23 3 1 13} (no longer issued, found in legacy certificates only)

  For user authentication only, no digital signature capability (comparable to PIV authentication with pivFASC-N name type). Uses: client authentication for physical access after private key activation; requires OCSP services. Note: a certificate asserting this policy OID is referred to as PIV-interoperable Authentication certificate.

- *id-stn-ssp-pivi-cardAuth* ::= {2 16 840 1 113733 1 7 23 3 1 17}

  Maps to *FBCA pivi-cardAuth*. For users with PIV-I cards as defined in section 6.2.1. Uses: client authentication for physical access (no digital signature capability) – private key can be used without subscriber activation; requires OCSP services.

- *id-stn-ssp-pivi-hardware* [2]::= {2 16 840 1 113733 1 7 23 3 1 18}

  Maps to *FBCA pivi-hardware*. For users with PIV-I cards as defined in section 6.2.1. Uses: digital signature, client authentication, encryption; requires OCSP services. Requirements associated with PIV-I Hardware are identical to Medium Hardware except where specifically noted in the text and further described in Appendix C.

- *id-stn-ssp-pivi-contentSigning* ::= {2 16 840 1 113733 1 7 23 3 1 20}

  Maps to *FBCA pivi-contentSigning*. Certificates are held on PIV-I cards as defined in section 6.2.1. Uses: exclusively for signing content on PIV-I certificates such as the card security objects by the Card Management System (CMS). Requirements associated with PIV-I Content Signing are identical to Medium Hardware except where specifically noted in the text and further described in Appendix C.

Certificates issued from a Non-Federal SSP CA may contain any or all of these OIDs. Certificates issued to users to support digitally signed documents or key management may contain the *id-stn-ssp-basic*, *id-stn-ssp-medium*, *id-stn-ssp-mediumHardware* or *id-stn-ssp-pivi-hardware*. Certificates issued to users supporting authentication but not digital signature may contain *id-stn-ssp-pivi-cardAuth* or *id-stn-ssp-pivi-hardware.* Certificates issued to users supporting authentication where the private key can be used without user activation shall contain *id-stn-ssp-pivi-cardAuth*.

The requirements associated with the *id-stn-ssp-mediumDevices* and *id-stn-ssp-mediumDevicesHardware* policies are identical to those defined for the Medium and Medium Hardware policies with the exception of identity proofing, re-key and activation data. The use of the *id-stn-ssp-mediumDevices* and *id-stn-ssp-mediumDevicesHardware* policies are restricted to devices and systems (ie, non-person entities).

End-Entity certificates issued to devices after January 15, 2017 shall assert the *id-stn-ssp-mediumDevices, id-stn-ssp-mediumDevicesHardware,* or *id-stn-ssp-pivi-contentSigning* policy. All other policies defined in this document should be reserved for human subscribers when used in End-Entity certificates.

Policy Object Identifiers are populated in accordance with CPS § 7.1.6.

1.3 PKI Participants

1.3.1 PKI Authorities

1.3.1.1 Federal PKI Policy Authority (FPKIPA)

The Federal PKI PA, a group of U.S. Federal government Agencies chartered by the Federal CIO Council, is responsible for authorizing an entity to interoperate using the FBCA and ensures continued conformance of that entity as a condition for allowing continued interoperability using the FBCA.

1.3.1.2 DigiCert Policy Authority

The DigiCert Policy Authority (DCPA) is responsible for maintaining the CP, approving the CPS and Compliance Audit for each CA that issues certificates under the CP. The DigiCert PA is a management body responsible for maintaining this CPS and for ensuring that all SSP PKI components (e.g., CAs, CSSs, CMSs, RAs) are operated in compliance with this CPS and the FBCA CP regardless of by whom the PKI component is managed and operated. The DCPA is responsible for notifying the FPKIPA of any change to the infrastructure that has the potential to affect the FPKI operational environment at least two weeks prior to implementation; all new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the change are provided to the FPKIPA within 24 hours following implementation.

[2] The *id-stn-ssp-pivi-hardware* assurance level includes three certificate types: Non-Federal SSP PIV-I Authentication, SSP PIV-I Digital Signature and Non-Federal SSP PIV-I Key Management, which are individually defined with certificate profiles in Appendix A.

1.3.1.3 Organization Policy Management Authority

Organizations that contract for Non-Federal SSP PKI services under this CPS shall establish a management body to manage any organization components (e.g., RAs or repositories) and resolve name space collisions. (see Section 3.1.6). This body shall be referred to as an Organization Policy Management Authority, or Organization PMA.

An Organization PMA is responsible for ensuring that all organization-operated PKI components (e.g., CMSs and RAs) are operated in compliance with this CPS and the FBCA Policy and shall serve as the liaison for that organization to the DCPA. The Organization PMA shall be responsible for notifying the DCPA of any change to the infrastructure that has the potential to affect the NFI SSP 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 DCPA within 24 hours following implementation.

1.3.1.4 Certification Authority (CA)

The Non-Federal SSP PKI is a complex PKI with three segments each chaining to a different DigiCert Trust Network Root CA. The Class 1 Intermediate CA is for issuing FBCA Rudimentary Assurance certificates; The Class 2 Intermediate CA is for issuing FBCA Basic Assurance certificates; and the Class 3 Intermediate CA is for issuing Medium and Medium-Hardware certificates.

DigiCert Root CAs serve as the "trust anchors" for all certificates issued by the DigiCert Non-Federal SSP PKI. The Non-Federal SSP Intermediate CAs create a partition in the DigiCert Trust Network for organizations that meet the requirements of the DigiCert Non-Federal SSP CPS.

The Non-Federal SSP Intermediate CAs issue certificates to SSP CAs hosted and operated by DigiCert on behalf of organizations such as government agencies, contractors, universities and other Non-Federal entities. Each of the Non-Federal SSP Intermediate CAs will be cross-certified with the Federal Bridge Certification Authority CA at the appropriate assurance levels. Non-Federal SSP CAs are entities authorized by the DCPA to create, sign and issue end-entity digital certificates that conform to the requirements of the CP and this CPS. DigiCert verifies that any CA under its PKI have only one trust path to the FBCA (regardless of path validation results).

Note: No other PKI services provided by the Symantec Trust Network are permitted in the Non-Federal SSP PKI hierarchy.

Organizations may have a dedicated SSP CA or use a shared SSP CA.
The Non-Federal SSP CA is responsible for all aspects of the issuance and management of SSP certificates including the certificate management process, publication of certificates, revocation of certificates and re-key; generation and destruction of CA signing keys, and for ensuring that all aspects of the CA services, operations and infrastructure related to Non-Federal SSP certificates are performed in accordance with the requirements, representations, and warranties of this CPS.

1.3.1.5 Certificate Status Authority/Certificate Status Server

The SSP provides online status information using OCSP as described in sections 4.9.9 and 4.9.10.

1.3.2 Registration

1.3.2.1 Registration Authority (RA)

DigiCert personnel and designated non-Federal organization personnel will perform the RA functions for the Non-Federal SSP PKI. The RA may rely on an in-person identity validation process performed by a Trusted Agent. DigiCert will establish a contractual relationship with an organization prior to the authorization of a Registration Authority or Trusted Agent to perform identity verification of employees/affiliates of the organization. RAs and Trusted Agents will be bound by contract to comply with the requirements of the CP and this CPS.

RA personnel will be issued administrator certificates to enable secure authenticated access to their organization's Non-Federal SSP CA. The RA certificate is stored on a FIPS 140 Level 2 hardware token. Persons holding roles on the PIV-I CMS will be issued a PIV-I Authentication certificate on a PIV-I smartcard to authenticate to the CMS. A cryptographic module, FIPS 140 Level 2 and above, will be issued through the CMS operating system a PIV-I Content signing certificate to perform the signing functions on the PIV-I cards being issued.

In conjunction with a CMS, the RA role may be separated into multiple functions including sponsor, registrar, issuer, etc. for the purpose of completing all RA procedures.

1.3.2.2 Trusted Agent

A Trusted Agent is a person who satisfies all the trustworthiness requirements for an RA and who performs identity proofing as a proxy for the RA. Authorized employees of DigiCert or SSP CAs may also serve as Trusted Agents. Trusted Agents are holders of SSP subscriber certificates, but they do not have privileged access to SSP functions. A Trusted Agent is responsible for validating a subscriber's identity based on the presentation of a government-issued photo ID and other identity documents. A Trusted Agent is not considered a Trusted Role as defined by

1.3.3 Card Management System (CMS)

The CMS is responsible for managing smart card token content and in the context of this CPS, the CMS is responsible for the PIV-I policies. The PIV-I CMS shall meet the requirements described throughout this CPS, and specifically in Appendix B and Appendix C.

The CMS is issued administrator certificates to enable secure authenticated access to their organization's Non-Federal SSP CA. The CMS has an additional cryptographic module, FIPS 140 Level 2 and higher, that is issued a PIV-I certificate that expresses the PIV-I Content Signing policy OID only and shall not be issued certificates that express the PIV-I Hardware or PIV-I Card Authentication.

1.3.4 Subscribers

A SSP PKI Subscriber is an entity whose name appears as the subject in a SSP certificate, and who asserts that it uses its key and certificate in accordance with this CPS. Subscribers include State and Local government employees, contractors and affiliated personnel, workstations, firewalls, routers, trusted servers (e.g., database, FTP, and WWW), and other infrastructure components. Certificates for these components must be issued to a human sponsor who accepts the certificate and is responsible for carrying out Subscriber duties and the correct protection and use of the associated private key.

Although a SSP CA is a subscriber, the term Subscriber as used in this document refers only to those who request certificates for uses other than signing and issuing certificates.

1.3.5 Affiliated Organization

Subscriber certificates may be issued in conjunction with an organization that has a relationship with the subscriber, referred to as an Affiliated Organization. The Affiliated Organization is identified in the subscriber certificate DN. The Affiliated Organization is responsible for verifying the affiliation at the time of certificate application and for requesting revocation of the certificate if the affiliation is no longer valid.

1.3.6 Relying Parties

A relying party is the entity that relies on the validity of the binding of the subscriber's name to a public key. The relying party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The relying party can use the certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate. A relying party may use information in the certificate (such as CP identifiers) to determine the suitability of the certificate for a particular use. For this CPS, the relying party may be any entity that wishes to validate the binding of a public key to the name of a State/Local government employee, contractor, or other affiliated personnel.

1.3.7 Other Related Participants

1.3.7.1 Compliance Auditor

DigiCert retains the services of an independent security auditing firm, which conducts a yearly examination of the controls associated with DigiCert's operations as set forth in DigiCert's practices documentation. The audit is performed in accordance with standards established by the American Institute of Certified Public Accounts (AICPA) as defined in the Service Organization Control (SOC) reporting framework and the WebTrust for CA guidelines. As such, the yearly independent SOC 2 and WebTrust for CA audits provide the assurance of DigiCert's compliance with this CPS.

1.3.7.2 Repository

DigiCert will operate a Repository from its secure data facility [Text Removed]. This repository contains SSP subscriber certificates, Certificate Revocation Lists (CRLs) and the SSP CA certificates and associated CRLs. Updates to information contained in the DigiCert Repository shall be controlled via certificate-based access over SSL/TLS and shall be limited to authorized DigiCert personnel and processes. Subscribers and relying parties may query, view, and download CA certificates and CRL entries in the repository via an http query.

1.4 Certificate Usage

The sensitivity of the information processed or protected using certificates issued by the CA 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 CPS.

1.4.1 Appropriate Certificate Uses

This CPS is intended to support the use of validated public keys to access government and commercial 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 CPS may also be used for key establishment. This CPS is intended to support applications involving unclassified information, which can include sensitive unclassified data protected pursuant to federal statutes and regulations.

Non-Federal SSP CAs are intended to meet the authentication level requirements defined as follows.

- Credentials issued under *id-stn-ssp-rudimentary* provide the lowest degree of assurance in the identity of the individual and are intended for use in environments were the risk of malicious activity is low.
- Credentials issued under *id-stn-ssp-basic* provide a basic level of assurance in identity and are intended for use in environments where the consequences of data compromise are not considered significant.
- Credentials issued under *id-stn-ssp-medium* are intended for use in environments where the consequences of the failure of security services are considered moderate.
- Credentials issued under *id-stn-ssp-pivi-cardAuth* are intended for use in environments where the consequences of the failure of security services are considered moderate and the use of an activation pin is not practical.
- Credentials issued under *id-stn-ssp-mediumHardware* and *id-stn-ssp-pivi-hardware* are intended for use in environments where the consequences of the failure of security services are considered high.
- Credentials issued under *id-stn-ssp-pivi-contentSigning* are reserved for the cryptographic module used with the Card Management System (CMS) for use in signing PIV-I card security objects.

1.4.2 Prohibited Certificate Uses

Certificates shall be used only to the extent the use is consistent with applicable law, and in particular shall be used only to the extent permitted by applicable export or import laws.

Certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage.

CA Certificates may not be used for any functions except CA functions. In addition, end-user Subscriber Certificates shall not be used as CA Certificates.

The SSP and its Participants do not issue any certificate that can be used for man-in-the-middle (MITM) or traffic management of domain names or IP addresses that the certificate holder does not legitimately own or control. Such certificate usage is expressly prohibited.

DigiCert periodically rekeys Intermediate CAs. Third party applications or platforms that have an Intermediate CA embedded as a root certificate may not operate as designed after the Intermediate CA has been rekeyed. DigiCert therefore does not warrant the use of Intermediate CAs as root certificates and recommends that Intermediate CAs not be embedded into applications and/or platforms as root certificates. DigiCert recommends the use of Primary Certificate Authority (PCA) Roots as root certificates.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CPS and the documents referenced herein are maintained by the DigiCert Policy Authority (DCPA), which can be contacted at:

DigiCert Policy Authority
Suite 500
2801 N. Thanksgiving Way
Lehi, UT 84043 USA
Tel: 1-801-701-9600
Fax: 1-801-705-0481
www.digicert.com
support@digicert.com

1.5.2 Contact Person

Parties having questions as to the content, applicability, or interpretation of this CPS may address their comments to: support@digicert.com.

1.5.3 Person Determining CPS Suitability for the Policy

The DigiCert Policy Authority (DCPA) determines the suitability of the DigiCert Non-Federal SSP CPS and asserts its compliance with the DigiCert Certificate Policy for the Symantec Trust Network based upon an independent compliance auditor's results as set forth in section 8. The Federal PKI Policy Authority determines the suitability for compliance with the Federal Bridge Certificate Policy.

1.5.4 CPS Approval Procedures

The DCPA is the first approval authority of any proposed changes to this CPS. The Non-Federal SSP CA and RA shall meet all of the requirements of the approved Non-Federal SSP CPS before commencing operations.

The FPKIPA is the final approval authority of any proposed changes to this CPS..

This CPS and corresponding compliance audit are submitted to the FPKIPA for approval.

1.6 Definitions and Acronyms

See sections 11 and 12 for definitions and acronyms.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

End users may search the SSP Repository for SSP certificates or CRLs using HTTP queries.

2.1.1 Repository Obligations

The SSP Repository is obligated to provide certificates, CRLs, and other revocation information. No confidential subscriber data not intended for public dissemination is published in the SSP Repository. Therefore, the SSP Repository provides unrestricted read-only access to subscribers, relying parties, and other interested parties. The SSP repository is accessible via methods described in Section 2.1.

DigiCert may replicate certificates and CRLs in additional repositories for performance enhancement. Such repositories may be operated by DigiCert or other parties.

2.2 Publication of Certification Information

2.2.1 Publication of Certificates and Certificate Status

CA and End Entity certificates contain only valid Uniform Resource Identifiers (URIs) that are accessible by relying parties. The SSP operates an online Repository available to Subscribers and Relying Parties. The SSP Repository shall maintain an availability of at least 99.5% per year for all components within its control.

This Repository will contain or provide access to the following minimum certificate and certificate status information:

1. All CA certificates issued by or to the SSP CA;
2. All valid and un-expired SSP Certificates, except for Certificates that contain the UUID in the subject alternative name extension such as PIV-I Authentication certificates and Card Authentication certificates;
3. Certificate status information, including revocation;
4. The most recently issued CRL;
5. SSP CA certificate(s) needed to validate the signature on SSP subscriber certificates; and
6. Any other relevant information the SSP considers relevant regarding the use of SSP certificates by its subscribers or relying parties.

2.2.2 Publication of CA Information

The DigiCert document repository at https://www.digicert.com/legal-repository provides access to a copy of the DigiCert Certificate Policy for Symantec Trust Network Certificate Policy and a redacted version of this CPS including at least the following topics:

- Section 1.4, SSP Contact Information;
- Section 3.1, Initial Registration;
- Section 4.9, Certificate Suspension and Revocation;
- Section 9, Business and Legal Matters;
- Section 9.12, Certificate Policy Administration; and
- Any additional information that the SSP deems to be of interest to the relying parties (e.g., mechanisms to disseminate SSP trust anchor, to provide notification of revocation of Federal Bridge CA root or SSP certificate).

Applicable updates to this CPS that affect Subscribers and relying parties will be posted on the DigiCert document repository as described in section 9.12.2.

2.2.3 Interoperability

See section 2.1.

2.3 Time or Frequency of Publication

All information to be published in the repository shall be published promptly after such information is available.

Upon the subscriber's acceptance of the certificate, the SSP CA shall immediately change the status of the certificate in the SSP Repository from pending to valid.

Upon revoking a certificate, the SSP CA shall immediately change the status of the certificate indicated in the SSP Repository from valid to revoked.

CRLs will be created and published as described in Section 4.9.7.

2.4 Access Controls on Repositories

The SSP shall not impose any read access restrictions to public information published in its repository. Subscribers and relying parties may access certificate and CRL information via HTTP queries.

The SSP shall protect any data in the repository (or data otherwise maintained by the SSP) that is not intended for public dissemination or modification.

Updates to information contained in the SSP repository shall be controlled via certificate-based access over SSL and shall be limited to authorized DigiCert personnel.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

Certificates issued by the DigiCert shall have a non-null subject DN name. These distinguished names shall be in the form of an X.501 distinguished name specifying a geo-political name. Certificates issued at the Rudimentary level of assurance may include a null subject DN if they include at least one alternative name form. Certificates at all levels of assurance may include alternative name forms.

All X.501 distinguished names assigned to subscribers shall be in the following directory information tree (*Base DN)*:

Base DN: C=US, o=[organization], [ou=department], [ou=agency] optional

The organizational unit, department and agency appear when applicable and are used to specify the entity that employs the subscriber. When this occurs, a least one organizational unit appears in the DN. Normally the organizational unit agency will only be applicable for State/Local government agencies.

Non-PIV-I Certificates
The distinguished name of the subscriber will take one of the four following forms:

- C=US, o=[organization], [ou=department], [ou=agency] optional, cn=nickname lastname
- C=US, o=[organization], [ou=department], [ou=agency] optional, cn=firstname initial. lastname
- C=US, o=[organization], [ou=department], [ou=agency] optional, cn=firstname middlename lastname
- C=US, o=[organization], [ou=department], [ou=agency] optional, cn=firstname middlename lastname, dnQualifier=integer

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. In the last form, dnQualifier is an integer value that may be added to any name, primarily used to ensure name uniqueness.

X.501 distinguished names assigned by Affiliated Organizations shall be within the same directory information tree. The distinguished name of the affiliated Subscribers will take one of the four following forms:

- C=US, o=[organization], [ou=department], [ou=agency] optional, cn=nickname lastname (affiliate)
- C=US, o=[organization], [ou=department], [ou=agency] optional, cn=firstname initial. lastname (affiliate)
- C=US, o=[organization], [ou=department], [ou=agency] optional, cn=firstname middlename lastname (affiliate)
- C=US, o=[organization], [ou=department], [ou=agency] optional, cn=firstname middlename lastname (affiliate), dnQualifier=integer

Certificates issued under *id-stn-ssp-basic*, *id-stn-ssp-medium*, or *id-stn-ssp-mediumHardware* shall include a non-null subject name field. The subject alternative name field may be used if marked non-critical.

Certificates issued under *id-stn-ssp-rudimentary* may either follow the *id-stn-ssp-basic* rules or may have a null subject name field if the subject alternative name field is populated and marked critical.

Devices that are the subject of certificates issued under *id-stn-ssp-mediumDevices* and *id-stn-ssp-mediumDevicesHardware* shall be assigned a geo-political name. Device names shall take the following form:

C=US, o=[organization], [ou=department], [ou=agency], cn=device name

where 'device name' is a descriptive name for the device. Where a device is fully described by the Internet domain name, the common name attribute is optional.

DigiCert SSP certificates may assert an alternate name form in the *subjectAltName* field.

PIV-I Certificates

X.501 distinguished names assigned to subscribers shall be in the same directory tree and affiliated persons shall be within a subordinate directory information tree. The distinguished name of the subscribers will take one of the following forms.

Certificates issued under *id-stn-ssp-pivi-hardware*:

- Affiliated: {*Base DN*}, ou=[*Affiliated Organization Name*], cn=Subscriber's full name
- Unaffiliated: {*Base DN*}, ou=[*Entity CA's Name*], ou=Unaffiliated, cn=Subscriber's full name

Where Subscriber's full name can take one of the following forms, and use of these forms shall be as described for non-PIV-I certificates:

  - nickname lastname
  - firstname initial. lastname
  - firstname middlename lastname
  - firstname middlename lastname, dnQualifier=integer

The PIV-I Authentication certificate shall include a non-null (UUID required, others also allowed) *subjectName* and *subjectAltName* value.

- Affiliated: {*Base DN*}, ou=[*Affiliated Organization Name*], cn=Subscriber's full name, serialNumber=UUID from the PIV-I card that holds the certificates.
- Unaffiliated: {*Base DN*}, ou=[*Entity CA's Name*], ou=Unaffiliated, cn=Subscriber's full name, serialNumber=UUID from the PIV-I card that holds the certificates.

The PIV-I Card Authentication certificate shall not include a common name value, and shall include a non-null (only UUID required) *serialNumber* value and non-null *subjectAltName* value:

- Affiliated: {*Base DN*}, ou=[*Affiliated Organization Name*], serialNumber=UUID from the PIV-I card that holds the certificates.
- Unaffiliated: {*Base DN*}, ou=[*Entity CA's Name*], ou=Unaffiliated, serialNumber=UUID from the PIV-I card that holds the certificates.

Certificates issued under *id-stn-ssp-pivi-contentSigning* shall indicate the organization administering the CMS using the following form.

- {*Base DN*}, ou=[*CMS organization name*], cn=CMS name

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

3.1.2 Need for Names to be Meaningful

The subscriber certificates issued pursuant to this CPS shall contain names that can be understood and used by relying parties. Names used in the certificates must identify in a meaningful way the subscriber to which they are assigned.

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

cn=firstname initial. lastname

For the subscriber that is a CMS, this will typically be a freeform descriptive name that may optionally include a location:

cn=CMS name.

The *serialNumber* in the DN of the PIV-I Card Authentication certificate will only be a UUID:

serialNumber=UUID (see Practice note).

The value of *subjectAltName* in the PIV-I Card Authentication certificate will only be a UUID:

subjectAltname=UUID (see Practice Note).

> Practice Note: *When the UUID is included within the serial number attribute of the DN in a PIV-I Card Authentication certificate, it shall be encoded using the string representation from Section 3 of [RFC 4122]. An example would be "f81d4fae-7dec-11d0-a765-00a0c91e6bf6".*
>
> *When the UUID appears in the subjectAltName extension of a PIV-I Authentication or PIV-I Card Authentication certificate, it shall be encoded as a uniformResourceIdentifier as specified in Section 3 of [RFC 4122]. An example would be "urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6".*

For other certificate types, User Principal Names (UPN) may be used in *subjectAltName* and must be unique and accurately reflect the organizational structures.

While the issuer name in CA certificates is not generally interpreted by relying parties, this CPS requires use of meaningful names by CAs. If included, the common name shall describe the issuer, such as:

cn=Organization CA-3.

The subject name in CA certificates must match the issuer name in certificates issued by the subject, as required by RFC 5280.

3.1.3 Anonymity or Pseudonymity of Subscribers

The SSP CAs shall not issue anonymous or pseudonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting distinguished name forms are contained in the applicable certificate profiles (See Section 7.1.2. and Appendix A). Rules for interpreting PIV-I certificate UUID names are specified in RFC 4122.

3.1.5 Uniqueness of Names

The Organization RA and the DCPA will ensure the uniqueness of names for all certificates issued within the SSP CA domain. Information contained in certificate enrollment requests will be automatically checked against the DigiCert SSP database to prevent duplication and to ensure the uniqueness of SSP certificate distinguished names and serial numbers.

The DCPA will investigate and correct, if necessary, any name collisions brought to its attention. If appropriate, Organization PMAs will resolve name collisions within their own space and describe that process in their RPS.

3.1.6 Recognition, Authentication, and Role of Trademarks

The Organization RA and the DCPA shall resolve any name collisions or disputes regarding NFI SSP-issued certificates brought to its attention. The DCPA will not knowingly use trademarks in names unless the subject has the rights to use that name.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

For all certificate requests in which either the subscriber generates the key pair (Signature certificate) or the DigiCert Key Manager generates the key pair on behalf of the subscriber (Encryption certificate), the SSP CA shall require proof of possession of the private key that corresponds to the public key in the certificate request. The technical mechanism to establish this proof is verification that the Subscriber's certificate enrollment request containing their public key is digitally signed with the corresponding private key. For PIV-I credentials, this proof is satisfied by verification of the Subscriber's client authentication key (no digital signature capability). For re-key of PIV-I credentials, proof of possession of the current PIV-I authentication key is sufficient to re-key all keys contained on the PIV-I card.

For smart card issuance, certificate enrollment requests are sent from a CMS workstation to the SSP CA as signed and encrypted messages (PKCS #7-enveloped PKCS #10 requests) over an HTTP link. For software credentials, certificate enrollment requests are sent over an SSL session from a FIPS 140 Level 1 browser to the SSP CA. The format for this data is dependent on the type of browser.

For all certificate enrollment requests, the SSP CA performs the digital signature validation checks to ensure it is a properly formed message and that its integrity has not been altered.

In cases where key generation is performed under the CA or RA's direct control, proof of possession is not required.

3.2.2 Authentication of Organization Identity

Requests for CA certificates in the name of an organization or subscriber certificates in the name of an Affiliated Organization shall include the organization name, address, and documentation of the existence of the organization. DigiCert shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the organization.

3.2.3 Authentication of Identity

Certificates issued under *id-stn-ssp-pivi-hardware* shall be issued only to human subscribers.

3.2.3.1 Authentication of Human Subscribers

Procedures used by organizations to issue identification to their own personnel and affiliates may be more stringent than the following. When this is the case, the organization's procedures for authentication of personnel shall apply in addition to the guidance in this section. Except for certificates issued under *id-stn-ssp-rudimentary*, subscriber information that is not verified shall not be included in certificates.

The RA shall ensure that the applicant's identity information is verified. For certificates issued under medium assurance, identity shall be established no more than 30 days before initial certificate issuance. RAs may accept notarized authentication of an applicant's identity to support identity proofing of remote applicants, assuming

organization identity badging requirements are otherwise satisfied. Minimal procedures for RA authentication and notarized authentication of employees and affiliated personnel are detailed below.

At a minimum, the authentication procedures for employees must include the following steps:

1) Verify that a request for certificate issuance to the applicant was submitted by organization management;
2) Applicant's employment shall be verified through use of official organization records.
3) Except for *id-stn-ssp-rudimentary* and *id-stn-ssp-basic* policies, applicant's identity shall be established by in-person or supervised remoted identity[3] proofing before the Registration Authority or Trusted Agent, based on the following processes:
    i) Identity source documents are presented as follows:
        - For non-PIV-I credentials, the applicant presents one Federal government-issued photo ID, one REAL ID Act compliant picture ID[4] or two non-Federal forms of ID, one of which must be a photo ID (e.g. non-REAL ID Act compliant driver's license) as proof of identity. A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement[5];
        - For PIV-I credentials, the applicant presents two identity source documents in original form. The identity source documents must come from the list of acceptable documents included in *Form I-9, OMB No. 1115-0136, Employment Eligibility Verification*. At least one document shall be a valid State or Federal Government-issued picture identification (ID). For PIV-I credentials, an in-person antecedent is not permitted;

    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) i) above shall be verified by the RA for currency and legitimacy (e.g., the organization ID is verified as valid). Typically this is accomplished by querying a database[6] maintained by the organization that issued the credential, but other equivalent methods may be used. Any credentials presented must be unexpired.
4) Biometric data is captured for PIV-I credentials and formatted in accordance with NIST SP800-76 as follows:
    i) an electronic facial image used for printing facial image on the card, as well as for performing visual authentication during card usage (a new facial image shall be collected each time a card is issued); and,
    ii) two electronic fingerprints to be stored on the card for automated authentication during card usage.

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/Affiliated Organization employee. For PIV-I credentials, validation includes the

[3] The minimum requirements associated with supervised remote identity proofing are described in NIST SP 800-63A, Digital Identity Guidelines: Enrollment and Identity Proofing, Section 5.3.3.
[4] REAL ID Act compliant IDs are identified by the presence of the DHS REAL ID star.
[5] Clarification on the trust relationship between the Trusted Agent and the applicant, which is based on an in-person antecedent identity proofing event, can be found in the *FBCA Supplementary Antecedent, In-Person Definition* document.
[6] Databases or other sources that are used to confirm Subscriber attributes shall provide 1) an auditable chain of custody of information obtained, and 2) secure exchange of data in a confidential and tamper-evident manner, and 3) protection of data from unauthorized access.

authentication of organization identity as specified in section 3.2.2 and inclusion of the organization name within the subscriber DN.

2) Sponsoring/Affiliated Organization employee's identity and employment shall be verified through either of the following methods:

   a) A digital signature verified by a currently valid employee Signature certificate issued by the CA, may be accepted as proof of both employment and identity, or

   b) Employee's identity shall be established by in-person proofing before the Registration Authority as in employee authentication above and employment validated through use of the official organization records.

3) Except for *id-stn-ssp-rudimentary* and *id-stn-ssp-basic* policies, applicant's identity shall be established by in-person or supervised remote sessions proofing before the Registration Authority, based on the following processes:

   i) Identity source documents are presented as follows:
      - For non-PIV-I credentials, the applicant presents one Federal government-issued ID or two Non-Federal government-issued IDs, one of which must be a photo ID (e.g., driver's license) as proof of identity. A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement;
      - For PIV-I credentials, the applicant presents two identity source documents in original form. The identity source documents must come from the list of acceptable documents included in *Form I-9, OMB No. 1115-0136, Employment Eligibility Verification*. At least one document shall be a valid State or Federal Government-issued picture identification (ID). For PIV-I credentials, an in-person antecedent is not permitted;

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

4) Biometric data is captured for PIV-I credentials and formatted in accordance with NIST SP800-76 as follows:
   i) an electronic facial image used for printing facial image on the card, as well as for performing visual authentication during card usage (a new facial image shall be collected each time a card is issued); and,
   ii) two electronic fingerprints to be stored on the card for automated authentication during card usage

Additionally, the RA shall record on a Subscriber Enrollment Form, the process that was followed for issuance of each certificate. The Subscriber Enrollment Form shall include the following:

- The identity of the person performing the identification;
- A signed declaration by that person that he or she verified the identity of the Applicant as required by the CPS using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury). The signature on the declaration may be either a handwritten or digital signature using a certificate that is of equal or higher level of assurance as the credential being issued;
- Unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- The date and time of the verification; and

- A declaration of identity signed by the applicant using a handwritten signature or appropriate digital signature[7] using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury). Except for *id-stn-ssp-rudimentary* and *id-stn-ssp-basic* policies, this signature shall be performed in the presence of the person performing the identity authentication. The Subscriber shall also attest that he or she understands and acknowledges the obligations contained in the Subscriber Agreement including use and protection of the private key and the need to report suspicion of loss or compromise of the private key.

For all levels except PIV-I , where it is not possible for applicants to appear in person before the RA either in-person or supervised remote, a Trusted Agent may serve as proxy for the RA. The Trusted Agent forwards the information collected from the applicant directly to the RA in a secure manner. The requirement for recording a biometric of the applicant may be satisfied by making a copy of the government issued photo ID (passport or driver's license) presented to the Trusted Agent. The Trusted Agent shall verify the photograph against the appearance of the applicant and notarize a copy of the photo ID. The notarized copy of the photo ID shall be included with the notarized Subscriber Enrollment form and sent to the SSP RA either by first class postal mail, Federal Express or other similar means.

Authentication by a Trusted Agent does not relieve the RA of its responsibility to perform steps 1), 2), the verification of identifying information (e.g., by checking official records) in step 3), and the maintenance of biometrics in step 4), above.

For *id-stn-ssp-basic*, identity proofing may optionally consist of a verification check against information (e.g., database) generally known only to the applicant and the information administrator. Such checks shall validate that the name, address and other personal information in records are consistent with the application and sufficient to identify the unique individual. Such checks can occur via an automated electronic mechanism or via telephone communications to a known phone number for the applicant while the conversation is recorded.

For certificates issued under *id-stn-ssp-rudimentary*, only a verification of an email address is required.

In the event an applicant is denied a credential based on the results of the identity proofing process, the RA shall describe the process for appeal or redress of the decision in their associated RPS.

3.2.3.2 Authentication of Human Subscribers for Role-based Certificates

The DigiCert SSP does not issue certificates to a Subscriber identified by a role.

3.2.3.3 Authentication of Human Subscribers for Group Certificates

Normally, a certificate shall be issued to a single Subscriber. For cases where there are several entities acting in one capacity, and where non-repudiation for transactions is not desired, a certificate may be issued that corresponds to a private key that is shared by multiple Subscribers. This capability is restricted to *id-stn-ssp-rudimentary* and *id-stn-ssp-basic* policies.

RAs shall record the information identified in Section 3.2.3 for the designated sponsor before issuing a group certificate. In addition to the authentication of the sponsor, the following procedures shall be performed for members of the group:

- The RA shall be responsible for ensuring control of the private key, including maintaining a list of

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

Subscribers who have access to use of the private key, and accounting for which Subscriber had control of the key at what time;
- The *subjectName* DN must not imply that the subject is a single individual, e.g. by inclusion of a human name form;
- The certificate shall not assert the *nonRepudiation* bit;
- The list of those holding the shared private key must be provided to, and retained by, the applicable CA or its designated representative; and
- The procedures for issuing tokens for use in shared key applications must comply with all other stipulations of the CP (e.g., key generation, private key protection, and Subscriber obligations).

3.2.3.4 Authentication of Devices

The SSP CA may provide device component certificates (e.g., for card management systems, routers, firewalls, servers, etc.). This capability is restricted to *id-stn-ssp-mediumDevices* and *id-stn-ssp-mediumDevicesHardware* policies. Enrollment for the certificate must be performed by a human PKI Sponsor as described in Section 5.2.1.6. The PKI Sponsor is responsible for providing the RA, or approved Trusted Agent, correct information regarding:

- Device name (equipment identification (eg, serial number or DNS name)) or unique software application name;
- Device (equipment or software application) public keys (using a Certificate Signing Request);
- Device (equipment or software application) authorizations and attributes (if any are to be included in the certificate); and
- Contact information to enable DigiCert to communicate with the PKI sponsor when required.

For certificates issued at the *id-stn-ssp-mediumDevices* and *id-stn-ssp-mediumDevicesHardware* policies, registration shall be verified commensurate with the Medium assurance level. Acceptable methods include but are not limited to in person or supervised remote registration of the PKI Sponsor, with the identity of the PKI Sponsor confirmed in accordance with the requirements of Section 3.2.3.1 commensurate with the assurance level of the certificate requested. Alternatively, if the PKI Sponsor has a valid certificate issued by the SSP PKI, verification of the signature on a digitally signed message from the Sponsor is acceptable for identity authentication. In the case a human sponsor is changed, the new sponsor shall review the status of each device under his/her sponsorship to ensure it is still authorized to receive certificates.

3.2.4 Non-Verified Subscriber Information

Except for certificates issued under *id-stn-ssp-rudimentary*, subscriber information that is not verified shall not be included in certificates.

Other than the subscriber email address, subscriber information for certificates issued under *id-stn-ssp-rudimentary* is not verified.

3.2.5 Validation of Authority

CA certificates issued in the name of an organization shall be issued only after verification that the requestor has the authorization to act on behalf of the organization.

3.2.6 Criteria for Interoperation

The DigiCert SSP shall comply with the certificate and CRL profiles defined by the FPKIPA. The FPKIPA shall

be responsible for all decisions to cross-certify the FBCA with an external PKI[8]. Under no circumstances shall any certificate have more than one intentional trust path to the FBCA, irrespective of extension processing. Multiple trust paths created as a result of certificate renewal or CA rekey do not violate the single trust path requirement in the FBCA CP.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

The DigiCert SSP supports re-key for Subscriber and CA certificates. If it has been less than nine (9) years since a Subscriber was identified as required in Section 3.1, re-key requests for Subscriber certificates may be authenticated on the basis of existing subscriber certificates. A Subscriber, whose certificates have not expired and whose initial subscriber enrollment data has not changed, may re-key his or her certificates based on electronic authentication of a currently valid Signature and Encryption certificates. The SSP CA provides separate SSL-protected web pages for re-keying of Signature and Encryption certificates.

If the previous re-key authentication method was the same as original enrollment, then an alternate method may be used. Acceptable alternate methods are through proof of possession of the private key or through the use of a Challenge Phrase (or the equivalent thereof). During original enrollment, Subscribers choose and submit a Challenge Phrase (or the equivalent thereof). Upon rekey of a Certificate, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's reenrollment information, and the enrollment information (including contact information) has not changed, a rekey Certificate is automatically issued.

The SSP CA may issue Subscriber certificates with a maximum of three (3) year lifetime. If more than nine (9) years have passed since a Subscriber's identity was authenticated as specified in Section 3.1, a Subscriber certificate re-key shall follow the same procedures as initial certificate issuance.

3.3.2 Identification and Authentication for Re-Key After Revocation

Subscribers must repeat the initial registration requirements, including in-person identity verification, for re-key after revocation.

3.4 Identification and Authentication for Revocation Request

The SSP CA provides an online SSL-secured Web page at which subscribers may request revocation of their SSP certificate(s). The Subscriber authenticates by presenting his or her challenge phrase selected during the certificate enrollment process. The subscriber may also request revocation of his or her certificate by sending a digitally signed e-mail message to the RA.

The RA will authenticate the request by verifying the digital signature on the signed-mail. If the Subscriber does not have access to the challenge phrase or his or her certificate, the Subscriber may communicate with the RA by telephone, facsimile, e-mail, postal mail, or courier service. The RA shall authenticate the communication before revoking the Subscriber's certificate(s).

Upon receiving a request from a representative of an Affiliated Organization, the RA shall verify the representative and the representative's authorization in accordance with section 3.2.2.

A Trusted Agent may request revocation of an affiliated Subscriber's certificate by sending a digitally signed e-mail message to DigiCert. The Organization RA will authenticate the request by validating the digital signature

[8] See also the *Federal Public Key Infrastructure Bridge Application Process Overview document [BRIDGE PROCESS]* and the *Federal Public Key Infrastructure Annual Review Requirements* document

on the signed e-mail and will check that the Trusted Agent is requesting revocation for a subscriber certificate that is affiliated with his or her organization.

A RA may revoke a Subscriber's certificate only for Subscribers affiliated with his or her organization.

The Organization RA may revoke a Subscriber's certificate for cause.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Submission of Certificate Application

A certificate application may be submitted to the SSP CA by the Subscriber or by an Organization RA on behalf of the Subscriber.

4.1.2 Enrolment Process and Responsibilities

SSP PKI Authorities perform the following steps when processing a certificate enrollment request from an applicant:

- Establish the applicant's authorization (by the employing or sponsoring/Affiliated Organization) to obtain a certificate. (per Section 3.1)
- Establish and record identity of the applicant (per Section 3.1)
- Obtain the applicant's public key and verify the applicant's possession of the private key for each certificate required (per Section 3.2.1)
- Verify authorization information requested for inclusion in the certificate.

Details of the certificate application process for each type of certificate issued by the SSP CA are described in section 3.1.

All communications among SSP PKI Authorities in processing certification applications are electronic and are protected by SSL.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Hardware Credential

1) Applicants (including human Subscribers and PKI Sponsors for Device Certificates) enrolling for a SSP certificate on a smart card must appear before a designated Organization official for authentication of identity as described in Section 3.2.3. After successfully completing the authentication requirements, applicants receive a completed enrollment authorization from the Organization official.

2) The Applicant must appear before an Organization RA and present the enrollment authorization form. The Organization RA initiates the process for personalization of the smart card, prints the smart card, and enrolls on behalf of the Subscriber for the certificate(s) (human or device). Alternatively, after issuance of the smart card the Subscriber receives a Passcode from the Organization RA which may be later presented to an Organization-hosted, SSL/TLS-protected web page for enrollment for the certificates.

3) Public/private key pairs for authentication certificates are generated on the smart card (including auth, cardAuth, digital signature, and/or other attributes as specified in the Certificate profile). A certificate signing request is generated which includes the public key, the subscriber name, e-mail address and organizational data necessary to populate the certificates which meets the attributes in the associated certificate profile specified in Appendix A. The certificate signing request is submitted over an SSL/TLS session to the SSP CA, which checks for proof of possession of the private key.

The SSP CA then signs the request and returns the certificates to the smart card issuance system where it is then downloaded onto the Subscriber's smart card. Only the digital signature certificates are posted to the SSP Repository.

4) An Organization-hosted Key Manager performs key pair generation and key escrow functions for the Encryption certificate. A certificate signing request is generated and submitted to the SSP CA, which checks for proof of possession of the private Encryption key. The SSP CA then signs the request, posts the certificate to the SSP Repository and returns the Encryption certificate to the smart card issuance system where it is downloaded to the Subscriber's smart card.

Software Credential

1) Applicants (including human Subscribers and PKI Sponsors for Device Certificates) must appear before a designated Organization official for in-person identity proofing in accordance with the requirements of Section 3.2.3. After successfully completing the identity authentication requirements, the Applicant receives an enrollment Passcode to be used for authentication during the certificate enrollment process.

2) Using a web browser, applicants connect to an Organization-hosted SSL/TLS-protected web page that includes general instructions for completing the certificate enrollment process. The applicant completes an online certificate enrollment form, including entry of the enrollment Passcode, and submits it as a request for a certificate. When the Subscriber completes the online form, a dual key generation process is initiated (unless the subscriber is *id-stn-ssp-rudimentary* or id-*stn-ssp-basic*, which are single pair certificates with no key escrow). First, the public-private key pair for the Signature certificate is generated locally on the Subscriber's workstation, and then the key pair for the Encryption certificate is generated in an Organization-hosted Key Manager, if key escrowing is part of the contract. Two certificate signing requests are sent to the SSP CA over an SSL/TLS session. The SSP CA checks for proof of possession of the respective private keys and creates both certificates, posts them to the repository and returns the certificates to the web browser for installation in the browser cache.

4.2.2 Approval or Rejection of Certificate Applications

SSP PKI Authorities will reject an application for a certificate if:

- Authentication of all required information in accordance with Section 3.2 cannot be completed, or
- Payment has not been received.

4.2.3 Time to Process Certificate Applications

DigiCert begins processing certificate applications within a reasonable time of receipt. There is no time stipulation to complete the processing of an application except that for medium assurance certificates identity shall be established no more than 30 days before initial certificate issuance.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Except for *id-stn-ssp-rudimentary* policy, all information included in the certificate shall be verified prior to certificate issuance.

The SSP CA verifies the source of a certificate request and issues a certificate as follows:

Hardware Credential
For certificate enrollment requests received from a smart card issuance system and signed by the RA key on the associated hardware security module, certificate issuance by the SSP CA is automatic. The certificate is immediately delivered back to the smart card issuance system, which downloads the certificate onto the Subscriber's smart card.

Software Credential
For certificate enrollment requests received from a browser and signed by the key on the RA hardware security module, certificate issuance by the SSP CA is automatic. The certificate is immediately delivered back to the browser, which stores the certificate in the browser cache or other comparable certificate store.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Notification of certificate generation is an integral part of the certificate issuance/acceptance process for both hardware and software credentials.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Hardware Credential
The Subscriber signs a statement declaring that he/she has read the Subscriber Agreement and understands and accepts their responsibilities as defined in Section 9.6.3. The Subscriber is also notified that the private key associated with their Encryption certificate is escrowed. After the Subscriber's certificates are downloaded to the smart card, the Subscriber takes possession of the smart card and signs a receipt. For acceptance of a PIV-I Card, the RA shall activate and release the PIV-I Card to the subscriber only after a successful 1:1 biometric match of the applicant against the biometrics collected in Section 3.2.3.1.

Software Credential
A Subscriber accepts a certificate when he or she downloads the certificate from the SSL/TLS-protected web sites designated for downloading SSP Signature and Encryption certificates. During the enrollment process, the Subscriber signs a statement declaring that they have read the subscriber agreement and understand and accept their responsibilities as defined in Section 9.6.3. The Subscriber is also notified that the private key associated with their Encryption certificate is escrowed.

In the case of non-human components (web servers, routers, firewalls, etc.), the PKI Sponsor (as defined in Section 5.2.1.6) shall perform a similar function for the acceptance of the component certificate. There is no escrow of private keys associated with certificates for non-human components.

4.4.2 Publication of the Certificate by the CA

The CA shall publish Subscriber certificates as specified in section 2.2.1.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The FPKIPA shall be notified of any CA certificate issuance by the Non-Federal SSP.

DigiCert will notify the FPKIPA at least two weeks prior to the issuance of a new CA certificate or issuance of new inter-organizational CA cross-certificates. The notification will assert that the new CA cross-certification does not introduce multiple paths to a CA already participating in the FPKI. In addition, all new artifacts (CA

certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the CA certificate issuance will be provided to the FPKIPA within 24 hours following issuance.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The Subscriber shall not use the Identity private key after the associated certificate has been revoked or has expired. The Subscriber may continue to use the decryption private key solely to decrypt previously encrypted information after the associated certificate has been revoked or has expired.

The use of private keys shall be limited in accordance with the key usage extension in the certificate. If the extended key usage extension is present and implies any limitation on the use of the private key, those constraints shall also be observed.

DigiCert SSP subscribers are obligated to prevent unauthorized disclosure of their private keys and activation data in accordance with sections 6.2.4.2 and 6.2.8.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties shall ensure that a public key in an SSP certificate is used only for the purposes indicated by the key usage extension, if the extension is present. If the extended key usage extension is present and implies any limitation on the use of the certificate, those constraints shall also be followed.

4.6 Certificate Renewal

Renewing a certificate means creating a new certificate with the same name, key, and authorizations as the old one, but a new, extended validity period and a new serial number. Following renewal, the old renewed or modified CA certificate may not be further renewed, re-keyed, or modified.
SSP CAs may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the Subscriber name and attributes are unchanged. SSP CA renewal requires notification to the FPKIPA as per Section 4.4.3.

4.6.1 Circumstance for Certificate Renewal

The SSP does not implement certificate renewal for Subscriber. In the event of a CA compromise, Subscribers shall be required to repeat the initial certificate application process.

The SSP may renew CA Certificates and OCSP responder certificates so long as the aggregated lifetime of the public key does not exceed the certificate lifetime specified in section 6.3.2.

4.6.2 Who May Request Renewal

For all CAs and OCSP responders operated by DigiCert, the request is internal and renewal of its own certificate is processed by the SSP CA after review and approval by the DCPA.

4.6.3 Processing Certificate Renewal Requests

For all CAs and OCSP responders operated by DigiCert, the request is internal and renewal of its own certificate is processed by the SSP CA after review and approval by the DCPA.

4.6.4 Notification of New Certificate Issuance to Subscriber

For all CAs and OCSP responders operated by DigiCert, renewal is internally communicated to relevant parties.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

For all CAs and OCSP responders operated by DigiCert, the request is internal and renewal of its own certificate is processed by the SSP CA after review and approval by the DCPA.

4.6.6 Publication of the Renewal Certificate by the CA

As specified in section 2.1, all CA certificates are published in repositories.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

When CA certificates are issued, The CA meets notification requirements of section 4.4.3

4.7 Certificate Re-Key

The SSP supports re-key for Subscriber and CA certificates. Re-keying a certificate means that a new certificate is created that is identical to the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key); a different serial number; and may be assigned a different validity period. After certificate re-key, the old certificate may or may not be revoked, but shall not be further re-keyed, renewed or modified.

4.7.1 Circumstances for Certificate Re-Key

The SSP certificate is re-keyed on Subscriber request, normally when it is nearing the end of its validity period. Revoked SSP certificates shall not be re-keyed.

4.7.2 Who May Request Certification of a New Public Key

The FPKIMA may request certification of a new public key for DigiCert.

DigiCert only accepts requests for a new public key from the subject of the certificate or PKI sponsors. Additionally, DigiCert and RAs may initiate re-key of a subscriber's certificates without a corresponding request.

The request for re-key shall be authenticated by an RA by electronic or in-person methods in accordance with the process described in Section 3.3.1 to those authenticated as Subscribers, PKI Sponsors, or Authorized parties.

4.7.3 Processing Certificate Re-Keying Requests

The re-key request shall be authenticated either by electronic or in-person methods in accordance with the process described in Section 3.3.1.

4.7.4 Notification of New Certificate Issuance to Subscriber

Notification of issuance of a re-keyed certificate to the Subscriber is in accordance with Section 4.3.2 or Section 4.9.12 in the case of CA key compromise, all in accordance with publication requirements set forth in Section 2.2.1.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

See section 4.4.1.

4.7.6 Publication of the Re-Keyed Certificate by the CA

The CA shall publish Subscriber certificates as specified in section 2.2.1.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of the issuance of certificates they approve.

When CA certificates are issued, the CA meets notification requirements of section 4.4.3

4.8 Certificate Modification

Modifying a certificate means creating a new certificate that has the same or a different key and a different serial number, and that differs in one or more other fields from the old certificate.

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

4.8.1 Circumstance for Certificate Modification

The SSP does not implement certificate modification for Subscriber certificates. If an individual's name, authorizations or privileges change, the Subscriber must enroll for a new certificate using the procedures defined in Section 4.1, and the old certificate shall be revoked.

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

4.8.2 Who May Request Certificate Modification

Requests for certification of a new public key are completed by the SSP CA and processed internally, including approvals by the DCPA, prior to issuance.

4.8.3 Processing Certificate Modification Requests

The SSP CA processes the modification of a CA, subordinate CA, or OCSP responder Certificate internally after approval by the DCPA, prior to issuance.

4.8.4 Notification of New Certificate Issuance to Subscriber

When DigiCert updates its SSP CA Certificate, it shall notify by e-mail all CAs, RAs and Subscribers that rely on the CA's certificate that it has been changed and shall provide instructions for how to obtain and validate the updated SSP CA certificate.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

For the SSP CA modification of a CA, subordinate CA, or OCSP responder Certificate, not applicable.

4.8.6 Publication of the Modified Certificate by the CA

All CA certificates modified will be published as specified in section 2.1.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

All CA certificates modified will be published as specified in section 2.2.1.

Any subordinate CAs will be communicated as stated in section 4.8.4.

4.9 Certificate Revocation and Suspension

A certificate shall be revoked upon receipt of an authenticated request from an appropriate entity. Revocation requests shall be authenticated in accordance with section 3.4.

For DigiCert, the FPKIPA will be notified at least two weeks prior to the revocation of a CA certificate, whenever possible. For emergency revocation, DigiCert follows the notification procedures in Section 5.7.

4.9.1 Circumstances for Revocation

An SSP certificate shall be revoked when the binding between the subject and the subject's public key defined within the certificate is no longer considered valid. Under the following circumstances a certificate will be revoked: Note: The following also applies if Subscribers are using hardware tokens.

- Identifying information including the organizational affiliation in the Subscriber's certificate changes, affiliation is terminated, or the organization no longer authorizes the affiliation before the certificate expires;
- Privilege attributes asserted in the Subscriber's certificate are reduced;
- The certificate subject can be shown to have violated the requirements of this CPS or the subscriber agreement;
- The private key is suspected of compromise, e.g. due to loss or theft;
- The subscriber fails to sign the declaration of identity during registration in accordance with section 3.2.3.1;
- The subscriber or other authorized party asks for his/her certificate to be revoked; or
- The continued use of the certificate may be harmful to the Non-Federal SSP PKI.

Whenever any of the above circumstances occur, the associated certificate is revoked and placed on the CRL. Certificates remain on the CRL until they expire; they are removed from subsequent CRLs issued after they expire. A revoked certificate will appear on at least one CRL.

The Affiliated Organization is responsible for requesting revocation of the certificate if the affiliation is no longer valid. If an Affiliated Organization has terminated its relationship with the SSP CA, the SSP CA shall revoke all certificates affiliated with that organization.

4.9.2 Who Can Request Revocation

The Subscriber is authorized to request the revocation of his or her own certificate. The Organization RA, the Subscriber's authorizing organization, or other authorized party including a Trusted Agent can request the revocation of a Subscriber's certificate on the Subscriber's behalf. For certificates issued in association with an Affiliated Organization, the revocation request shall be accepted from the Affiliated Organization named in the certificate. A Trusted Agent can only request revocation of a certificate for a subscriber that is affiliated with the Trusted Agent's organization. Notice including a reason for the revocation is provided by the SSP to a subscriber whose certificate has been revoked.

4.9.3 Procedure for Revocation Request

The revocation request must uniquely identify the certificate to be revoked and must include the reason for revocation. The certificate to be revoked must be uniquely identified with information including: the organization name, the subject name and the email address on the certificate. The revocation requests may be manually or digitally signed and must be authenticated by an RA. If the revocation is being requested for reason of key compromise or suspected fraudulent use, then the subscriber's and the RA's revocation request must so indicate. The processes for revocation are as follows:

Certificate Revocation Request by Subscriber: An SSP Subscriber may request revocation of a certificate by sending a digitally signed message to the Organization RA. The message must include a reason for the revocation. The Organization RA will validate the request by verifying the signature on the signed message. If the Subscriber is not in possession of their private Signature key, he or she may also request revocation of his or her certificate by presenting the unique challenge phrase selected during certificate enrollment to a revocation Web page hosted by DigiCert. The Web page is protected using SSL/TLS. Upon successful validation of the revocation request by the RA, the SSP CA will change the certificate status in the repository from "valid" to "revoked" and place the revoked certificate's serial number on the next published CRL.

A Subscriber ceasing its relationship with the SSP PKI shall, prior to departure, surrender to the appropriate Trusted Agent or RA, all cryptographic hardware tokens issued to the Subscriber. The tokens shall be zeroized or destroyed promptly upon surrender and shall be protected from use between surrender and zeroization or destruction. If the hardware tokens cannot be obtained from the Subscriber, then all Subscriber certificates associated with the un-retrieved tokens shall be revoked.

The SSP CA (or delegate) shall collect and destroy PIV-I Cards from subscribers whenever the cards are no longer valid, whenever possible, and shall record the destruction of PIV-I Cards.

Certificate Revocation Request by Trusted Agent: A Trusted Agent may request revocation of a Subscriber's certificate by sending a digitally signed message to the Organization RA. The TA shall receive a request from a Subscriber uniquely identifying the Subscriber whose certificate(s) is to be revoked and the reason for the revocation. The TA shall authenticate the Subscriber's request for revocation either by validating the Subscriber's signature on a digitally signed-e-mail, by validating the Subscriber's identity in person, or by consulting an appropriate entity in the Subscriber's organization.

The Organization RA will validate the request received from the TA by verifying the signature on the signed message, that the TA is on the list of approved Trusted Agents and confirming that the affiliation in the Subscriber certificate is the same as the Trusted Agent affiliation. The message must identify the name and e-mail address of the subscriber whose certificate(s) is to be revoked and the reason for the revocation. Upon successful validation of the revocation request by the Organization RA, the SSP CA will change the certificate status in the repository from "valid" to "revoked" and place the revoked certificate's serial number on the next published CRL.

Certificate Revocation Request by RA: An RA may request revocation of any SSP subscriber certificate affiliated with their organization. Access to the SSP CA to request revocation requires presentation of a valid RA certificate. The SSP CA validates the RA certificate and checks that the RA affiliation is the same as the organizational affiliation in the certificate to be revoked. If these checks are successful, the SSP CA will change the certificate status in the repository from "valid" to "revoked" and place the revoked certificate's serial number on the next published CRL.

The SSP CA will aggregate all revoked certificates, digitally sign a new Certificate Revocation List, and post the CRL to the repository per the frequency specified in Section 4.9.7.

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

4.9.4 Revocation Request Grace Period

There is no grace period for the revocation of the certificate by the SSP CA.

4.9.5 Time within Which CA Must Process the Revocation Request

The Subscriber or RA is obligated to request that the SSP CA revoke the certificate as soon as possible after the need for revocation has been determined. The SSP CA will revoke certificates as quickly as practical upon receipt of a proper revocation request. Revocation requests shall 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 shall be processed before the next CRL is published.

4.9.6 Revocation Checking Requirement for Relying Parties

The SSP publishes information on how to obtain information on revoked certificates and advises relying parties via the SSP CPS of the need to check certificate revocation status. If a Relying party is unable to obtain revocation information for an SSP-issued certificate, the Relying party must either reject use of the certificate, or make an informed decision to accept the risk, responsibility, and consequences of using certificate whose authenticity cannot be guaranteed.

4.9.7 CRL Issuance Frequency (If Applicable)

For routine revocations of certificates issued under policies *id-stn-ssp-basic* and *id-stn-ssp-rudimentary*, the SSP CA will issue CRLs at least every twenty four (24) hours and these CRLs shall have a twenty four (24) validity interval (*nextUpdate*). For all other assurance levels, the SSP CA will issue CRLs at least every twelve (12) hours, and these CRLs shall have a twenty-four (24) hour validity interval (*nextUpdate*).

Superseded CRLs are removed from the repository upon posting of the latest CRL. When a CA certificate is revoked because of compromise or suspected compromise of a private key in accordance with section 4.9.12, a CRL will be issued within six (6) hours of notification.

DigiCert Root CAs are operated offline and are used only for issuing certificates to other CAs and signing CRLs. CRLs for these offline CAs and their operations shall be published every 30 days, never to exceed 31 days.

4.9.8 Maximum Latency for CRLs

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

4.9.9 On-Line Revocation/Status Checking Availability

The SSP will provide an online Certificate Status Authority (CSA) to enable certificate status checking using the Online Certificate Status Protocol.

OCSP compliant with RFC 5019 and/or RFC 6960. OCSP responses either:

1. Are signed by the CA that issued the Certificates whose revocation status is being checked, or
2. Are signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

In the latter case, the OCSP signing Certificate contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC 6960.

The OCSP responder certificate will be issued on a FIPS 140 Level 3 hardware token. The OCSP responder certificate is signed by the same CA using the same key that signed the certificates whose status is to be checked. The OCSP responder shall ensure that accurate and up-to-date information is provided in the revocation status response and shall digitally sign all responses. Distribution of OCSP status information will meet or exceed the CRL issuance requirements specified in section 4.9.7.

Where a certificate is revoked for key compromise, the status information will be updated and available to relying parties within 6 hours. Where a certificate is revoked for a reason other than key compromise, the status information will be updated and available to relying parties within 18 hours.

4.9.10 On-line Revocation Checking Requirements

For PIV-I certificates, SSP CAs provide on-line status checking via OCSP.

Client software using online status checking need not obtain or process CRLs.

4.9.11 Other Forms of Revocation Advertisements Available

DigiCert does not support any other method for Revocation advertisement.

4.9.12 Special Requirements Regarding Key Compromise

In the event of a CA key compromise, the FPKIPA and any cross-certified CAs shall be immediately informed. The SSP shall initiate procedures to notify Subscribers of the compromise.

Subsequently, the DigiCert SSP will generate a new signing key pair and reconstitute its operation using the same procedures that were performed during initial system initialization and re-key all subscriber certificates. The new SSP CA certificate will be distributed as defined in section 6.1.4.

Organization RA is responsible for notification and revocation of subscriber certificates due to key compromise. This will trigger the serial number to be posted onto the CA's CRL in accordance with section 4.9.7.

4.9.13 Circumstances for Suspension

For CA certificates, suspension is not permitted. For end-entity certificates DigiCert allows certificate suspension to support temporary invalidation of certificates concurrent with the period that temporary replacement credentials are granted to subscribers.

4.9.14 Who Can Request Suspension

The Subscriber is authorized to request the suspension of their own certificate. The Organization RA, the Subscriber's authorizing organization, or other authorized party including a Trusted Agent can request the suspension of a Subscriber's certificate on the Subscriber's behalf. For certificates issued in association with an Affiliated Organization, the suspension request shall be accepted from the Affiliated Organization named in the certificate. A Trusted Agent can only request suspension of a certificate for a subscriber that is affiliated with

the Trusted Agent's organization. Notice including a reason for the suspension is provided by the SSP to a subscriber whose certificate has been suspended.

4.9.15 Procedure for Suspension Request

Certificate Suspension Request by RA: An RA may request suspension of any SSP subscriber certificate affiliated with their organization. Access to the SSP CA to request suspension requires presentation of a valid RA certificate. The SSP CA validates the RA certificate and checks that the RA affiliation is the same as the organizational affiliation in the certificate to be suspended. If these checks are successful, the SSP CA will change the certificate status in the repository from "valid" to "suspended" and place the suspended certificate's serial number on the next published CRL.

4.9.16 Limits on Suspension Period

A certificate may remain in a suspended state for no longer than thirty (30) days. The Organization RA or the SSP CA will track the timeframe through manual or systematic means in the records maintained of the original suspension request. If the suspension remains in place through the 30 day period, the Organization RA or SSP CA will either remove the suspension or revoke the Certificate prior to the end of the 30th day. This practice, if used, will be defined in the respective RPS.

4.10 Certificate Status Services

SSP CAs provide certificate status services via OCSP and via CRLs accessible by HTTP. See sections 4.9.7 to 4.9.11 inclusive.

4.11 End of Subscription

Subscription for a SSP certificate is synonymous with the certificate validity period. The subscription ends when the certificate is revoked or expired.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Key escrow is an integral part of the key generation of private encryption keys as described in sections 6.2.3 and 6.1.2 of this CPS. The Subscriber private signature key is never escrowed. Under no circumstances shall a Subscriber's Signature key be held in trust by a third party.

Escrowed keys shall be protected at no less than the level of security in which they are generated, delivered, and protected by the subscriber. Recovery of the private encryption key is under dual-person control by the RAs under this SSP CPS. The methods, procedures, and controls which apply to the storage, request for, extraction and/or retrieval, delivery, protections and destruction of the requested copy of an escrowed SSP Subscriber private encryption key are described in the respective RA's RPS, Appendix C, Key Recovery Practices and in the Appendix of this document for RA's to reference when needed..

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

DigiCert SSP PKI does not support session key encapsulation and recovery.

5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 Physical Controls

The SSP equipment is dedicated to CA functions and does not perform non-CA related functions. The SSP equipment includes, but is not limited to, the system running the SSP CA software, SSP CA hardware cryptographic module, and databases and directories located on SSP equipment. Databases located on the SSP computer system are not accessible to Subscribers or Relying Parties.

Unauthorized use of CA equipment is forbidden. Physical security controls are implemented to protect the CA hardware and software from unauthorized use. Certificate Management Authority (CMA) cryptographic modules are protected against theft, loss and unauthorized use. The security mechanisms shall be commensurate with the level of threat in the equipment environment.

5.1.1 Site Location and Construction

The system components and operation of the DigiCert SSP will be contained within a physically protected environment to deter, detect, and prevent unauthorized use of, access to, or disclosure of sensitive information. The primary site location is in [Text Removed], key storage rooms in [Text Removed] and a separate location in [Text Removed] (as described in section 5.1.2.2 and 5.1.2.3), and the DRF is in [Text Removed]. The facilities housing the primary and back-up CA provide extensive physical security and access control systems to limit access only to authorized personnel and authorized visitors. The primary and backup datacenters facilities reside in geographically diverse areas separate from one another.

Locks are of appropriate construction and strength and building keys are controlled and managed. Perimeter walls are slab to slab in construction and there are no windows that open.

Security guards and trusted facility employees perform site perimeter inspections of the primary and disaster recovery facility datacenters at least every 24 hours.

5.1.2 Physical Access

The system components (including RAs, CAs, Key Manager Database (KMD) and CSAs) of the in DigiCert SSP will be contained within a physically protected environment to deter, detect, and prevent unauthorized use of, access to, or disclosure of sensitive information. In addition, RA workstations are similarly protected with security mechanisms commensurate with the level of threat in the RA equipment environment and these protections are described in the respective RPS.

5.1.2.1 Physical Access for CA Equipment

Each building has an alarm system that actively monitored with redundant power and notification methods. Sensitive areas within the facilities, such as power and network connection areas, are also controlled areas within the protected facility. The building alarm systems are activated at a minimum when the building is unattended for periods greater than 8 hours. The datacenter operations facilities are manned around the clock. More sensitive areas, such as the data center containing active cryptographic modules, are continuously alarmed and monitored by cameras. Two-person access control is enforced for these areas.

Each building has multiple layers of perimeter security enforced through employee ID badges, electronic keys (proximity cards), and biometric readers. Employees are required to wear a picture ID badge, and visitors are escorted at all times. All visitors must sign the visitor log (name, signature, company/organization, date/time, and escort) prior to obtaining a visitor badge.

5.1.2.1.1 Data Centers

The primary and backup facilities are continually staffed (24x7), either by trusted data center employees or by an on-site guard service. Background checks are performed on the guards or trusted data center employees who are specifically trained for the facility. The guard force or trusted data center employees perform security checks at least once per 24 hours.

Both building's access control system is continuously (24x7) armed. Guards or trusted data center personnel located in a security station monitor access to the building electronically and by video cameras. Access to the outer perimeters are controlled by electronic key. Electronic keys and biometric readers control access to the inner, more secure parts of the facility. The access control systems have an anti-passback feature that automatically arms itself when someone enters. It logs all entries, exits, and system events. There are redundant connections for remote monitoring, with wireless backup. The system's power is backed-up with battery and diesel generator. Video cameras provide 24 hour recording of access to the buildings, the roofs, sensitive areas such as the data centers (e.g., the cryptographic key storage rooms/cages).

Offline cryptographic hardware is stored in secure containers requiring at least two trusted personnel to access the material. Removable cryptographic modules are inactivated before storage. Activation information is stored in locked containers separate from the cryptographic hardware.

5.1.2.1.2 Offline CA Key Storage Rooms

DigiCert securely stores the cryptomodules used to generate and store offline CA Private Keys. Access to the rooms used for key storage is controlled and logged by the building access card system. When not in use during a key ceremony, CA cryptomodules are locked in a safe that provides two-person physical access control. Activation data is protected in accordance with section 6.4. Cryptomodule activation keys (operator cards and PED keys) are either sealed in tamper-evident bags and placed in safe deposit boxes or stored in the two-person safe when not in use. Access to the safe is manually logged. Access card logs and the manual logs of access to the safe are reviewed on a regular basis.

5.1.2.1.3 CA Key Generation and Signing Rooms

CA Key Generation and Signing Rooms CA key generation and signing occurs either in the secure storage room described in section 5.1.2.2 or in a room of commensurate security in close proximity thereto. DigiCert's Administrators retrieve cryptographic materials necessary to perform key generation and certificate signing. At no time are cryptographic materials left unattended by fewer than two persons serving in trusted roles.

5.1.2.2 Physical Access for RA Equipment

5.1.2.2.1 Physical Access for PIV-I CMS Equipment

CMS equipment and the cryptographic module containing the PIV-I Content Signing key shall meet the physical access requirements specified for CA equipment including:

- Ensure no unauthorized access to the hardware is permitted
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers
- Ensure manual or electronic monitoring for unauthorized intrusion at all times
- Ensure an access log is maintained and inspected periodically
- Require two person physical access control to both the cryptographic module and computer systems
- Place removable cryptographic modules, activation information used to access or enable cryptographic modules, and other sensitive CA equipment in secure containers when not in use. Activation data shall not be stored together with the associated cryptographic module or removable hardware used to administer the CMS equipment.

- A security check of the facility housing the CMS equipment shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:
    - The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when "open", and secured when "closed";
    - Any security containers are properly secured;
    - Physical security systems (e.g., door locks, vent covers) are functioning properly; and
    - The area is secured against unauthorized access.

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

5.1.2.3 Physical Access for CSS Equipment

Physical access control requirements for CSS equipment, shall meet the CA physical access requirements specified in 5.1.2.1.

5.1.3 Power and Air Conditioning

The DigiCert SSP primary and backup facility datacenters are supplied with power and air conditioning sufficient to create a reliable operating environment.

Power for the primary site is backed up in case of emergency failure. If a major power failure occurs, a battery based UPS system can supply sufficient power to complete any pending actions and record the state of the equipment until the diesel generators are activated. The diesel generators are supplied from external to the building for unlimited refueling capacity. The diesel generators can operate for a minimum of 30 hours without refueling. In the event of loss of all power including the diesel generators, the UPS system has sufficient power to allow completing pending actions and take the SSP system offline.

5.1.4 Water Exposures

The DigiCert SSP primary and backup facility datacenters are installed on elevated flooring. The primary fire suppression systems for these facilities do not use water sprinklers.

5.1.5 Fire Prevention and Protection

An automated fire detection and suppression system has been installed in both datacenters in accordance with local fire policy and code.

5.1.6 Media Storage

Critical system data is incrementally backed-up on a daily basis. Full back-ups are performed on a weekly basis and the data is sent off site. The Symantec SSP has a disaster recovery (hot) site in [Text Removed]. Access to media is limited to authorized personnel and stored within disaster recovery site servers.

5.1.7 Waste Disposal

The SSP has disposal units for sensitive information separate from routine waste in all facilities. Sensitive information is carefully handled prior to destruction in approved shredder machines. Magnetic media such as backup tapes and hard disk drives are erased using an industrial grade degaussing system and shredded afterwards

5.1.8 Off-Site Backup

See section 5.1.6.

5.2 Procedural Controls

5.2.1 Trusted Roles

All employees, contractors, and consultants of the SSP that have access to or control cryptographic operations that may materially affect the issuance, use, suspension, or revocation of certificates, including access to restricted operations of the Repository, are considered as serving in a trusted position meeting the requirements of section 5.3.1. Such personnel include, but are not limited to, customer service personnel, system administration personnel, security auditors, designated engineering personnel, and executives who are designated to oversee the trustworthy infrastructures. All employees serving in a trusted position must acquire and periodically re-qualify (every ten years) for "trusted employee" status as a condition of employment

Within the context of trusted positions for the SSP, the SSP operation manifests itself in a number of functional roles required to securely and efficiently operate and manage a large data center operation. The PKI security-relevant roles are described below. Individuals assigned to one of these operational roles are not permitted to perform in another trusted role. DigiCert maintains lists, including names, organizations and contact information, of those who act in trusted roles, and shall make them available during compliance audits.

5.2.1.1 CA Trusted Roles

5.2.1.1.1 CA Administrator

The CA Administrator performs the following duties for the SSP CA; installing, configuring, and maintaining the CA; establishing and maintaining associated system accounts; configuring audit parameters; and generating component keys.

CA Administrators do not issue certificates to Subscribers.

5.2.1.1.2 CA Officer

The Officer role is fulfilled by the following entities for the SSP CA; authorizing and approving Certificate issuance and revocations

5.2.1.1.3 CA Auditor

The CA auditor(s) are in a department separate from engineering, operations, and system administrators. The SSP Audit Manager is responsible for reviewing, maintaining, and archiving audit logs associated with the SSP.

5.2.1.1.4 CA Operator

The Operator role is responsible for performing system backup and recovery for the SSP.

5.2.1.2 Organization RA Trusted Roles

RAs maintain and meet each of these trusted roles in accordance with section 5.3.1 of this CPS and will describe each in their respective RPS.

5.2.1.2.1 RA Administrator

The RA Administrator role is authorized to install, configure, and maintain the RA/CMS; establish and maintain system accounts; configure audit parameters; and generate RA related component keys

5.2.1.2.2 Registration Agent

An Organization Registration Agent is a representative of an organization that has entered into a contract with DigiCert for SSP PKI services. The Organization Registration Agent is authorized to request or approve certificate issuance and revocations on behalf of the Organization.

5.2.1.2.3 RA Auditor

The RA Auditor is authorized to review, maintain and archive RA audit logs.

5.2.1.2.4 RA Operator

The RA Operator is responsible for the operations and administration of the SSP RA equipment deployed at an Organization facility.

5.2.1.2.5 Trusted Agent

A Trusted Agent is a person authorized to act as a representative of the Registration Agent in providing Subscriber identity verification during the registration process. Trusted Agents do not have automated interfaces with the SSP CA or are considered trusted personnel required to adhere to stipulations at section 5.3.1.

5.2.1.2.6 PKI Sponsor

A PKI Sponsor fills the role of a Subscriber in the registration, validation and re-validation of certificate requests for non-human system components and organizations that are named as public key certificate subjects. The PKI Sponsor works with the Registration Agent and, when appropriate, Trusted Agents, to register components (web servers, routers, firewalls, etc.) in accordance with Section 3.2.3.4, and is responsible for meeting the obligations of Subscribers as defined throughout this document. PKI Sponsors are not considered trusted personnel required to adhere to stipulations at section 5.3.1

5.2.2 Number of Persons Required Per Task

The most sensitive tasks require at least two trusted employees with different roles. Multiparty control of CA operations shall exclude personnel that serve in the Auditor Trusted Role.

In DigiCert this includes access to and management of Cryptographic Signing Units (CSU), CA key generation, CA signing key activation, and CA private key backup. These activities require at least two trusted employees with different roles, one of which must be a holder of the Administrator role.

For Organization RAs, activities that require at least two persons are specific to gaining physical access to the CMS equipment to perform logical activities. One person filling the RA Administrator trusted role and one person from Enterprise IT Operations must be present with their respective keys and/or combination lock codes to gain physical access to the CMS server.

Logical access to the Key Escrow database and HSM cryptographic modules on the CMS is separated into two separate RA Administrator roles, one who controls the password to the HSM and configures the CMS system for HSM access, and another Administrator role that utilizes the CMS RA private keys and the CMS PIV-I Content Signing private keys during certificate issuance processes and revocation.. This process will be described in the RPS by the RA.

5.2.3 Identification and Authentication for Each Role

Individuals assigned to a SSP role defined above shall identify and authenticate using multi-factor authentication tokens before being permitted to perform any action set for that role according to section 10.4 of the DigiCert System Security Plan.

5.2.4 Roles Requiring Separation of Duties

The DigiCert SSP maintains a policy and rigorous control procedures to ensure segregation of duties based on job responsibilities. For all assurance levels, no person assigned to a trusted role has more than one identity on the CA, the RA, the CSA and the CMS. SSP RAs (Officers) do not have any other roles on the SSP CA, CSA or CMS systems.

The most sensitive tasks, such as access to and management of Cryptographic Signing Units (CSU), CA key generation, CA signing key activation and CA private key backup, require at least two trusted employees with different roles, one of which must be a holder of the Administrator role. A person holding the Auditor role may not participate in any other role.

5.3 Personnel Controls

5.3.1 Qualifications, Experience and Clearance Requirements

All persons with unattended access to the SSP and Repository are expressly approved and must be of unquestionable loyalty, trustworthiness, integrity, and U.S. Citizens.

The SSP institutes an extensive personnel security program that identifies specific "high risk" duties and requires "trusted personnel" to be assigned to these duties. The trusted status is only granted upon successful completion of a background investigation, performed by an independent investigation firm. Employees are trained and made fully aware of their responsibilities to maintain compliance with corporate security, unique program security, and personal security/integrity requirements as a condition of continued employment as a trusted employee.

Personnel appointed to operate CMA equipment shall:

- Have successfully completed an appropriate training course;
- Have demonstrated the ability to perform their duties;
- Be trustworthy;
- Have no other duties that would interfere with their duties as a CMA;
- Have not knowingly been previously relieved of CMA or other trusted duties for reasons of negligence or non-performance of duties;
- Have not knowingly been denied a security clearance, or had a security clearance revoked;
- Have not been convicted of a felony offense; and
- Be appointed in writing by an approving authority, or be a party to a contract for PKI services.

5.3.2 Background Check Procedures

As specified in section 5.2.1 (Trusted Roles), all persons filling trusted roles for the SSP shall either be US citizens or, in Organization RA roles, citizens of the country where their function is operating. All DigiCert persons filling trusted roles shall undergo a background investigation initially and a subsequent refresh every ten years. The scope of the background investigation is similar to the DOD Industrial Secret criteria. DigiCert retains the services of an independent investigation firm to perform the background investigations on its current and potential employees. In the conduct of its background investigations, investigators perform the following checks over the past seven (7) years:

1. Criminal history;
2. Credit history;
3. Previous employment;
4. Professional references;

5. Education (verification of highest or most relevant degree);
6. DMV records; and
7. Social Security trace.

Information revealed during a background investigation that would preclude an employee or potential employee from obtaining "trusted employee" status includes, but may not be limited to the following:

1. Any conviction or multiple arrests for a crime involving violence or attempted violence;
2. Any conviction or multiple arrests for a crime involving theft or attempted theft;
3. Any conviction or multiple arrests for a crime, other than mere possession of marijuana, involving controlled substances or illegal drugs;
4. Any pattern of behavior indicating personal irresponsibility, such as:
    (a) Multiple driving under the influence arrests (lifetime);
    (b) Multiple declarations of bankruptcy (lifetime);
    (c) Multiple recent (5 years) credit problems, including missed mortgage or car payments;
5. Any embellishment on a resume or job application involving:
    (a) Falsely stating an employer; or
    (b) Falsely stating academic qualifications.

5.3.3 Training Requirements

Operations personnel are sufficiently trained prior to performing independent, unattended duties. Training topics include the operation of the SSP software and hardware, operational and security procedures, disaster recovery and business continuity operations, and requirements of this CPS.

A training log is retained of each student who successfully completes a training (or retraining) module indicating the student trained, the training received, and the date the training was completed.

5.3.4 Retraining Frequency and Requirements

Personnel filling SSP PKI roles shall be aware of changes in the SSP operation. Any significant change to the SSP operations shall have a training plan and the execution of such plan shall be documented. Re-training is performed, as required, as new system functionality is deployed, or if there is any substantive change in SSP security or operational procedures.

5.3.5 Job Rotation Frequency and Sequence

DigiCert shall manage job rotation frequency and sequence to provide continuity and integrity of the SSP service.

5.3.6 Sanctions for Unauthorized Actions

DigiCert SSP personnel understand that service in the capacity of a trusted position is contingent on successful performance of the security and functional responsibilities commensurate with the trusted position. DigiCert SSP personnel who violate the provisions of this CPS are subject to administrative and disciplinary action, including suspension or termination.

5.3.7 Independent Contractor Requirements

Any DigiCert SSP subcontractor employed for a position is held to the same functional and security criteria as if he or she were a full-time DigiCert employee. All subcontractors shall comply with the requirements of the CP and this CPS.

5.3.8 Documentation Supplied to Personnel

Documentation, including this CPS, DigiCert's security policy, system documents and role-specific training materials necessary to define duties and procedures for a role, shall be provided to the personnel filling that role.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

SSP equipment will record events for the CA, RAs, and the CSA. The events include server installation, modification, accesses and application requests, responses, actions, publications, and error conditions. For CAs operated in a virtual machine environment (VME)[9], audit logs shall be generated for all applicable events on both the virtual machine (VM) and isolation kernel (i.e. hypervisor). The information recorded includes the type of event, the time the event occurred, and the identity of the operator that caused the event. Depending on the type of event, additional information such as the success or failure, the source and destination of a message or the disposition of a created object (e.g., a filename) will also be recorded. Electronic-based audit data is automatically collected. Physical data is recorded in a logbook, paper form, or other physical mechanism as appropriate to the process being audited. All security audit logs, both electronic and non-electronic, are retained and made available subject to compliance audits.

Records are also maintained regarding modifications to the CMA equipment configuration (e.g., changes in configuration files, security profiles, administrator privileges).

Logs used to record operator (for manned installations), room entry/exit, or security checks (per section 5.1.2) are kept for audit. Attempts to access the CMA equipment, such as login to accounts or enabling cryptographic modules, are recorded. The records include the identity asserted in the attempt, the time, and the success or failure.

Requests, responses, and publications are recorded for audit review purposes. These include certificate creation, modification, and revocation requests and responses; certificate publication, receipt acknowledgment, and proof-of-possession messaging; key compromise notices and responses; and CRL and CPS publications.

All actions related to the receipt, servicing and shipping of hardware cryptographic modules is recorded.

Physical access to, loading, zeroizing, transferring keys to or from, backing up, acquiring or destroying CMA cryptographic modules is recorded.

Actions performed in carrying out requests and in support of normal operation of the CA equipment are recorded, such as certificate and CRL creation, accesses to CA databases, and use of the CA's signature key.

DigiCert records all audit events and records data for the CA, CSA and RA in either manual (M) or electronic logs (E). Specific audit events recorded include:

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

[9] For the purposes of this policy, the definition of a virtual machine environment does not include cloud- based solutions (e.g. platform-as-a-service) or container-type solutions (e.g. Docker), which are not permitted for any CA cross-certified with the FBCA.

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

• LOCAL DATA ENTRY:
  - All security-relevant data that is entered in the system

• REMOTE DATA ENTRY:
  - All security-relevant messages that are received by the system

• DATA EXPORT AND OUTPUT:
  - All successful and unsuccessful requests for confidential and security-relevant information

• KEY GENERATION:
  - Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)

• PRIVATE KEY LOAD AND STORAGE:
  - The loading of Component private keys
  - All access to certificate subject private keys retained within the CA for key recovery purposes

• TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE:
  - All changes to the trusted public keys, including additions and deletions

• SECRET KEY STORAGE:
  - The manual entry of secret keys used for authentication

• PRIVATE AND SECRET KEY EXPORT:
  - The export of private and secret keys (keys used for a single session or message are excluded)

• CERTIFICATE REGISTRATION:
  - All certificate requests

• CERTIFICATE REVOCATION:
  - All certificate revocations

• CERTIFICATE STATUS CHANGE APPROVAL:
  - The approval or rejection of a certificate status change request

• CA CONFIGURATION:
  - Any security-relevant changes to the configuration of the CA

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

• CERTIFICATE PROFILE MANAGEMENT:
  - All changes to the certificate profile

• REVOCATION PROFILE MANAGEMENT:
  - All changes to the revocation profile

• CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT:
  - All changes to the certificate revocation list profile

• MISCELLANEOUS:

- Appointment of an individual to a trusted role
- Designation of personnel for multiparty control
- Installation of the operating system
- Installation of the CA
- Installing hardware cryptographic modules
- Removing hardware cryptographic modules
- Destruction of cryptographic modules
- System startup
- Logon attempts to CA applications
- Receipt of hardware / software
- Attempts to set or modify passwords
- Backing up CA internal database
- Restoring CA internal database
- File manipulation (e.g., creation, renaming, moving)
- Posting of any material to a repository
- Access to CA internal database
- All certificate compromise notification requests
- Loading tokens with certificates
- Shipment of tokens
- Zeroizing tokens
- Re-key of the CA
- Configuration changes to the CA server involving:
  - Hardware
  - Software
  - Operating system
  - Patches
  - Security profiles

• PHYSICAL ACCESS / SITE SECURITY:

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

• ANOMALIES:

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

5.4.2 Frequency of Processing Log

Audit logs are removed by trusted personnel. The system continuously monitors the available storage space and automatically sends a warning alert when storage capacity reaches 70% and a critical alert at 90%. The data is backed up onto tape media on a daily basis and labeled with a system generated barcode to support tape media inventory management. The archived media is placed in a secure container before being transferred to the offsite storage facility operated by a secure off-site storage vendor.

A copy of SSP audit logs is kept on site for reviews. The CA system is continuously monitored to provide real time alerts of significant security and operational events for review by designated system security personnel. Monthly reviews of the audit logs include verifying that the logs have not been tampered with and thoroughly investigating any alerts or irregularities detected in the logs. A statistically significant portion (typically 20%) of the security audit data generated by the SSP CA since the last review is examined. All significant events are explained in an audit log summary and any action taken as a result of the reviews is documented.

5.4.3 Retention Period for Audit Log

All electronic audit data for the SSP CAs, RAs and CSAs is collected and maintained by the SSP. The SSP has the ability to recover audit log information from on-line and archive storage. DigiCert currently retains all audit data of database records online to facilitate rapid response to audit-related issues. Audit logs are included in daily incremental and weekly full backups to facilitate recovery of the online system. Once a month, the full backup media is sent to a secure off-site facility for long-term archive storage. Deletion of the audit log from the CA equipment is performed by SSP System Operators and not by authorized operators of the certification and validation services. Access control to system logs is password based.

Audit logs are retained as archive records in accordance with section 5.5.2 of this CPS.

5.4.4 Protection of Audit Log

As a general design practice, the system audit log is not open for reading or modification by any human, or by any automated process other than those that perform audit processing. Entities that do not have modification access to the audit log may archive it. Weekly/monthly audit data is moved to a safe, secure storage location separate from the CA equipment. The DigiCert SSP currently relies on procedural (personnel and facility) controls to protect audit records from accidental or malicious overwrite or destruction. The audit data is under supervision of trusted DigiCert personnel. Data integrity is ensured through the use of a hash [Text Removed] of the image of the audit records. The hash value is stored separately from the associated audit record.

5.4.5 Audit Log Backup Procedures

The audit log is backed up on the same schedule as the rest of the data on the CA equipment. Incremental backups are produced daily. Full system backups are produced weekly.

5.4.6 Audit Collection System (Internal vs. External)

DigiCert produces audit data at the application, network and operating system level. Failure of the application level audit system is equivalent to cessation of operations inasmuch as the CA operations software is comprised in part of automated application audit functions.

Audit processes are invoked at system startup, and only cease at system shutdown.

If it becomes apparent that an automated audit system has failed, CA operations, with the exception of revocation, will cease until the audit capability is restored.

5.4.7 Notification to Event-Causing Subject

No notification is provided to an event-causing subject.

5.4.8 Vulnerability Assessments

DigiCert has instituted a multi-faceted, proactive approach to ensuring a trustworthy SSP operation.

All personnel are trained as to their responsibilities and duties with regard to secure and trustworthy conduct. Managers and supervisors provide the first level of oversight, and the DigiCert Manager of Security provides an additional oversight and enforcement role.

The DigiCert SSP has implemented a comprehensive system approach to actively detect erroneous operation of the system and to detect evidence of penetration attempts. The SSP certificate issuance and management application is designed to detect and record events that pertain to faulty or potentially insecure operation. The priority events that are logged to the error file are then examined by trusted operational personnel on a continuous basis. In addition, the SSP application performs a series of periodic self-tests to verify critical system operation. Failure of these self-tests will result in an immediate page to operations personnel to take remedial action.

The DigiCert SSP system is designed to protect itself from unauthorized access by remote users to back-end functions or data. A number of intrusion prevention and detection mechanisms are configured to primarily prevent and then capture and report on certain events that may indicate unauthorized penetration attempts. A networking intrusion detection system is used to continuously (twenty four by seven) monitor the system and to detect potentially malicious activity. The audit logs are regularly checked for events such as repeated failed actions, requests for escrowed keys, attempted access of escrowed keys, unauthenticated requests, gaps in the audit log, or other suspicious or unusual activity. Certain critical alerts, as defined in DigiCert's written procedures, will result in an immediate page and prompt response by operational personnel.

DigiCert conducts quarterly vulnerability assessments to determine its ability to protect against external network threats. DigiCert personnel, in addition to external consultants, perform this routine assessment. Finally, DigiCert datacenters described in section 5.1.2.1 undergo yearly extensive SOC 2 security audits and the CA undergoes a WebTrust audit to validate its operation in accordance with this practice documentation.

5.5 Records Archival

5.5.1 Types of Events Archived

The SSP audit process records the following information, in either paper or electronic record format, upon initialization of a CA key pair:

- CA system equipment configuration files,
- CA accreditation (if necessary),
- SSP CPS and any contractual agreements to which the CA is bound.

The following data shall be recorded for archive during CMA operation:

- CA accreditation (if applicable)
- Certificate Policy
- Certification Practice Statement
- Contractual obligations
- Other agreements concerning operations of the CA
- System and equipment configuration

- Modifications and updates to system or configuration
- Certificate requests
- All certificates issued and/or published
- Receipt and Acceptance of certificates
- Record of Re-key
- Security audit data (in accordance with Section 5.4.1)
- Revocation requests
- Subscriber identity Authentication data as per Section 3.2.3
- Subscriber agreements
- Documentation of receipt of tokens
- All CARLs and CRLs issued and/or published
- Other data or applications to verify archive contents
- Documentation required by compliance auditors
- Compliance Audit Reports
- Access to escrowed Subscriber private encryption keys
- Any changes to the Audit parameters, e.g., audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs
- Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)
- All access to certificate subject private keys retained within the CA for key recovery purposes
- All changes to the trusted public keys, including additions and deletions
- The export of private and secret keys (keys used for a single session or message are excluded)
- The approval or rejection of a certificate status change request
- Appointment of an individual to a Trusted Role
- Destruction of cryptographic modules
- All certificate compromise notifications
- Remedial action taken as a result of violations of physical security
- Violations of Certificate Policy
- Violations of Certification Practice Statement

5.5.2 Retention Period for Archive

SSP archive records, including certificates, CRLs and SSP public keys, are retained for a period of at least ten (10) years and six (6) months. Currently, all database records are retained online for immediate access. Offsite storage of full systems backups is maintained to ensure recovery of the online system in the event of a catastrophic system fault. System backups are stored at an offsite third party facility.

Media used for archiving SSP records can support the retention periods noted above.

5.5.3 Protection of Archive

The ability to write to, modify, or delete the archive is strictly controlled. A list of people authorized to modify or delete the archive is maintained. The contents of the archive are not released as a whole, except as required by law. Records of individual transactions may be released upon request of any entities involved in the transaction or their legally-recognized agents.

Archive media are only handled by trusted employees and stored in a separate, safe, secure storage facility on magnetic media. Archives are labeled with system-generated barcodes to identify the contents of the magnetic media. Associated databases provide reference to the specific CA servers and content sufficient for recovery purposes. Archive media is tested for completeness of backup and media viability on a regular basis. A manual

backup and restore operation is performed on a regular basis, usually twice a year during standard system maintenance, as verification of proper working condition.

The media used to archive SSP records can retain data for the periods specified in section 5.5.2. Applications need to recover archived records shall be maintained for the periods specified in section 5.5.2.

5.5.4 Archive Backup Procedures

A full image tape backup of the SSP system and database is prepared once a week and sent to a secure off-site storage under the control of trusted personnel. Once a month, these full image backups are sent to a secure off-site location where they are retained for the archive period specified in section 5.5.2.

5.5.5 Requirements for Time-Stamping of Records

Certificates, CRLs, revocation database entries and all archive data contain time and date information. Such time information is not cryptographic-based. See section 6.8.

5.5.6 Archive Collection System (Internal vs. External)

DigiCert archive collection systems are internal, except for RA Customers. Agent RAs are responsible for preserving their own audit trails as specified in their individual RPS.

5.5.7 Procedures to Obtain and Verify Archive Information

Procedures for creating, verifying, packaging, transmitting and storing archive information are detailed in Sections 5.4.2, 5.4.3 and 5.4.4. In the event it becomes necessary for an external party to obtain archive information, Production Services personnel, upon receipt of a duly authorized request, will produce such information. Procedures to verify the accuracy of the archived information includes a DigiCert NetBackup system that obtains the logs directly off the operating system using a secured channel and the ability to verify the integrity of the data on the tape. The system also automatically verifies the integrity of the information when it is restored.

This information will be produced from the current online data store (see Section 5.4.6) and written to magnetic media, which will be provided manually to a duly authorized agent of the external party requesting such information. For archive information not available in the current online data store, Productions Services personnel will retrieve the magnetic media containing the archive information from the offsite storage facility. The archive information will be retrieved under two-man control and provided to a duly authorized agent of the external party requesting such information.

5.6 Key Changeover

The SSP CA will use its private signature keys for signing certificates and CRLs only. CA key pairs established under this CPS will be prevented by technical means from signing subscriber certificates whose validity periods would extend beyond the expiration dates of the CA certificate's validity interval. When an SSP CA key is changed, the old SSP CA key pair will be retained and protected to issue CRLs for Subscribers that have been issued certificates signed with the old SSP CA signing key. The SSP CA does not support key rollover certificates. Key changeover of a CA requires the new certificate to be issued.

After a SSP CA performs a Key Changeover, the CA may continue to issue CRLs with the old key until all certificates signed with that key have expired. As an alternative, after all certificates signed with that old key have been revoked, the SSP CA may issue a final long- term CRL using the old key, with a nextUpdate time past the validity period of all issued certificates. This final CRL shall be available for all relying parties until the

validity period of all issued certificates has past. Once the last CRL has been issued, the old private signing key of the SSP CA may be destroyed.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

DigiCert has created and maintains business continuity plans so that in the event of a business disruption, critical business functions may be resumed. DigiCert maintains a Disaster Recovery Facility (DRF) located at a facility geographically separate from the primary Production Facility. The DRF is a hardened facility designed to federal government and military specifications and is also specifically equipped to meet DigiCert's security standards.

In the event of a natural or man-made disaster requiring permanent cessation of operations from DigiCert's primary facility, the Business Continuity Team and the DigiCert Authentication Operations Incident Management Team will coordinate with cross functional management teams to make the decision to formally declare a disaster situation and manage the incident. Once a disaster situation is declared, restoration of DigiCert's Production services functionality at the DRF will be initiated.

DigiCert has developed Disaster Recovery Plan for its Managed PKI services including the SSP PKI service. The Disaster Recovery Plan defines the procedures for the teams to reconstitute DigiCert SSP operations using backup data and backup copies of the SSP keys. The target recovery time for restoring critical Production service functionality is no greater than 24 hours.

DigiCert conducts at least one disaster recovery test per calendar year to ensure functionality of services at the DRF. Formal Business Continuity Exercises are also conducted yearly in coordination with the Business Continuity Team where procedures for additional types of scenarios (e.g. pandemic, earthquake, flood, power outage) are tested and evaluated.

DigiCert takes significant steps to develop, maintain, and test sound business recovery plans, and DigiCert's planning for a disaster or significant business disruption is consistent with many of the best practices established within the industry.

Should an incident occur that involves the Disaster Recovery or Business Continuity teams, DigiCert will post a notice on its public web page identifying the incident and provide notification to the FPKPA within 10 days of incident resolution. The public notice will include the following:

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

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

5.7.2 Computing Resources, Software and/or Data are Corrupted

If the SSP CA equipment is damaged or rendered inoperative, but the CA signature keys are not destroyed, CA operation shall be reestablished as quickly as possible, giving priority to the ability to generate certificate status information.

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

5.7.3 Entity (CA) Private Key Compromise Procedures

In the event of a CA key compromise, the DCPA shall be immediately informed, as well as the FPKIPA. The DigiCert SSP will also conduct appropriate corrective action to preclude recurrence of the causative events and report these measures to the FPKIPA. The DigiCert SSP in turn will assist in communicating the revocation of the SSP CA certificate to all relying parties by publishing a CRL.

Subsequently, the SSP will reconstitute its operation under a new PKI hierarchy using the same procedures that were performed during initial system initialization. Subscribers will be required to re-key and must repeat the initial application process. The new SSP CA certificate will be distributed as defined in section 6.1.4. DigiCert will post a notice on its web page describing the compromise. See Section 5.7.1 for contents of the notice.

In the event of the compromise of the SSP OCSP responder, the SSP shall revoke the OCSP responder certificate, add the certificate serial number to a CRL, and subsequently re-key the OCSP responder. In addition, DigiCert will notify the SSP participants and end entities as it would for CA compromise noted in section 5.7.1.

5.7.4 Business Continuity Capabilities after a Disaster

In the case of a disaster in which the primary operational set of the SSP equipment is damaged and inoperative, but the primary operational copy of a SSP CA private key is not destroyed, the SSP operations will be re-established as quickly as possible, giving priority to the ability to revoke subscribers' certificates and generate CRLs. If the SSP cannot reestablish revocation capabilities within 72 hours after the time specified in the next update field of the currently valid CRL, the FPKIPA shall be informed. Notification shall be by both e-mail and telephone.

In the case of a disaster whereby the SSP installation is physically damaged and the primary operational copy of a SSP CA signature key is destroyed as a result, the SSP will initiate certificate management operations from its Disaster Recovery site using a backup copy of the SSP CA key site giving priority to the generation of a new CA key pair if the backup pair is not available. If all copies of an SSP CA signature key are destroyed, the FPKIPA shall be notified as soon as possible.

5.8 CA or RA Termination

In the event of termination of the SSP CA, notice shall be provided to all Subscribers, SSP RAs, and the FPKI PA prior to termination. Any actions needed to ensure continued support for certificates issued by the SSP CA shall be taken in accordance with agreements with the SSP RAs. All certificates signed by the SSP CA will be revoked. The SSP Cryptographic Device Manager, when informed of SSP CA termination, shall initiate the issuance of a final long term CRL with a nextUpdate time past the validity period of all issued certificates. This final CRL shall be available for all relying parties until the validity period of all issued certificates has passed. After the final CRL has been issued, the private signing key of the SSP CA will be destroyed.

Dissemination of revocation notice will be achieved as discussed in CPS sections 5.7.1 and 5.7.3.

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

In the event of termination of an SSP RA, the RA certificate shall be revoked and the RA shall provide all archived data to the archival facility specified by DigiCert. DigiCert shall continue to retain all archive data for the terminated CA/RA in accordance with section 5.5.2.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Key pairs are generated in such a way that the private key is not known by anyone other than the authorized user of the key pair. Private keys do not appear outside of the modules in which they are generated unless encrypted for local transmission or for processing or storage by a key recovery mechanism.

6.1.1.1 CA Key Pair Generation

SSP CA and CSA key pairs are generated within DigiCert's secure Key Ceremony room on hardware tokens. The ceremony is recorded and a full audit record is created to ensure that all security requirements, including separation of roles were followed. Key ceremonies must be performed under dual control of a Key Ceremony Administrator and another independent trusted employee as a witness. The audit record identifies any failures or anomalies in the key generation process, and any corrective action taken. At no time does the SSP CA or CSA private key appear in plain-text form outside the hardware protection boundary of the hardware token. CA and CSA certificate signing keys are generated in FIPS 140 Level 3 validated cryptographic hardware modules. The corresponding key ceremony documentation is reviewed by an independent third party on an annual basis.

6.1.1.2 Subscriber Key Pair Generation

Subscriber key pairs for Signature certificates are generated on the subscriber's local system, and Subscriber key pairs for encryption certificates are generated by the Key Management System. At no time does the subscriber private key appear in plain-text form outside the hardware protection boundary of the cryptographic module. DigiCert RA and Organization RA keys are generated in a FIPS 140 Level 2 validated cryptographic module.

DigiCert SSP uses validated FIPS 140 software or hardware cryptographic modules to generate all subscriber key pairs, as well as pseudo-random numbers and parameters used in key pair generation. Any pseudo-random numbers used for key generation material shall be generated by a FIPS-approved method. Symmetric keys may be generated by means of either software or hardware mechanisms.

For *id-stn-ssp-basic, id-stn-ssp-medium* or *id-stn-ssp-mediumDevices* certificates, Subscriber signature key pairs are generated in a FIPS 140 Level 1 cryptographic module (i.e., browser software).

For *id-stn-ssp-pivi-hardware,* used for digital signature and/or authentication, and *id-stn-ssp-pivi-cardAuth*, Subscriber key pairs are generated in a hardware token that meets the requirements of a PIV-I Card as described in Appendix C. For all other certificates issued at the Medium Hardware assurance level, including *id-stn-ssp-mediumHardware* and *id-stn-ssp-mediumDevicesHardware,* Subscriber signature key pairs are generated in a FIPS 140 Level 2 cryptographic hardware module and may not be exported from the module that generated the key pairs (e.g., smart card).

For *id-fpki-common-piv-contentSigning* certificates are generated on a validated FIPS 140 Level 2 or 3 hardware cryptographic module. For PIV issuing systems or devices that sign PIV objects on PIV cards that contain certificates that assert *id-fpki-common-High*, the module(s) must meet or exceed FIPS 140 Level 3. For all other PIV issuing systems or devices, the module(s) must meet or exceed FIPS 140 Level 2.

6.1.2 Private Key Delivery to Subscriber

Subscriber private keys are delivered as follows:

Hardware Credential

Key generation for authentication certificates stored on smart cards is performed on the hardware secure module. The private key never leaves the cryptographic boundary of the hardware secure module, and thus, there is no need to deliver the Subscriber's private key. The hardware secure modules is in the possession of the Organization RA until the Subscriber accepts possession of it. The Subscriber acknowledges receipt of the hardware secure modules.

Private Encryption keys hardware secure modules are generated in anOrganization hosted Key Manager which delivers the keys to the issuance system for downloading to the Subscriber's hardware secure module. A PKCS#12 file is downloaded to the RA's workstation where it is decrypted by the card management software and injected into the hardware secure module. After the private Encryption key is injected into the hardware secure modules, the PKCS#12 file and password are erased by the card management software.

For issuance of a PIV-I credential, the RA shall activate and release the PIV-I Card to the subscriber only after a successful 1:1 biometric match of the applicant against the biometrics collected in Section 3.2.3.1.

Software Credential

Private Signature keys associated with software certificates are generated and stored in software cryptographic modules (FIPS 140 Level 1 web browser certificate cache or other comparable certificate store). The Signature key pair will be generated in and remain within the cryptographic boundary of the cryptographic module. Since the owner generates the Signature key pair locally, there is no need to deliver the Subscriber's private key.

Private encryption keys associated with software certificates are generated in hardware cryptographic modules and escrowed by the Organization hosted Key Manager. Immediately after escrowing of the private Encryption keys, all keying material is deleted from the Key Manager cryptographic module. Subscribers download the private encryption keys in a server-side SSL-protected session using a cryptographic algorithm and key size at least as strong as the private key in accordance with section 6.1.5. The private encryption keys are delivered in a PKCS#12 format to the Subscriber via the SSL-protected session. After the Subscriber successfully enters the PIN and password, the PKCS#12 file is downloaded to the Subscriber's workstation where it is decrypted by the browser and stored in the browser's cryptographic module.

6.1.2.1 Acknowledgement of Private Key Delivery

When CAs or RAs generate keys on behalf of the Subscriber, Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases the following requirements must be met:

- Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key after delivery of the private key to the Subscriber;
- The private key must be protected from activation, compromise, or modification during the delivery process;
- The Subscriber shall acknowledge receipt of the private key(s); and
- Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers:
    - For hardware modules, accountability for the location and state of the module must be maintained until the Subscriber accepts possession of it.

- For electronic delivery of private keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data shall be delivered using a separate secure channel.

The CA or RA shall maintain a record of the Subscriber acknowledgement of receipt of the token.

In only certain cases as noted in section 3.2.3.3, the SSP PKI will support several entities acting in one capacity and will allow multiple end users to share a group Certificate and associated private key. Such certificates will indicate a group or organizational name in the Subject of the certificate and will not set the *nonRepudiation* bit. Such Certificates will have a custodian identified who will act as the primary Subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

The Subscriber's identity information and public key are securely delivered to the certificate issuer as follows.

Hardware Credential
The Subscriber's identity information and public key are delivered from the smart card issuance system to the SSP CA in an encrypted format using the CSR (PKCS#10) protocol over https.

Software Credential
The Subscriber's identity information and public key are delivered in a certificate signing request to the SSP CA over an SSL-protected session. The format for the delivery of this data is dependent on the type of web browser used. For all browser types, the public key is signed by the corresponding private key as the mechanism to prove possession of the private key.

6.1.4 CA Public Key Delivery to Relying Parties

Non-Federal SSP CA certificates shall be delivered to users and relying parties by downloading the certificates from a web site secured with a web server certificate. Relying Parties will be required to compare the CA Certificate hash against the hash value received from a Trusted Agent, DigiCert RA or Organization RA. Alternatively, these certificates may be imported onto the Subscriber smart card at the time of certificate enrollment by the Organization RA.

6.1.5 Key Sizes

Signature algorithms shall conform to RSA PKCS#1. All end-entity certificates associated with PIV-I shall contain public keys and algorithms that conform to NIST SP 800-78. CSAs shall sign responses using the same signature algorithm, key size, and hash algorithm used by the CA to sign CRLs. Key sizes and hash algorithms are detailed below:

- The key pairs for the SSP CAs that expire before 12/31/2030 are 2048-bit RSA key pairs and those that expire after 12/31/2030 shall be at least 3072 bit RSA or 256 bits for elliptic curve algorithms.
- The key pairs for the Non-Federal SSP CAs, including the Non-Federal SSP Intermediate CAs and the Non-Federal Entity SSP CAs that expire before 12/31/2030 are 2048-bit RSA key pairs and those that expire after 12/31/2030 shall be at least 3072 bit RSA or 256 bits for elliptic curve algorithms.
- The key pairs for all end entity certificates are at least 2048-bit RSA key pairs.
- All Non-Federal SSP CAs, including the Non-Federal SSP Intermediate CAs and the Non-Federal Entity SSP CAs shall use SHA-256 for digital signature. Signatures on certificates and CRLs shall be generated using SHA-256.

- SSP CA-issued Transport Layer Security (TLS) or Secure Socket Layer (SSL) certificates use AES (128 bits) for symmetric keys and 2048 bit RSA for asymmetric keys.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters
Prime numbers for use with the RSA algorithm defined in [PKCS-1] shall be generated and checked in accordance with [PKCS-1].

Parameter Quality Checking
Public key parameters for signature algorithms defined in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186. Parameter checking (including primarily testing for prime numbers) shall be performed in accordance with FIPS 186-4.

6.1.7 Key Usage Purposes (as per x509v3 field)

The SSP CA shall issue client Signature certificates with the key usage extension for signing and client authentication and issue encryption certificates with the key usage extension for encryption.

Domain controller certificates are the only certificates enabled with both signing and encryption functionality. Subscriber certificates that assert *id-stn-ssp-rudimentary* are single key and assert only the *digitalSignature* bit.

Subscriber certificates that assert *id-stn-ssp-basic* may be single key for use with encryption and signature in support of legacy applications . Such dual use certificates are not used for authenticating data using the dual use certificate at a future date.

Public keys that are bound into human subscriber certificates that assert *id-stn-ssp-medium* or *id-stn-ssp-mediumHardware* are used only for signing or encrypting, but not both. Subscriber certificates to be used for digital signatures assert the *digitalSignature* and *nonRepudiation* bits. Certificates to be used for key transport assert the *keyEncipherment* bit. When the subject public key of a certificate is used for key agreement, the certificate asserts the *keyAgreement* bit. Shared Group Certificates used for authentication do not assert the *nonRepudiation* bit.

Subscriber certificates that assert *id-stn-ssp-pivi-hardware* are used only for signing or encrypting, but not both. The PIV-I Authentication certificate type only assert the *digitalSignature* bit while the PIV-I Digital Signature certificate type assert both the *digitalSignature* and *nonRepudiation* bits.

Subscriber certificates that assert *id-stn-ssp-pivi-cardAuth* and *id-stn-ssp-pivi-contentSigning* include a key usage extension and assert only *digitalSignature* bit.

For Subscriber certificates issued after June 30, 2019, the Extended Key Usage extension is always present and does not contain *anyExtendedKeyUsage* {2.5.29.37.0}. Extended Key Usage OIDs are consistent with key usage bits asserted.

If a certificate is used for authentication of ephemeral keys, the Key Usage bit in the certificate asserts the *digitalSignature* bit and may or may not assert *keyEncryption* and *keyAgreement* depending on the public key in the certificate.

PIV-I Content Signing certificates include an extended key usage of *id-fpki-pivi-content-signing.*

Public keys that are bound into the SSP CA certificates are used only for signing certificates and status information (e.g., CRLs). SSP CA certificates whose subject public key is to be used to verify other certificates

asserts the *keyCertSign* bit. SSP CA certificates whose subject public key is to be used to verify CRLs assert the *cRLSign* bit. For SSP CA certificates used to verify both certificate and CRLs, both the *keyCertSign* and *cRLSign* bits are asserted. CSA certificates whose subject public key is to be used to verify Online Certificate Status Protocol (OCSP) responses assert the *digitalSignature* and/or *nonRepudiation* bits.

Public keys that are bound into device certificates are used for signing, encrypting, or both. Device certificates to be used for digital signatures (including authentication) assert the *digitalSignature* bit. Device certificates that contain RSA public keys that are to be used for key transport assert the *keyEncipherment* bit. Device certificates do not assert the *nonRepudiation* bit.

The *dataEncipherment*, *encipherOnly*, and *decipherOnly* bits are not asserted in certificates issued per this CPS. All certificates meet the certificate profiles defined in Appendix A.

6.2 Private Key Protection & Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

All cryptographic modules shall meet the requirements of FIPS 140, Security Requirements for Cryptographic Modules.

SSP Subscribers utilizing software-based cryptographic modules (*id-stn-ssp-basic*, *id-stn-ssp-medium*, *id-stn-ssp-mediumDevices*) are obligated to use cryptographic modules that meet at least the criteria for FIPS 140 Level 1 for all cryptographic operations.

SSP Subscribers utilizing hardware-based cryptographic modules (*id-stn-ssp-mediumHardware, id-stn-ssp-mediumDevicesHardware, id-stn-ssp-pivi-hardware*, or *id-stn-ssp-pivi-cardAuth*) are obligated to use cryptographic modules that meet at least the criteria for FIPS 140 Level 2 hardware for all cryptographic operations.

PIV-I Cards are PKI tokens that have private keys associated with certificates asserting the *stn-ssp-pivi-hardware* or *stn-ssp-pivi-cardAuth* policy. PIV-I Cards shall only be issued using card stock that has been tested and approved by the FIPS 201-2 Evaluation Program and listed on the GSA Approved Products List (APL). Card stock that has been removed from the APL may continue to be issued for no more than one year after GSA approved replacement card stock is available. PIV-I cards issued using the deprecated card stock may continue to be used until the current subscriber certificates expire, unless otherwise notified by the FPKIPA/FPKIMA. On an annual basis, for each PCI configuration used (as defined by the FIPS 201-2 Evaluation Program), one populated, representative sample PIV-I Card shall be submitted by the RA to the FIPS 201-2 Evaluation Program for testing.

A comprehensive list of requirements for PIV-I smart cards is provided in Appendix C.

The DigiCert SSP RA and Organization RAs workstations shall use cryptographic modules that meet at least the criteria for FIPS 140 Level 2 for all cryptographic operations.

The SSP CA and CSA shall use a (minimum) FIPS 140 Level 3 hardware cryptographic module.

All cryptographic modules dedicated to management of DigiCert SSP certificate signing key pairs are operated such that the private asymmetric cryptographic keys are never output in plain-text.

The SSP RA key and certificates are contained on FIPS 140 Level 2 hardware cryptographic tokens. The RA function, either performed by DigiCert or an Organization RA, is physically separated from the SSP CA which is located within the DigiCert datacenters described in section 5.1.2.1.

6.2.1.1 Custodial Subscriber Key Stores

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

Cryptographic modules for Custodial Subscriber Key stores at the Rudimentary Assurance Level shall be no less than FIPS 140 Level 1 (Hardware or Software). For all other levels, the cryptographic module shall be no less than FIPS 140 Level 2 Hardware.

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

6.2.2 Private Key Multi-Person Control

Both the operational and backup versions of SSP private keys are subject to multi-person control for activation of the hardware token containing the private key.

When SSP certificate signing key pairs are generated in DigiCert's Key Ceremony rooms in 5.1.2.3, the PIN required to activate the associated hardware token is also generated automatically and is composed of a large random value. This value is automatically decomposed into multiple shares in a 3-of-16 secret sharing scheme. These shares are written to magnetic media and distributed individually to trusted employees (see Section 6.4 Activation Data for additional detail). The names of the parties holding the secret shares shall be maintained and made available for inspection during compliance audits.

Once the token is so initialized, the key pair generated and the associated CA certificate signed by its superior CA, the token is ultimately moved to a separate Secure Data Center room for activation into an operational state. Activation of the token requires the personal presence of a designated quorum of shareholders established during the Key Ceremony (i.e., 3 of 16). Each shareholder presents his or her value to the system intended to activate and use the token. After a quorum of such values is collected, this system automatically reconstitutes the PIN value.

6.2.3 Private Key Escrow

6.2.3.1 Escrow of CA private signature key

CA private keys are not escrowed.

6.2.3.2 Escrow of CA encryption keys

CA private keys are not escrowed.

6.2.3.3 Escrow of Subscriber private signature keys

Subscriber private signature keys are not escrowed.

6.2.3.4 Escrow of Subscriber Private Encryption and Dual Use Keys

The SSP provides key escrow and key recovery services for SSP Subscriber private encryption keys through the respective RA agencies that access it through the Key Manager system. The public/private key pair for Subscriber encryption certificates is generated locally in a Key Manager System (KMS) which is hosted at the Organization facility. The private keys are stored [Text Removed] in a database associated with the Key Manager. The key recovery process and procedures are described in the RPS maintained by Agency RAs.

The SSP does not provide key escrow for dual use keys. If a device has a separate key management key certificate, the key management private key may be escrowed.

The information needed to decrypt the private encryption key resides in a database stored at DigiCert. DigiCert trusted personnel do not have access to the encrypted private keys.

6.2.4 Private Key Backup

6.2.4.1 Backup of Entity CA Private Signature Key

Backup copies of the SSP CA and CSA private keys are made to facilitate disaster recovery. These copies are maintained in secure facilities and are subject to the same access control policies and practices established for the operational copy. Because of the high availability configuration of the SSP CA (i.e. redundant hot-standby systems at both the primary data center and the Disaster Recovery site, DigiCert maintains a total of four (4) copies of the SSP CA and CSA private keys. There is no need to back up RA private keys because the RA key is not used to sign any data. In the SSP, the RA key/certificate is only used for access control to the SSP CA.

Backup copies of the SSP CA key pair are made during the original key ceremony process using a secure process specifically designed for cloning of key pairs. The hardware tokens DigiCert deploys for these purposes enable strong cryptographic authentication of a recipient token as a legitimate token to receive a backup copy. Once this authentication is established, the program DigiCert uses to control the process will activate the source token and the destination token to create a one-time shared [Text Removed] encryption key, which is used to protect the private key while in transit from the source token to the destination token. The value of this encryption key is known only to the tokens themselves. It is never exposed to the software that controls the process.

6.2.4.2 Backup of Subscriber Private Signature Key

SSP subscribers are obligated to prevent unauthorized disclosure of their private keys. This includes any means undertaken to establish a backup copy of their keys in support of disaster recovery. The SSP provides escrow of subscriber private Encryption keys, but Subscriber private Signature keys are never escrowed.

Subscriber private signature keys whose corresponding public key is contained in a certificate asserting any of the following policies may not be backed up or copied:

- *id-stn-ssp-pivi-hardware*
- *id-stn-ssp-pivi-cardAuth*
- *id-stn-ssp-pivi-contentSigning*
- *id-stn-ssp-mediumHardware*
- *id-stn-ssp-mediumHardware-CBP*
- *id-stn-ssp-mediumDevicesHardware*

Subscriber private signature keys whose corresponding public key is contained in a certificate that does not assert any of the above listed policies may be backed up or copied. Such private signature keys stored in a FIPS 140 Level 2 cryptographic module may be backed up to another FIPS 140 Level 2 cryptographic module that is held in the Subscriber's control. Such private signature keys stored in a FIPS 140 Level 1 software cryptographic module may be backed up using the mechanism provided by the cryptographic module (usually a web browser with PKCS #12 export capability).

6.2.4.3 Backup of Subscriber Key Management Private Key

DigiCert SSP subscribers are obligated to prevent unauthorized disclosure of their private keys. This includes any means undertaken to establish a backup copy of their keys in support of disaster recovery ensuring security controls consistent with the protection provided by the subscriber's cryptographic module. Backup private key management keys shall not be stored in plain text form outside the cryptographic module.

6.2.4.4 Backup of CSS Private Key

See 6.2.4.1.

6.2.4.5 Backup of PIV-I Content Signing Key

The CMS shall create backup copies of the PIV-I Content Signing private signing keys under multi-person control to facilitate disaster recovery. These copies are maintained in secure facilities and are subject to the same access control policies and practices established for the operational copy. Backup copies of the PIV-I Content Signing private signing key pair are made during the original key generation process using a secure process specifically designed for cloning of key pairs. Backup procedures are documented in the RPS of the respective RA.

6.2.4.6 Backup of Device Private Keys

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

6.2.5 Private Key Archival

CA private Signature keys and Subscriber private Signature keys are not archived. The DigiCert SSP provides escrow of Subscriber private Encryption keys. See Section 6.2.3 and Section 6.2.4 for additional details.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

When the SSP makes a backup copy of the SSP CA private key, the key is transferred to hardware token in encrypted form. At no time does the key exist in plaintext form outside the hardware protection boundary. Private keys for RAs are generated by and within a FIPS 140 Level 2 cryptographic module. RA private keys never exist in plaintext form outside of the boundary of the cryptographic module.

Subscribers whose certificates do not assert the *id-stn-ssp-pivi-hardware*, *id-stn-ssp-pivi-cardAuth*, *id-stn-ssp-mediumHardware* or *id-stn-ssp-mediumDevicesHardware* policy may use the secure export/import capability in the latest versions of the browsers that support PKCS #12 to transfer keys and certificates via the PKCS#12 protocol.

6.2.7 Private Key Storage on Cryptographic Module

Private keys are stored in software or hardware cryptographic modules is accordance with section 6.2.1.

6.2.8 Method of Activating Private Keys

The SSP CA and CSA hardware tokens utilize a PIN-based activation mechanism. This PIN is generated during initialization of the token and split into shares for use in multi-party access control. Activation data is changed upon re-key.

SSP subscribers are obligated to select a password or PIN during key generation. Entry of the password or PIN is required to activate the private key whose corresponding public key is contained in a certificate asserting the *id-stn-ssp-medium*, or *id-stn-ssp-mediumHardware* policy object identifier. When pass-phrases or PINs are used, they shall be a minimum of six (6) characters. The subscriber is the only entity that knows the password; at no time does the SSP become aware of the subscriber's password. The subscriber shall protect the entry of activation data from disclosure. Similarly, the RA is the only entity that knows the password for the RA hardware token.

SSP subscribers for *id-stn-ssp-pivi-hardware* are obligated to select a password or PIN to activate the PIV-I Card. For id-*stn-ssp-pivi-hardware*, in the event that activation data must be reset a successful biometric 1:1 match of the requester against the biometrics collected in Section 3.2.3.1 is conducted by the RA.

For certificates issued asserting *id-stn-ssp-pivi-cardAuth*, *id-stn-ssp-mediumDevices* and *id-stn-ssp-mediumDevicesHardware,* subscriber activation is not required to use the associated private key.

For certificates issued under the *id-stn-ssp-mediumDevices* and *id-stn-ssp-mediumDevicesHardware*, the device may be configured to activate its private key without requiring its human sponsor or authorized administrator to authenticate to the cryptographic token, provided that appropriate physical and logical access controls are implemented for the device and its cryptographic token. The strength of the security controls shall be commensurate with the level of threat in the device's environment and shall protect the device's hardware, software, and the cryptographic token and its activation data from compromise.

For certificates issued asserting *id-stn-ssp-pivi-contentSigning*, key activation requires multi-party control as stipulated in section 5.2.2.

PIV-I Cards may support card activation by the CMS to support card personalization and post-issuance card update. To activate the card for personalization or update, the CMS shall perform a challenge response protocol using cryptographic keys stored on the card in accordance with [SP800-73].

When cards are personalized, card management keys shall be set to be specific to each PIV-I Card. That is, each PIV-I Card shall contain a unique card management key. Card management keys shall meet the algorithm and key size requirements stated in Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification [SP800-78].

6.2.9 Method of Deactivating Private Keys

The SSP CA and CSA hardware tokens are operated in a secure data center within an access-controlled secure facility. Access to the data center is strictly controlled. The token will deactivate its private key upon removal from its reader. When not in use, the token is stored in a vault. RA tokens are deactivated by removing them from the RA workstation.

Subscriber smart cards are automatically deactivated after a time out period or by removing them from the smart card reader.

6.2.10 Method of Destroying Private Keys

Private signature keys shall be destroyed when they are no longer needed or when the certificates to which they correspond expire or are revoked. In the event the SSP CA or CSA private key requires destruction, the hardware token's "zeroize" command will be performed by individuals in trusted roles to do so. In the event the RA private key requires destruction, the RA token "initialize" command is used by individuals in trusted roles to zeroize the private key. In the event the Subscriber's private key stored on a smart card requires destruction, the Organization RA may re-initialize the card to zeroize the private key.

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

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

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The key usage periods for keying material are described in Section 3.3.1 and Section 5.6. The usage period for a SSP CA key pair is a maximum of ten (10) years. The SSP CA private key may be used to sign certificates for at most four (4) years. The SSP CA private key may be used to sign CRLs and OCSP responder certificates for the entire usage period.

Subscriber public keys and private keys have a maximum usage period of three (3) years. The usage period for Subscriber key management keys is not restricted. The SSP CA shall not issue subscriber certificates that extend beyond the expiration date of their own certificate and public keys.

Subscriber public keys in certificates that assert *id-stn-ssp-pivi-contentSigning* OID in the extended key usage extension have a maximum usage period of eight (8) years. The private keys corresponding to the public keys in these certificates have a maximum usage period of three (3) years.

PIV-I Cards shall have an expiration date not to exceed 6 years of issuance. PIV-I Subscriber certificate expiration shall not be later than the expiration date of the PIV-I hardware token on which the certificates reside. Expiration of the PIV-I Card shall not be later than expiration of PIV-I Content Signing certificate residing on the card.

OCSP Responder certificates that provide revocation status for PIV-I have a maximum certificate validity period of 30 days.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

SSP subscribers are requested to select their own password/PIN with an appropriate level of strength to protect their private key.

RAs are also required to choose their own PINs with an appropriate level of strength to protect their private key. The PIV-I Content Signing key pairs shall be generated by an operating system component of the CMS as

described in Appendix B and put on a FIPS 140-2 Level 2 Cryptographic Module and conform to [NIST SP 800-78] requirements, including PIN generation requirements to protect the PIV-I content signing private key. The PINs used to protect the SSP CA and CSA tokens are randomly and automatically generated. Activation data protecting access to the SSP CA hardware token is generated within the FIPS 140 certified cryptographic module. The activation PIN is 384 bits and is split into several shares using the n-of-m scheme as described in Section 6.2.2.

6.4.2 Activation Data Protection

The SSP CA and CSA activation data PINs are split into 16 shares, each portion of which is written to a separate non-volatile storage medium (hardware token). Shares are provided to designated trusted employees, one share per employee. 3 of 16 shares are required to reconstitute a PIN. Each trusted employee maintains a separate safe deposit box where the share under their control is stored when not in use. Individuals only hold one of the two keys needed to unlock the safe deposit box. The safe deposit boxes are stored inside a 3 number combination safe, which is maintained inside a two man controlled area. Since shares are stored electronically, at no time is the value of a share, or the PIN, able to be written down. The SSP CA and SSP CSA PINs are only changed at key changeover.

CA and RA keys are stored on FIPS 140 tokens which are locked after a pre-determined number of unsuccessful PIN entries. Subscriber keys which are stored on FIPS 140 tokens are locked after a pre-determined number of unsuccessful PIN entries. The RA and Subscriber activation PINs are only known by the holder of the token.

6.4.3 Other Aspects of Activation Data

See Section 6.4.1.

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

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The SSP CA and CSA and Virtual Machines employ an operating system that has been evaluated for security functionality, including audit requirements, identification and authentication, domain integrity enforcement, and discretionary access controls. [Text Removed]

The SSP operator accounts are implemented to provide individual I&A. The SSP has instituted sufficient system level and procedural controls to be able to effectively determine which authorized and trusted individual performed a security sensitive event. [Text Removed]

Security critical cryptographic processes are implemented on dedicated servers physically segregated from other system components. Key ceremonies for CA key generation are performed on off-line dedicated servers not connected to the system network. Recovery from a key or system failure is facilitated by automatic failover to a redundant, load-balanced system.

6.5.2 Computer Security Rating

[Text Removed]

[Text Removed]

The DigiCert SSP implements system-level controls that provide for identification and authentication, discretionary access controls, and audit of security critical events.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Software applications for the SSP CA, RA and CSA are developed in-house in a controlled environment in accordance with DigiCert systems development and change management procedures. There is a formal process by which features or enhancements are introduced into the software. A change/enhancement request is first logged in a commercially available defect/feature tracking system. Software is then developed or modified to implement the request. All software has revision controls and changes are not implemented or merged into the software for testing until the code for the change has been reviewed and approved by the product development manager. The process is enforced by a proprietary build change control tool.

DigiCert developed software when first loaded, provides a method to verify that the software originated from DigiCert, has not been modified prior to installation, and is the version intended for use. Procured SSP, RA and CSA software, when first loaded, is verified as being that supplied by the vendor, with no modifications, and the correct version.

The CA hardware and software, including the VME hypervisor, shall be dedicated to operating and supporting the CA. (i.e., the systems and services dedicated to the issuance and management of certificates). There are no other applications, hardware devices, network connections, or component software installed that are not parts of the CA operation. Where the CA operation supports multiple CAs, the hardware platform may support multiple CAs. In a VME, a single hypervisor may support multiple CAs and their supporting systems, provided all systems have comparable security controls and are dedicated to the support of the CA.

In a VME, all VM systems must operate in the same security zone as the CA.

6.6.2 Security Management Controls

Equipment (hardware and software) procured to operate the DigiCert CA, RA and CSA is purchased in a fashion to reduce the likelihood that any particular component was tampered with, such as random selection. Intended use of procured hardware and software is never indicated on order forms/paperwork.

For all cryptographic hardware a verifiable chain of custody is maintained through all life cycle stages including: procurement, transportation, equipment receipt, physical storage and acceptance testing, key generation ceremony, allocation and destruction, and storage. Cryptographic equipment is always handled by two trusted employees (dual control). All cryptographic hardware whether designated for SSP operational or customer use is procured and handled by trusted employees of the DigiCert PKI Operations (PKI Ops) organization. PKI Ops tracks all cryptographic hardware using a unique serial number. All cryptographic hardware is transported in tamper evident packaging that is double-wrapped and shipped via a commercial shipping service with automated tracking. All double wrapped packages are inspected upon receipt for signs of tamper/neglect. Any cryptographic hardware that is received unsealed in a tamper evident package is deemed compromised. All testing of newly purchased, un-initialized cryptographic hardware is performed by two trusted employees, neither of whom has unescorted access to the secure cryptographic storage areas. After successful acceptance testing, all cryptographic hardware is stored in tamper evident envelopes in a six-tier secure storage area.

CA and CSA equipment is dedicated to the specific function of administering a PKI. The configuration of CA and CSA systems, as well as any modifications and upgrades, is documented. No application or component software is installed on the CA and CSA system that is not part of CA or CSA configurations. The systems have a capability installed and operating to detect unauthorized modifications to CA and CSA software or configurations.

Only authorized IT personnel, known as CMS Administrators, are given administrator privileges to install software on RA equipment. The installation and setup of software and hardware for Organization RAs is performed by CMS Administrators. Only applications required to perform the RA functions is loaded on RA computers, and all such software is obtained from sources authorized by the SSP. Virus scanning software is installed on all RA equipment. Scans are conducted on first use and periodically afterward.

Equipment updates are purchased or developed in the same manner as original equipment, and are installed by trusted and trained personnel in a controlled and audited manner.

6.6.3 Life Cycle Security Controls

See section 6.6.1.

6.7 Network Security Controls

The SSP is designed to mitigate risk to external threats. Filtering at the routers is based on destination IP address and services. Firewalls use packet filtering and stateful inspection. The DMZ is segregated, with multiple firewalls internal and external to the DMZ. Communications with subscribers are encrypted using TLS protocol. All communications between the Organization RA and the SSP are via an TLS session with certificate-based access control. All communications between the organization-hosted KMS and the SSP and optionally the DigiCert-hosted KMD are secured [Text Removed].

[Text Removed] The DigiCert SSP firewall is configured such that all unused ports and services are turned off, only required user accounts are present and only required network services software is installed.

Security monitoring is performed on the firewalls and critical servers. Throughout the day, automated scripts that test network response time, application status and application response times are run. Results are stored on a central logging host. Each shift has personnel who is responsible for the first-line response in the event of system problems. Automated scripts notify Operations personnel if script results exceed specified parameters. Text messages describing the problem are sent to Operations personnel. Daily system management statistics detailing disk and CPU usage, system load statistics, and system uptime are stored centrally. These records are maintained for the current and prior month.

Security monitoring tools used include:

- Commercial security management products used for [Text Removed]
- Security monitoring tools on the [Text Removed], including but not limited to:
  - [Text Removed], for configuration management
  - Security audit scripts that log password hashes, for verifying password strength
  - [Text Removed], for checking file integrity and malicious code detection
  - [Text Removed], for controlling access to [Text Removed] network services
- Security monitoring tools on the network, including but not limited to:
  - [Text Removed] for scanning for network issues
  - [Text Removed] for network intrusion detection.
- Security monitoring tools [Text Removed], including but not limited to:
  - Virus scanners.

6.7.1 Network Security Controls for PIV-I CMS Equipment

CMS equipment shall be located on internal networks behind boundary/perimeter network defenses and shall implement network security controls and protections consistent with commercial best practices for network security. Functions on CMS equipment shall be limited to those required to perform CMS functions. A firewall shall be used to protect the network on which the CMS equipment is hosted. The firewall shall provide for audit of security events and protection of the security audit log. Networking equipment shall turn off unused network ports and services. Any network software present shall be necessary to the functioning of the equipment.

6.8 Time-Stamping

A DigiCert time server, synchronized via Global Positioning Service to the Coordinated Universal Time is accurate to within one (1) second.

7. CERTIFICATE, CRL AND OCSP PROFILES

Appendix A contains the formats for the various certificates and CRLs.

7.1 Certificate Profile

7.1.1 Version Number(s)

SSP shall issue X.509 Version 3 certificates only.

7.1.2 Certificate Extensions

The SSP uses the certificate profiles as described in this CPS. These profiles, which are based on the FPKI X.509 Certificate and CRL Extensions Profile comply with RFC 5280. PIV-I certificate profiles also comply with the X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards. No private critical extensions are included in certificates issued by the SSP.

7.1.3 Algorithm Object Identifiers

Certificates under this CPS will use the following OIDs for signatures:

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
ecdsa-with-SHA256	{iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2 (3) 2 }

Certificates under this CPS will use the following OIDs for identifying the algorithm for which the subject key was generated.

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

Where certificates issued contain an elliptic curve public key, the parameters shall be specified as one of the following named curves:

ansip256r1	{ iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7 }
ansip384r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 34 }

Signature algorithms for PIV-I credentials are limited to those identified by NIST SP 800-78.

The SSP shall certify only public keys associated with the crypto-algorithms identified above, and shall only use the signature crypto-algorithms described above to sign certificates, certificate revocation lists and any other PKI product, including other forms of certificate status information such as OCSP.

7.1.4 Name Forms

The subject and issuer fields in all SSP certificates issued shall be populated with an X.500 Distinguished Name, with the attribute type as further constrained by RFC 5280.

The issuer field of certificates issued under the policies in this document shall be populated with an X.500 Distinguished Name, with the attribute type as further constrained by RFC 5280.

In the *id-stn-ssp-pivi-cardAuth* and *id-stn-ssp-pivi-authentication* certificates, the subject alternative name extension shall be present and include the UUID name form.

id-stn-ssp-rudimentary certificates shall populate the subject field or subject alternative name extension per Section 3.1.1 with the attribute type as further constrained by RFC 5280.

7.1.5 Name Constraints

The SSP does not enforce name constraints; however, RAs are limited to the jurisdictional name space assigned to their RA domain.

7.1.6 Certificate Policy Object Identifier

Certificates issued by the SSP CA shall assert one or more of the OIDs as defined in Section 1.2.

7.1.7 Usage of Policy Constraints Extension

The SSP does not enforce policy constraints.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued by the DigiCert SSP shall not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Certificates issued by the SSP CA shall not contain a critical certificate policy extension.

7.1.10 Inhibit Any Policy Extension

Certificates issued by the SSP CA shall not contain an InhibitAnyPolicy extension in CA certificates.

7.2 CRL Profile

CRLs issued by the Non-Federal SSP CA shall conform to the CRL profile specified in X.509 Certificate and CRL Extensions Profile or where applicable with PIV-I certificate profiles also comply with the X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards.

7.2.1 Version Number(s)

CRLs issued under this CPS will be X.509 version 2 CRLs. The Non-Federal SSP CA will not issue Authority Revocation Lists (ARLs) or any other partitioned CRLs.

7.2.2 CRL and CRL Entry Extensions

The Non-Federal SSP CA shall issue CRLs that comply with the extensions specified in the CRL profiles detailed in X.509 Certificate and CRL Extensions Profile or where applicable with PIV-I certificate profiles also comply with the X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards.

7.3 OCSP Profile

Non-Federal SSP CSAs shall sign responses using algorithms designated for CRL signing.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The DCPA shall be responsible for ensuring audits are conducted for all PKI functions regardless of how or by whom the PKI components are managed and operated. DigiCert and its RAs are subject to an annual review by the FPKIPA to ensure their policies and operations remain consistent with the policy mappings in the certificate issued to DigiCert by the FBCA.

8.1 Frequency or Circumstances of Compliance Audit

The SSP CA, CSA and RA shall undergo an annual compliance audit as part of the DigiCert annual PKI audit. The organization RA and CMS shall undergo an annual compliance audit. This audit will be a period-of-time audit performed between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. Compliance audits shall be conducted in accordance with the *FPKI Annual Review Requirements* document located at https://www.idmanagement.gov/fpki-cas-audit-info/.

8.2 Identity/Qualifications of Reviewer

The auditing team shall have extensive experience in all relevant matters of physical, personnel, technical, and logical security. Specifically, the compliance audit team shall have at least five (5) years experience performing PKI compliance audits.

The Organization PMA is responsible for identifying and engaging a qualified auditor of its operations implementing aspects of this CPS with the following qualifications:

- Demonstrated competence in the field of compliance audits, and familiar with the CMS requirements in this CPS and the corresponding requirements in the FBCA CP.
- Perform such compliance audits as their regular ongoing business activity.
- Be a certified information system auditor (CISA) or IT security specialist. The compliance auditor must be a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

8.3 Assessor's Relationship to Audited Party

The SSP auditor is under a contractual relationship to DigiCert for its security audit services and has no role or responsibility relating to the SSP operation. The Organization RA and/or CMS auditor shall be an independent organization[10] engaged under a contractual relationship for audit services and may not have any other role or responsibility relating to the organization's SSP operation.

8.4 Topics Covered by Compliance Audit

The Compliance Audit shall verify that DigiCert has in place a system to assure the quality of the SSP services that it provides and that it complies with the requirements of the CP and this CPS as well as any MOAs between the Entity PKI and any other PKI. All aspects of the DigiCert or the organization CA/RA/CMS operations shall be subject to compliance audit inspections.

Components other than CAs may be audited fully or by using a representative sample. If the auditor uses a statistical sampling, all components, component managers and operators shall be considered in the sample and the samples shall vary on an annual basis.

---

[10] The compliance auditor shall be either a private firm that is independent from the entity being audited or, it shall be sufficiently organizationally separate from the entity (not in the same chain of command) to provide an unbiased, independent evaluation. An example of the latter may be an Agency inspector general. To ensure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining the entity's RA facility or RPS. If the compliance auditor is not an external firm, the auditor must sufficiently substantiate their independence within the Auditor Letter.

8.5 Actions Taken as a Result of Deficiency

When the compliance auditor finds a discrepancy between the requirements of the CP or the stipulations in the CPS and the design, operation, or maintenance of the PKI Authorities, the following actions shall be performed:

- The compliance auditor shall note the discrepancy;
- The compliance auditor shall promptly notify the responsible parties identified in Section 8.6 of the discrepancy;
- The party responsible for correcting the discrepancy will propose a remedy, including expected time for completion, to the FPKIPA.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the DigiCert PA may decide to temporarily halt operation of the CA, RA or CMS, revoke a certificate issued to the CA or RA, or take other actions it deems appropriate.

8.6 Communication of Results

The SSP compliance auditor shall report the results of a compliance audit to DigiCert and supply a signed Auditor Letter of Compliance addressed to the DCPA. The organization RA and/or CMS compliance auditor shall report the results of a compliance audit to the organization and supply a signed Auditor Letter of Compliance addressed to the DCPA. The organization shall supply the signed Auditor Letter of Compliance to the DCPA. Additionally, on request from the FPKIPA, the organization shall supply the full audit results report.

On an annual basis, the DCPA shall submit an annual review package to the FPKIPA. This package shall be prepared in accordance with the *FPKI Annual Review Requirements* document and shall include Multiple Auditor Letters of Compliance, signed by their respective auditors, covering the Principal CA and all PKI components and functions under the overall responsibility of the Entity PKI PMA, including those that are separately managed and operated. This package shall include an assertion from the DCPA that all PKI components have been audited, including any components that may be separately managed and operated. The package shall identify the versions of CPS or RPS and the CP used in the assessment.

Additionally, where necessary, the results shall be communicated as set forth in section 8.5 above.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

DigiCert is entitled to charge the Subscriber for the issuance, management and renewal of certificates.

9.1.2 Certificate Access Fees

DigiCert SSP certificates shall be available to relying parties at no charge.

9.1.3 Revocation or Status Information Access Fees

SSP certificate revocation lists (CRLs) shall be available to relying parties at no charge.

9.1.4 Fees for Other Services

If offered, the SSP or RA may charge a fee for key recovery services.

9.1.5 Refund Policy

The SSP adheres to, and stands behind, rigorous practices and policies in undertaking certification operations and in issuing certificates. Nevertheless, if for any reason a subscriber is not completely satisfied with the certificate issued to him, her, or it, the subscriber may request the DigiCert revoke the certificate within thirty (30) days of issuance and provide the subscriber with a refund. Following the initial thirty (30) day period, a subscriber may request that DigiCert revoke the certificate and provide a refund if DigiCert has breached a warranty or other material obligation under this CPS relating to the Subscriber or the Subscriber's certificate. Subscribers may request a refund in accordance with DigiCert's refund policy at https://www.digicert.com/digital-certificate-guarantee.htm. This refund policy is not an exclusive remedy and does not limit other remedies that may be available to Subscribers.

9.2 Financial Responsibility

DigiCert has sufficient financial resources to maintain its operations and perform its duties, and it is reasonably able to bear the risk of liability to Subscribers and recipients of certificates and other persons who may rely on the certificates and time stamps it issues. DigiCert also maintains professional liability insurance.

9.2.1 Insurance Coverage

DigiCert maintains commercially reasonable levels of errors and omissions insurance coverage.

9.2.2 Other Assets

An annual report of DigiCert can be obtained by submitting a written request to the address specified in section 1.4.

9.2.3 Insurance or Warranty Coverage for End-Entities

The non-federal SSP does not offer warranty protection.

9.3 Confidentiality of Business Information

Information deemed confidential is protected in accordance with section 9.4.

9.3.1 Scope of Confidential Information

The following records of Subscribers shall, subject to Section 9.3.2, be kept confidential and private ("Confidential/Private Information"):

- CA application records, whether approved or disapproved,
- Certificate Application records,
- Private keys held by Customers,
- Transactional records (both full records and the audit trail of transactions),
- Audit trail records created or retained by DigiCert or a Customer,
- Audit reports created by DigiCert or a Customer (to the extent such reports are maintained), or their respective auditors (whether internal or public),
- Contingency planning and disaster recovery plans, and
- Security measures controlling the operations of DigiCert hardware and software and the administration of Certificate services and designated enrollment services.

9.3.2 Information Not Within the Scope of Confidential Information

Certificates, Certificate revocation and other status information, DigiCert repositories and information contained within them are not considered Confidential/Private Information. Information not expressly deemed Confidential/Private Information under Section 9.3.1 shall be considered neither confidential nor private. This section is subject to applicable privacy laws.

9.3.3 Responsibility to Protect Confidential Information

DigiCert secures private information it receives from compromise and disclosure to third parties.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Any information about Subscribers that is not publicly available through the content of the issued certificate, certificate directory and online CRLs is treated as private. Private information will be handled as sensitive, stored locally on the SSP equipment and access will be limited to authorized personnel using certificate-based access control over SSL/TLS.

9.4.2 Information Treated as Private

All non-certificate information received from Subscribers shall be treated as confidential by the SSP and shall not be posted in the DigiCert repository. This information including: Dun and Bradstreet numbers, business or home addresses, telephone numbers and credit card data shall be handled as sensitive.

For RAs, collection of PII shall be limited to the minimum necessary to validate the identity of the subscriber. This may include attributes that corelate identity evidence to authoritative sources. RAs must provide explicit notice to the subscriber regarding the purpose for collecting and maintaining a record of the PII necessary for identity proofing and the consequences for not providing the information. PII collected for identity proofing

purposes shall not be used for any other purpose. These procedures and processes will be described in the RA's respective RPS.

9.4.3 Information Not Deemed Private

SSP certificates shall only contain information that is relevant and necessary to effect secure transactions with the certificate. Information in an SSP certificate is not considered private or privacy act information.

Certificates that contain the UUID in the subject alternative name extension shall not be distributed via publicly accessible repositories (e.g., HTTP).

9.4.4 Responsibility to Protect Private Information

DigiCert will not disclose confidential information to any third party unless required by law, government rule or regulation, or order of a court of competent jurisdiction. DigiCert shall not release or be required to release any confidential information without an authenticated, reasonably specific request prior to such release.

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

The SSP shall not disclose or sell applicant names or other identifying information, and shall not share such information, except in accordance with this CPS.

9.4.5 Notice and Consent to Use Private Information

Unless otherwise stated in this CPS or by agreement, confidential information will not be used without the consent of the party to whom that information applies. All notices shall be in accordance with the applicable laws.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

All disclosure shall be pursuant to applicable laws.

9.4.7 Other Information Disclosure Circumstances

All disclosure shall be pursuant to applicable laws.

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: Certificates and CRLs are the personal property of the SSP. DigiCert licenses relying parties to use certificates and CRLs.
- CPS: This CPS is personal property of DigiCert, Inc.
- Distinguished Names: Distinguished names are the personal property of the persons named (or their employer or principal).

- Subscriber Private Keys: Subscriber 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 or protected.
- Subscriber Public Keys: Subscriber public keys are the personal property of subscribers (or their employers or principal), regardless of the physical medium within which they are stored or protected.
- DigiCert Private Keys: SSP CA private keys are the personal property of DigiCert, Inc.
- DigiCert Public Keys: SSP CA public keys are the property of DigiCert, Inc. DigiCert licenses relying parties to use such keys.

9.6 Representations and Warranties

The parties are hereby notified of the following rules and obligations governing the respective rights and obligations of the parties among themselves. These rules and obligations are deemed to be agreed by the parties effective:

- Upon publication of this CPS in the case of the CA, RA, Trusted Agent;
- Upon submission of an application for a certificate, in the case of a Subscriber; and
- Upon reliance of a certificate or digital signature verifiable with reference to a public key listed in the certificate, in the case of a Relying Party or other recipient of a certificate issued under this CPS.

This section sets forth the warranties, disclaimers of warranties, and limitations of liability provided by Certificate Authorities to Subscribers and Relying Parties pursuant to this CPS.

Additional obligations are set forth in other provisions of this CPS and the Subscriber Agreement.

9.6.1 CA Representations and Warranties

DigiCert warrants to Subscribers that:

- There are no material misrepresentations of fact in such Certificate known to or originating from DigiCert;
- There are no errors in the information in the Certificate that were introduced by DigiCert as a result of its failure to exercise reasonable care in creating the Certificate;
- Such certificate meets all material requirements of this CPS; and
- Revocation services and use of a Repository conform to this CPS in all material respects.

DigiCert warrants to Relying Parties who reasonably rely on a Certificate that:

- All information in or incorporated by reference in such Certificate is accurate as of the date of issue;
- The Certificate has been issued to the individual named in the Certificate as the Subscriber; and
- DigiCert has materially complied with the CPS when issuing the Certificate.

The SSP shall conform to the stipulations of this document, including—

- Providing to the FPKIPA a CPS, as well as any subsequent changes, for conformance assessment;
- Maintaining its operations in conformance to the stipulations of the approved CPS;
- Ensuring that registration information is accepted only from approved RAs operating under an approved CPS;
- Including only valid and appropriate information in certificates, and maintaining evidence that due diligence was exercised in validating the information contained in the certificates;
- Revoking the certificates of Subscribers found to have acted in a manner counter to their obligations in accordance with Section 9.6.3; and

- Operating or providing for the services of an online repository that satisfies the obligations under Section 2.1.1, and informing the repository service provider of their obligations if applicable.

Each SSP CA shall comply with the following requirements:

- For PIV-I credentials issued for Affiliated Organizations, the SSP CA shall maintain an agreement with the Affiliated Organization concerning the obligations pertaining to authorizing the affiliation with subscribers of PIV-I certificates.
- Upon termination of an affiliation relationship, the SSP CA shall revoke all certificates affiliated with that organization.

9.6.2 RA Representations and Warranties

An RA and TA who performs registration functions as described in this CPS shall comply with the stipulations of this CPS and the CP. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities. An RA supporting this policy shall conform to the stipulations of this document, including:

- Performing in-person identify verification of certificate applicants in accordance with Section 3.2.3;
- Maintaining its operations in conformance to the stipulations of the approved 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; and
- 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.

9.6.3 Subscriber Representations and Warranties

By accepting a SSP certificate issued by DigiCert, the Subscriber certifies to and agrees with DigiCert and to all who reasonably rely on the information contained in the certificate that at the time of acceptance and throughout the operational period of the certificate, until notified otherwise by the Subscriber:

- each digital signature created using the private key corresponding to the public key listed in the certificate is the digital signature of the Subscriber and the certificate has been accepted and is operational (not expired, suspended or revoked) at the time the digital signature is created;
- no unauthorized person has ever had access to the Subscriber's private key;
- all representations made by the subscriber to DigiCert regarding the information contained in the certificate are true;
- all information contained in the certificate is true to the extent that the subscriber had knowledge or notice of such information and does not promptly notify DigiCert of any material inaccuracies in such information as set forth in CPS § 2.3.1;
- the certificate is being used exclusively for authorized and legal purposes, consistent with this CPS; and
- the Subscriber is an end-user and will not use the private key corresponding to any public key listed in the certificate for purposes of signing any certificate (or any other format of certified public key) or CRL.

By accepting a certificate, the Subscriber acknowledges that they agree to the terms and conditions contained in this CPS and the applicable subscriber agreement including:

- Notify DigiCert, in a timely manner, if the Subscriber believes or has reason to believe that their private keys are compromised or lost. Such notification shall be made directly or indirectly through mechanisms consistent with the CP and this CPS;
- Agree not to monitor, interfere with, or reverse engineer the technical implementation of the SSP except as explicitly permitted by this CPS or upon written approval by DigiCert; and

- Agree not to submit to DigiCert or the DigiCert repository any materials that contains statements that are (i) libelous, defamatory, obscene, pornographic, abusive, bigoted, hateful, or racially offensive, (ii) advocate illegal activity or discuss illegal activities with the intent to commit them, or (iii) otherwise violate any law.

PKI Sponsors (as described in Section 5.2.1.6) assume the obligations of Subscribers for the certificates associated with their components.

9.6.4 Relying Party Representations and Warranties

The following summarizes the obligations and responsibilities of parties who rely upon a certificate received from the DigiCert Repository or by other means:

- Perform a risk analysis to decide whether the level of assurance provided by the certificate is adequate to protect the Relying Party based upon the intended use;
- Use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension);
- Check each certificate for validity, using procedures described in the X.509 standard [ISO 9594-8], prior to reliance;
- Establish trust in the CA who issued a certificate by verifying the certification path in accordance with the guidelines set by the X.509 Version 3 Amendment; and
- Preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data. Note: data format changes associated with application upgrades may invalidate digital signatures and shall be avoided.

Relying parties that do not perform the obligations in this section assume all risks with regard to the digital signature and/or certificate on which they are relying.

9.6.5 Representations and Warranties of Other Participants

9.6.5.1 DigiCert PA Obligations

The DigiCert PA shall –

- Develop the CPS for the SSP CA and submit it to the FPKIPA for approval under the SSP policy;
- Review periodic compliance audits to ensure the SSP CA is operating in compliance with the approved CPS;
- Notify appropriate entities in the event of disaster, CA compromise or termination;
- Review name space control procedures to ensure that distinguished names are uniquely assigned for all certificates issued under this CPS;
- Publicly distribute the approved SSP CPS in accordance with section 2.2.2; and
- Coordinate modifications to the CPS to ensure continued compliance under the approved CPS.

9.6.5.2 Organization PMA Obligations

The Organization PMA shall

- Review periodic compliance audits to ensure that RAs and other components operated by the Organization are operating in compliance with the CPS and associated RPS and communicate results of the annual compliance audit to the DCPA as stipulated in section 8.6;
- Review name space control procedures to ensure that distinguished names are uniquely assigned within their Organization; and
- Notify appropriate entities in the event of RA compromise or termination.

9.6.5.3 Affiliated Organization Obligations

The Affiliated Organization shall authorize the affiliation of subscribers with the organization and shall inform the SSP CA of any severance of affiliation with any current subscriber.

9.7 Disclaimers of Warranties

9.7.1 Specific Disclaimers

Except as otherwise set forth in this CPS, DigiCert:

a) Shall not incur liability to any person or entity for representations contained in a certificate, provided the certificate was prepared substantially in compliance with the CPS, and provided further that the foregoing disclaimer shall not apply to DigiCert's liability in tort for negligent, reckless, or fraudulent conduct;

b) Does not warrant "nonrepudiation" for any DigiCert certificate or any message (because nonrepudiation is determined exclusively by law and the applicable final dispute resolution mechanism); and

c) Does not warrant the standards or performance of any hardware or software not under exclusive ownership of, exclusive control of, or licensed to DigiCert.

See also CPS § 2.3.2 (Disclaimer of Fiduciary Relationship).

9.7.2 General Disclaimer

Except as set forth in this CPS and the applicable subscriber agreement, and to the extent permitted by applicable law, DigiCert disclaims any and all other express or implied warranties and obligations of any type to any person or entity, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of the accuracy of information provided by certificate applicants, Subscribers, and third parties, and further disclaims any and all liability for any acts by DigiCert that constitute or may be held to constitute strict liability, whether sole or jointly with any other person or entity.

9.7.3 Disclaimer of Fiduciary Relationships

DigiCert is not the agent, fiduciary, trustee, or other representative of Subscribers or Relying Parties. The relationship between DigiCert and Subscribers and that between DigiCert and Relying Parties is not that of agent and principal. Neither Subscribers nor Relying Parties have any authority to bind DigiCert, by contract or otherwise, to any obligation. DigiCert shall make no representations to the contrary, either expressly, implicitly, by appearance, or otherwise.

9.8 Limitations of Liability

9.8.1 Limitations on Amount of Damages

In the event a Subscriber or Relying Party initiates any claim, action, suit, arbitration, or other proceeding separate from a request for payment under this CPS and to the extent permitted by applicable law, DigiCert's liability shall be limited as follows:

The total liability of DigiCert to any party for general contract, tort or any other damages for negligent, reckless, or fraudulent conduct by the DigiCert CAs, its RAs or Trusted Agents in connection with a single transaction

involving the use or reliance on a Non-Federal SSP certificate shall be limited to ten thousand dollars ($10,000). Furthermore, DigiCert's total liability for any incident (aggregate of all transactions) involving the use or reliance on a certificate shall be limited to one hundred thousand ($100,000 USD). These liability caps shall be the same regardless of the number of digital signatures, acts of authentication, or encrypted messages related to, or claims arising out of such transaction.

Notwithstanding the foregoing, to the extent DigiCert has issued and managed the Certificate(s) at issue in compliance with its Certification Practice Statement, DigiCert shall have no liability to the Subscriber, any Relying Party, or any other third parties for any damages or losses suffered as a result of the use or reliance on such Certificate(s).

9.8.2 Exclusion of Certain Elements of Damages

Except as expressly provided in this CPS, and to the extent permitted by applicable law, DigiCert shall not be liable in contract to any person or entity for any indirect, special, reliance, incidental, or consequential damages (including but not limited to any loss of profits or loss of data), arising from or in connection with the use, delivery, license, performance, or nonperformance of certificates, digital signatures, or any other transactions, products, or services offered or contemplated by this CPS, even if DigiCert has been advised of the possibility of such damages.

To the extent permitted by applicable law, DigiCert shall not be liable to any person or entity for any punitive damages arising from or in connection with the use, delivery, license, performance, or nonperformance of certificates, digital signatures, or any other transactions or services offered or contemplated by this CPS.

9.9 Indemnities

Without limiting other Subscriber obligations stated in this CPS, 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.

By accepting a certificate, the Subscriber agrees to indemnify and hold DigiCert and its agent(s) and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable attorneys' fees, that DigiCert and its agents and contractors may incur, that are caused by the use or publication of a certificate, and that arises from (i) falsehood or misrepresentation of fact by the Subscriber (or a person acting upon instructions from anyone authorized by the Subscriber); (ii) failure by the Subscriber to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive DigiCert or any person receiving or relying on the certificate; or (iii) failure to protect the Subscriber's private key, to use a trustworthy system, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key.

9.10 Term and Termination

9.10.1 Term

The term of this CPS shall last through the end of the archive period specified in section 5.5.2.

9.10.2 Termination

See section 4.9.

9.10.3 Effect of Termination and Survival

Each SSP CA shall comply with the following requirements.

The obligations and restrictions contained within CPS sections 5.5 (Records Archival), 8 (Compliance Audit and Other Assessments), 9.2 (Financial Responsibility), 9.3 (Confidentiality of Business Information), 9.4 (Privacy of Personal Information), 9.5 (Intellectual Property Rights), 9.7 (Disclaimers of Warranties), 9.8 (Limitations of Liability), 9.9 (Indemnities), 9.10 (Term and Termination), 9.11 (Communications with Participants), 9.13 (Dispute Resolution Procedures), 9.14 (Governing Law), 9.15 (Compliance with Applicable Law), 9.16 (Miscellaneous Provisions) and 9.17 (Other Provisions) shall survive the termination of this CPS.

9.11 Individual Notices and Communications with Participants

Whenever any person hereto desires or is required to give any notice, demand, or request with respect to this CPS, such communication shall be made either using digitally signed messages consistent with the requirements of this CPS, or in writing. Electronic communications shall be effective upon the sender's receiving a valid, digitally signed acknowledgment of receipt from the recipient. Such acknowledgment must be received within five (5) days, or else written notice must then be communicated. Communications in writing must be delivered by a courier service that confirms delivery in writing or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows:

To DigiCert:

Attn: Legal Counsel
DigiCert Policy Authority
Suite 500
2801 N. Thanksgiving Way
Lehi, UT 84043 USA
www.digicert.com
support@digicert.com

By DigiCert to another person:
To the most recent address of record to another person on file with DigiCert, Inc.

If any planned change to the infrastructure that has the potential to affect the FPKI operational environment, that change 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

Comments or issues with this CPS should be directed to the parties identified in Section 1.4.2 of this document.

The PA, prior to enactment, must approve material amendments to this CPS.

9.12.2 Notification Mechanism and Period

Upon approval of a CPS modification by the DCPA, an updated version of this document will be provided to the FPKIPA for final approval. Once approval is given by the FPKIPA, the Non-Federal SSP CPS will be published on the legal repository and available for relying parties as soon as feasible.

9.12.3 Circumstances under Which OID must be Changed

If the FPKI PA determines that a change is necessary in the object identifier corresponding to a Certificate policy, the amendment shall contain new object identifiers for the Certificate policies corresponding to each Class of Certificate. Otherwise, amendments shall not require a change in Certificate policy object identifier. The DCPA will update the OIDs within this CPS based on those changes.

9.13 Dispute Resolution Provisions

The DCPA shall facilitate the resolution between entities when conflicts arise as a result of the use of certificates issued under this CPS
DigiCert shall investigate and correct, if necessary, any name collisions brought to its attention. If appropriate, DigiCert shall coordinate with and defer to the naming authority.

Disputes among SSP participants shall be resolved pursuant to provisions in the applicable agreements among the parties. To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall contain a dispute resolution clause. Disputes involving DigiCert require an initial negotiation period of sixty (60) days followed by litigation in the federal or state court encompassing Salt Lake County, Utah, in the case of claimants who are U.S. residents, or in the case of all other claimants, arbitration administered by the International Chamber of Commerce ("ICC") in accordance with the ICC Rules of Conciliation and Arbitration, unless otherwise approved by DigiCert.

9.14 Governing Law

The relationship between this CPS and the CP shall be governed by the laws of the State of Utah.

For individuals or entities not within the United States Government, the laws of the State of Utah, U.S.A., shall govern the enforceability, construction, interpretation, and validity of this CPS, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in Utah. This choice of law is made to ensure uniform procedures and interpretation for all users, no matter where they reside or use their certificates.

9.15 Compliance with Applicable Law

This CPS is subject to applicable national, state, and local laws, rules regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

9.15.1 Compliance with Export Laws and Regulations

Export of certain software used in conjunction with the DigiCert SSP may require the approval of appropriate government authorities. The parties shall conform to applicable export laws and regulations.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Not applicable.

9.16.2 Assignment

This CPS inures to the benefit of, and shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties. The rights and obligations

detailed in this CPS are assignable by the parties, by operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with CPS § 4.9, concerning termination or cessation of CA operations; and provided further, that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

9.16.3 Severability

If any provision of this CPS, or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this CPS (and the application of the invalid or unenforceable provision to other persons or circumstances) shall be interpreted so as best to reasonably effect the intent of its parties. It is expressly understood and agreed that each and every provision of this CPS that provides for a limitation of liability, disclaimer of or limitation upon any warranties or other obligations, or exclusion of damages is intended to be severable and independent of any other provision and is to be enforced as such.

9.16.4 Merger

No term or provision of this CPS directly affecting the respective rights and obligations of DigiCert may be orally amended, waived, supplemented, modified, or terminated, except by an authenticated message or document of such affected party, except to the extent provided otherwise herein.

9.16.5 Enforcement (Attorney Fees and Waiver of Rights)

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

9.16.6 Choice of Cryptographic Methods

All persons acknowledge that they (not DigiCert) are solely responsible for and have exercised independent judgment in choosing security software, hardware, and encryption/digital signature algorithms, including their respective parameters, procedures, and techniques.

9.16.7 Force Majeure

DigiCert shall not be responsible for any breach of warranty, delay, or failure in performance under this 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

9.17.1 Conflict of Provisions

In the event of a conflict between this CPS and other rules, guidelines, or contracts, the Subscriber shall be bound by the provisions of this CPS except to the extent that the provisions of this CPS are prohibited by law. In the event of a conflict between the DigiCert CP for Symantec Trust Network and this CPS, the DigiCert CP for Symantec Trust Network shall take precedence over this CPS.

9.17.2 Interpretation

Unless otherwise provided, this CPS shall be interpreted consistently with what is commercially reasonable under the circumstances.

9.17.3 Headings and Appendices of this CPS

The headings, subheadings, and other captions in this CPS are for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this CPS. The appendices, including the definitions to this CPS, are an integral and binding part of the CPS.

10. REFERENCES

The following documents contain information that provides background, examples, or details about the contents of this policy.

Number	Title	Revision	Date
ABADSG	*Digital Signature Guidelines, 1996-08-01.* *http://itlaw.wikia.com/wiki/American_Bar_Association_(ABA)_Digital_Signature_Guidelines*		1 August 1996
AUDIT	*FPKI Annual Review Requirements*		
FPKI-E	*Federal PKI Version 1 Technical Specifications: Part E-X.509 Certificate and CRL Extensions Profile*		*7 July 1997*
FPKI-PROF	*Federal PKI X.509 Certificate and CRL Extensions Profile* http://www.idmanagement.gov/fpki-documents		
E-Auth	*E-Authentication Guidance for Federal Agencies, M-04-04*		16 Dec 2003
FIPS140	*Security Requirements for Cryptographic Modules* http://csrc.nist.gov/publications/index.html		21 May 2001
FIPS112	*Password Usage* http://csrc.nist.gov/		5 May 1985
FIPS186-2	*Digital Signature Standard* *http://www.itl.nist.gov/fipspubs/fip186.htm*		27 January 2000
FIPS201-2	*Personal Identity Verification (PIV) of Federal Employees and Contractors* https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf		August 2013
FOIAACT	*5 U.S.C. 552, Freedom of Information Act* http://www4.law.cornell.edu/uscode/5/552.html		
NIST SP 800-63-3	*Digital Identity Guidelines* *https://csrc.nist.gov/publications/detail/sp/800-63/3/final*		
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 http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf		
NIST SP 800-78	Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV) http://csrc.nist.gov/publications/nistpubs/800-78-2/sp800-78-2.pdf		
NS4009	*NSTISSI 4009, National Information Systems Security Glossary*		January 1999
PACS	*Technical Implementation Guidance: Smart Card Enabled Physical Access Control (SCEPACS)*http://www.idmanagement.gov/fpki-documents	2.2	30 July 2004
PIV-I Profile	X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards, April 23, 2010, http://www.idmanagement.gov/fpki-documents		April 23, 2010
PKCS-1	*PKCS #1 v2.1: RSA Cryptography Standard* http://www.rsasecurity.com/rsalabs/node.asp?id=2125	2.1	14 June 2002
PKCS-12	*Personal Information Exchange Syntax Standard* http://www.rsasecurity.com/rsalabs/node.asp?id=2138	1.0	24 June 1999
SSPKRPS	*Key Recovery Practices Statement for DigiCert SSP PKI Service*		
RFC3647	*Certificate Policy and Certification Practices Framework,* Chokhani and Ford http://www.ietf.org/rfc/rfc3647.txt		2003
RFC 5019	The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, *http://www.rfc-editor.org/pipermail/rfc-dist/2007-September/001760.html*		September 2007

Number	Title	Revision	Date
RFC 5280	*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*		April 2002

11. ACRONYMS AND ABBREVIATIONS

AES	Advanced Encryption Standard
AID	Application Identifier
CA	Certification Authority
CMA	Certificate Management Authority
CMS	Card Management System
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSA	Certificate Status Authority
CSS	Certificate Status Service
CSOR	Computer Security Objects Registry
DCPA	DigiCert Policy Authority
DES	Data Encryption Standard
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECDSA	Elliptic curve Digital Signature Algorithm
FASC-N	Federal Agency Smart Credential Number
FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standard
FPKI	(US) Federal Public Key Infrastructure
GSA	General Services Administration
HTTP	HyperText Transfer Protocol
HSM	Hardware Security Module
I&A	Identification and Authentication
ID	Identity (also, a credential asserting an identity)
ISO	International Organization for Standards
KMD	Key Manager Database
KRP	Key Recovery Policy
KRPS	Key Recovery Practice Statement
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification - Interoperable
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PMA	Policy Management Authority
POC	Point of Contact
RA	Registration Authority
RFC	Request For Comment
RSA	Rivest, Shamir, Adleman (encryption and digital signature algorithm)
S/MIME	Secure Multipurpose Internet Mail Extensions
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer
SSP	Shared Service Provider
TA	Trusted Agent
TLS	Transport Layer Security
USC	United States Code
USD	United States Dollar
UUID	Universally Unique Identifier (defined by RFC 4122)

VM	Virtual Machine
VME	Virtual Machine Environment

12. GLOSSARY

access	Ability to make use of any information system (IS) resource.
access control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems.
accreditation	Formal declaration by a Designated Approving Authority that an IS is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
Affiliated Organization	Organizations that authorize affiliation with Subscribers of PIV-I certificates
Agency	Any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Executive Branch of the Federal Government.
applicant	The Subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed.
archive	Long-term, physically separate storage.
Attribute Authority	An entity, recognized by a CMA, as having the authority to verify the association of attributes to an identity.
audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
audit data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event.
authenticate	To confirm the identity of an entity when that identity is presented.
authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
backup	Copy of files and programs made to facilitate recovery if necessary.
binding	Process of associating two related elements of information.
biometric	A physical or behavioral characteristic of a person.
card management system	The system for managing the issuance of a smart card that may provide the electronic and graphical personalization of the card
certificate	A digital representation of information which at least (1) identifies the CA 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 CA issuing it.
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.
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.
Certification Authority (CA)	An authority trusted by one or more users to create and assign certificates.
CA facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
certificate-related information	Information, such as a Subscriber's postal address, that is not included in a certificate, but that may be used by a CA in certificate management.
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.

compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by NIST
confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.
cryptographic module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.
cryptoperiod	Time span during which each key setting remains in effect.
data integrity	Assurance that the data are unchanged from creation to reception
dual use certificate	A certificate that is intended for use with both digital signature and data encryption services.
e-commerce	The use of network technology (especially the Internet) to buy or sell goods and services
Encryption (or Confidentiality) certificate	A certificate containing a public key that is used to encrypt or decrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes. The process of storing protecting and escrowing the private component of the key pair associated with the encryption certificate is sometimes referred to as key management.
erroneous issuance	Issuance of a certificate not materially in accordance with the procedures required by the CPS, issuance of a certificate to a person other that the one named as the subject of the certificate, or issuance of a certificate without the authorization of the person named as the subject of such certificate.
firewall	Gateway that limits access between networks in accordance with local security policy.
Hypervisor	Computer software, firmware or hardware that creates and runs virtual machines. A hypervisor uses native execution to share and manage hardware, allowing for multiple environments which are isolated from one another, yet exist on the same physical machine. Also known as an isolation kernel or virtual machine monitor.
impersonation	Requesting and being issued a certificate issued under this CPS based on false or falsified information relating to naming or identity.
integrity	Protection against unauthorized modification or destruction of information.
intellectual property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
key escrow	The retention of the private component of the key pair associated with a subscriber's encryption certificate to support key recovery.
key exchange	The process of exchanging public keys (and other information) in order to establish secure communication.
key generation material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
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.

Key Recovery Practices Statement (KRPS)	A statement of the practices that a Key Recovery System employs in protecting and recovering key management private keys, in accordance with specific requirements (i.e., requirements specified in the KRP).
Local Registration Authority (LRA)	An RA with responsibility for a local community.
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 U.S. 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.
Non-verified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.
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 OIDs are used to uniquely identify each of the four policies and cryptographic algorithms supported.
Organization CMS	The SSP customer organization operating the CMS function for the SSP service.
Out-of-Band	Communication between parties using 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).
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 the FBCA CP and this CPS.
Policy Authority (PA)	Authority that oversees the creation and update of Certificate Policies, reviews Certification Practice Statements, reviews the results of CA audits for policy compliance, evaluates non-domain policies for acceptance within the domain, and generally oversees and manages the PKI certificate policies. The individual or group that is responsible for maintaining the SSP CPS and for ensuring that all SSP PKI components (e.g., CAs, CSSs, CMSs, RAs) are operated in compliance with this CPS and the CP,
privacy	State in which data and system access is restricted to the intended user community and target recipient(s).
Private key compromise	A loss, theft or modification, or unauthorized access of a private key corresponding to the public key listed in a certificate governed by this CPS, including without limitation by cryptographic analysis or key extraction.
Public Key Infrastructure (PKI)	Framework established to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	Entity responsible for identification and authentication of certificate subjects that has automated equipment for the communication of applicant data to Certification Authorities and does not sign or directly revoke certificates.

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.
re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application.
Relying Party	A person who has received a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
repository	A trustworthy system for storing and retrieving certificates or other information relevant to certificates.
revocation	The act or process of prematurely ending 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.
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. Also referred to as an Identity Certificate.
subordinate CA	In a hierarchical PKI, a CA whose certificate signing key is certified by another CA, and whose activities are constrained by that other CA. (see superior CA)
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to such an entity, and (2) holds a private key that corresponds to a public key listed in that certificate. Current subscribers possess valid CDS-issued certificates.
superior CA	In a hierarchical PKI, a CA who has certified the certificate signing key of another CA, and who constrains the activities of that CA. (see subordinate CA)
Supervised Remote identity Proofing	A real-time identity proofing event where the RA/Trusted Agent is not in the same physical location as the applicant/subscriber. The RA/Trusted Agent controls a device which is utilized by the applicant/subscriber in order to ensure the remote identity proofing process employs physical, technical and procedural measures to provide sufficient confidence that the remote session can be considered equivalent to a physical, in-person identity proofing process. Supervised Remote Identity Proofing must meet the criteria specified in NIST SP 800-63A Section 5.3.3; and must have the capacity to capture an approved biometric when utilized for PIV-I credential issuance.
system equipment configuration	A comprehensive accounting of all system hardware and software types and settings.
technical non-repudiation	The contribution public key mechanisms make to the provision of technical evidence supporting a non-repudiation security service.
threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.
trust list	Collection of Trusted Certificates used by Relying Parties to authenticate other certificates.
tier	A barrier such as a locked door or closed gate that provides mandatory access control for individuals and requires a positive response (e.g., door unlocks or gate opens) for each individual to proceed to the next area. Each successive tier provides more restricted access and greater physical security against intrusion or unauthorized access. Moreover, each physical security tier encapsulates the next inner tier, such that an inner tier must be fully contained in an outside tier and cannot have a common outside wall with the outside tier, the outermost tier being the outside wall of the building.

Trusted Agent	Entity authorized to act as a representative of a Certificate Management Authority in providing Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure, authenticated delivery. The public keys included in Trusted Certificates are used to start certification paths. Also known as a "trust anchor".
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
two person control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements.
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.
Virtual Machine Environment	An emulation of a computer system (in this case, a CA) that provides the functionality of a physical machine in a platform-independent environment. It consists of a host (virtual machine) and isolation kernel (hypervisor) and provides functionality needed to execute entire operating systems. At this time, allowed VMEs are limited to Hypervisor type virtual environments. Other technology, such as Docker Containers, is not permitted.
unauthorized revocation	Revocation of a certificate without the authorization of the subscriber.
zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data.

APPENDIX A: CERTIFICATE AND CRL FORMATS

The certificates and CRLs associated with the Non-Federal SSP PKI service are derived from the certificate and CRL formats specified in the FPKI X.509 CRL Extensions Profile and X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards

The following profiles are included:

A.1: Non-Federal SSP Intermediate Certificate Profile

A.2: Non-Federal SSP CRL Profile

A.3: Non-Federal SSP Signature Certificate Profile

A.4: Non-Federal SSP Encryption Certificate Profile

A.5: Non-Federal SSP Device Certificate Profile

A.6: Non-Federal SSP PIV-I Card Authentication Certificate Profile

A.7: Non-Federal SSP PIV-I Authentication Certificate Profile

A.8: Non-Federal SSP PIV-I Digital Signature Certificate Profile

A.9: Non-Federal SSP PIV-I Key Management Certificate Profile

A.10: Non-Federal SSP PIV-I Content Signing Certificate Profile

A.11: Non-Federal SSP OCSP Responder Certificate Profile

The *id-stn-ssp-pivi-hardware* assurance level includes certificate types Non-Federal SSP PIV-I Authentication, SSP PIV-I Digital Signature and Non-Federal SSP PIV-I Key Management.

The *id-stn-ssp-class3-devices-sha1* profile is used for all device certificate types including PIV-I contentSigning.

A.1: Non-Federal SSP Intermediate Certificate Profile

Field	Criticality Flag	Value	Comments
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		INTEGER	Unique positive integer.
signature			
algorithm		Choice of following algorithms:	
		1.2.840.113549.1.1.11	Sha256WithRSAEncryption
		1.2.840.10045.4.3.2	ecdsa-with-SHA256
issuerName			Must use one of the name forms specified in section 3.1.1 of the CPS.
validity			
notBefore			
notAfter			
subjectName			X.500 Distinguished name of the owner of the subject public key in the certificate. Subject name should be encoded exactly as it is encoded in the issuer field of certificates issued by the subject.
subjectPublicKeyInfo			
AlgorithmIdentifier			Public key algorithm associated with the public key.
algorithm		1.2.840.113549.1.1.1	RSA Encryption
		1.2.840.10045.2.1	Elliptic curve key
subjectPublicKey		BIT STRING	For RSA public keys: certificates shall have a modulus of at least 2048 bits.
required extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	The value in this field must be the same as the value that the subject CA uses in the authority key identifier extension of the certificates and CRLs that it signs with the private key that corresponds to the subject public key included in this certificate.
keyUsage	TRUE		If the subject public key may be used for purposes other than certificate and CRL signing (e.g., signing OCSP responses), then the digitalSignature and/or nonRepudiation bits may be set as well.
digitalSignature		0	
nonRepudiation		0	
keyEncipherment		0	
dataEncipherment		0	
keyAgreement		0	
keyCertSign		1	
cRLSign		1	
encipherOnly		0	
decipherOnly		0	

Field	Criticality Flag	Value	Comments
certificatePolicies	FALSE		
PolicyInformation			CA certificates may assert one or more of the following OIDs. Other policy OIDs may be asserted as well.
policyIdentifier		2.16.840.1.113733 1.7.23.1.1.1	*id-stn-ssp-rudimentary*
		2.16.840.1.113733 1.7.23.2.1.1	*id-stn-ssp-basic*
		2.16.840.1.113733 1.7.23.3.1.6	*id-stn-ssp-medium*
		2.16.840.1.113733 1.7.23.3.1.7	*id-stn-ssp-mediumHardware*
		2.16.840.1.113733 1.7.23.3.1.8	*id-stn-ssp-mediumDevices*
		2.16.840.1.113733 1.7.23.3.1.36	*id-stn-ssp-mediumDevicesHardware*
		2.16.840.1.113733 1.7.23.3.1.13	*id-stn-ssp-authentication (in legacy certs only)*
		2.16.840.1.113733 1.7.23.3.1.14	*id-stn-ssp-Medium CBP*
		2.16.840.1.113733 1.7.23.3.1.15	*id-stn-ssp-MediumHardware CBP*
		2.16.840.1.113733 1.7.23.3.1.17	*id-stn-ssp-pivi-cardAuth*
		2.16.840.1.113733 1.7.23.3.1.18	*id-stn-ssp-pivi-hardware*
		2.16.840.1.113733 1.7.23.3.1.20	*id-stn-ssp-pivi-contentSigning*
basicConstraints	TRUE		This extension must appear in all CA certificates.
cA		TRUE	
pathLenConstraint		Absent	.
cRLDistributionPoints	FALSE		This extension must contain at least one HTTP URI. The reasons and cRLIssuer fields must be omitted.
authorityInfoAccess	FALSE		authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates must include an authorityInfoAccess extension with at least one instance of the calssuers access method that specifies an HTTP URI. The OCSP access method may also be included if status information for this certificate is available via OCSP.
accessMethod		id-ad-calssuers (1.3.6.1.5.5.7.48.2)	When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible Web server where certificates issued to the issuer of this certificate may be found.
uniformResourceIdentifier		http://…	See preamble text on URIs.
subjectInfoAccess	FALSE		CA Certificates issued must include a subjectInfoAccess extension (unless the certificate subject does not issue any CA certificates. subjectInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Only one access method is defined for use in CA certificates.
accessMethod		id-ad-caRepository (1.3.6.1.5.5.7.48.5)	Each CA certificate must include at least one instance of this access method that includes a URI name form to specify an HTTP accessible Web server. Each URI should point to a location where certificates issued by the subject of this certificate may be found.
uniformResourceIdentifier		http://…	See preamble text on URIs.

Field	Criticality Flag	Value	Comments
optional extensions			
policyMappings	FALSE		This extension must be included in cross-certificates .
issuerDomainPolicy		OID	OID of policy from the issuing CA domain that maps to the equivalent policy in the subject CA's domain.
subjectDomainPolicy		OID	OID of policy in the subject CA's domain that may be accepted in lieu of the issuing domain policy.

A.2: Non-Federal SSP CRL Profile

Field	Criticality Flag	Value	Comments
version		1	Integer Value of "1" for Version 2 CRL.
signatureAlgorithm		Choice of following algorithms:	
		1.2.840.113549.1.1.11	Sha256WithRSAEncryption
		1.2.840.10045.4.3.2	ecdsa-with-SHA256
issuer			
Name			Issuer name should be encoded exactly as it is encoded in the issuer fields of the certificates that are covered by this CRL.
thisUpdate			
nextUpdate			
revokedCertificates			
userCertificate		INTEGER	serial number of certificate being revoked
revocationDate			
crlEntryExtensions			
reasonCode	FALSE		
CRLReason			Any one of these CRL reasons may be asserted: keyCompromise, cAcompromise, affiliationChanged, superseded, cessationOfOperation. If the revocation reason is unspecified, then the reasonCode extension should not be included. The removeFromCRL reason code may only be used in delta CRLs and the use of certificateHold is deprecated.
crlExtensions			
authorityKeyIdentifier	FALSE		Must be included in all CRLs.
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
cRLNumber	FALSE	INTEGER	Monotonically increasing sequential number. Must be included in all CRLs.

A.3: Non-Federal SSP Signature Certificate Profile

Field	Criticality Flag	Value	Comments
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		INTEGER	Unique positive integer.
signatureAlgorithm		Choice of following algorithms:	
		1.2.840.113549.1.1.11	Sha256WithRSAEncryption
		1.2.840.10045.4.3.2	ecdsa-with-SHA256
issuerName			Must use one of the name forms specified in section 3.1.1 of the CPS.
validity			
notBefore			
notAfter			
subjectName			X.500 Distinguished name of the owner of the certificate.
RDNSequence			Must use one of the name forms specified in section 3.1.1 of the CPS.
subjectPublicKeyInfo			
AlgorithmIdentifier			Public key algorithm associated with the public key. either RSA or elliptic curve.
algorithm		1.2.840.113549.1.1.1	RSA Encryption
		1.2.840.10045.2.1	Elliptic curve key
subjectPublicKey		BIT STRING	For RSA public keys: certificates shall have a modulus of at least 2048 bits.
required extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
keyUsage	TRUE		Both digitalSignature and nonRepudiation shall be set.
digitalSignature		1	
nonRepudiation		1	
certificatePolicies	FALSE		
PolicyInformation			Digital signature certificates issued to human subscribers should assert one of the following policies. Other policy OIDs may be asserted as well.
policyIdentifier		2.16.840.1.113733 1.7.23.1.1.1	*id-stn-ssp-rudimentary*
		2.16.840.1.113733 1.7.23.2.1.1	*id-stn-ssp-basic*
		2.16.840.1.113733 1.7.23.3.1.6	*id-stn-ssp-medium*
		2.16.840.1.113733 1.7.23.3.1.7	*id-stn-ssp-mediumHardware*
		2.16.840.1.113733 1.7.23.3.1.14	*id-stn-ssp-medium CBP*
		2.16.840.1.113733 1.7.23.3.1.15	*id-stn-ssp-mediumHardware CBP*

Field	Criticality Flag	Value	Comments
cRLDistributionPoints	FALSE		This extension is required in all end entity certificates and must contain at least one HTTP URI. The reasons and cRLIssuer fields must be omitted.
uniformResourceIdentifier		http://…	See preamble text on URIs.
extKeyUsage		BOOLEAN	This extension must appear in certificates issued after June 30, 2019. The extension should be noncritical and shall not include the anyExtendedKeyUsage value. The values listed below for keyPurposeID are recommended for inclusion. Additional keyPurposeIDs, consistent with signing purposes, may be specified. Note: For certificates issued prior to June 30, 2019, anyExtendedKeyUsage may be present or the entire extension may be absent.
keyPurposeID		1.3.6.1.5.5.7.3.4	id-kp-emailProtection
		1.3.6.1.4.1.311.10.3.12	MSFT Document Signing
authorityInfoAccess	FALSE		authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued under the Common Certificate Policy must include an authorityInfoAccess extension with at least one instance of the caIssuers access method that specifies an HTTP URI. The OCSP access method may also be included if status information for this certificate is available via OCSP.
accessMethod		id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible Web server where certificates issued to the issuer of this certificate may be found.
accessLocation			
GeneralName			
uniformResourceIdentifier		http://…	See preamble text on URIs.
subjectAltName	FALSE		Must include the rfc822Name. Other name types may be present to support local applications.
rfc822Name		IA5String	This field contains the electronic mail address of the subject.
optional extensions			

A.4: Non-Federal SSP Encryption Certificate Profile

Field	Criticality Flag	Value	Comments
Certificate			
tbsCertificate			Fields to be signed.
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		INTEGER	Unique positive integer.
signature			
AlgorithmIdentifier		Choice of following algorithms:	
		1.2.840.113549.1.1.11	Sha256WithRSAEncryption
		1.2.840.10045.4.3.2	ecdsa-with-SHA256
		NULL	For all RSA algorithms except id-RSASSA-PSS
issuerName			Must use one of the name forms specified in section 3.1.1 of the CPS.
validity			
notBefore			
notAfter			
subjectName			X.500 Distinguished name of the owner of the certificate.
RDNSequence			Must use one of the name forms specified in section 3.1.1 of the FBCA CP.
subjectPublicKeyInfo			
AlgorithmIdentifier			Public key algorithm associated with the public key.
algorithm		1.2.840.113549.1.1.1	RSA Encryption
		1.2.840.10045.2.1	Elliptic curve key
RSAParameters		NULL	For RSA, parameters field is populated with NULL.
subjectPublicKey		BIT STRING	For RSA public keys: certificates shall have a modulus of at least 2048 bits.
required extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
keyUsage	TRUE		
digitalSignature		0	
nonRepudiation		0	
keyEncipherment		1	Asserted when public key is RSA.
dataEncipherment		0	
certificatePolicies	FALSE		
PolicyInformation			Key management certificates issued to human subscribers should assert one of the following policies. Other policy OIDs may be asserted as well.
policyIdentifier		2.16.840.1.113733 1.7.23.1.1.1	*id-stn-ssp-rudimentary*
		2.16.840.1.113733 1.7.23.2.1.1	*id-stn-ssp-basic*

Field	Criticality Flag	Value	Comments
		2.16.840.1.113733 1.7.23.3.1.6	*id-stn-ssp-medium*
		2.16.840.1.113733 1.7.23.3.1.7	*id-stn-ssp-mediumHardware*
		2.16.840.1.113733 1.7.23.3.1.14	id-stn-ssp-medium CBP
		2.16.840.1.113733 1.7.23.3.1.15	id-stn-ssp-mediumHardware CBP
cRLDistributionPoints	FALSE		This extension is required in all end entity certificates and must contain at least one HTTP URI. The reasons and cRLIssuer fields must be omitted.
uniformResourceIdentifier		http://…	See preamble text on URIs.
extKeyUsage		BOOLEAN	This extension MUST appear in certificates issued after June 30, 2019. The extension should be noncritical and shall not include the anyExtendedKeyUsage value. The values listed below for keyPurposeID are recommended for inclusion. Additional keyPurposeIDs, consistent with key management purposes, may be specified. Note: For certificates issued prior to June 30, 2019, anyExtendedKeyUsage may be present or the entire extension may be absent.
authorityInfoAccess	FALSE		authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued under the FBCA Certificate Policy must include an authorityInfoAccess extension with at least one instance of the caIssuers access method: one that specifies an HTTP URI. The OCSP access method may also be included if status information for this certificate is available via OCSP.
AccessDescription			
accessMethod		id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible Web server where certificates issued to the issuer of this certificate may be found.
accessLocation			
GeneralName			
uniformResourceIdentifier		http://…	See preamble text on URIs.
subjectAltName	FALSE		Must include the rfc822Name. Other name types may be present to support local applications.
rfc822Name		IA5String	This field contains the electronic mail address of the subject.

A.5: Non-Federal SSP Device Certificate Profile

Field	Criticalit	Value	Comments
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		INTEGER	Unique positive integer.
signature			
AlgorithmIdentifier			Must match Algorithm Identifier in signatureAlgorithm field. The parameters field is only populated when the algorithm is RSA.
algorithm		Choice of following algorithms:	
		1.2.840.113549.1.1.11	Sha256WithRSAEncryption
		1.2.840.10045.4.3.2	ecdsa-with-SHA256
parameters		NULL	
issuerName			Must use one of the name forms specified in section 3.1.1 o CPS
validity			
notBefore		YMMDDHHMMSSZ	
notAfter		YMMDDHHMMSSZ	
subject			
Name			X.500 Distinguished name of the owner of the certificate.
RDNSequence			Must use one of the name forms specified in section 3.1.1 of the CPS.
subjectPublicKeyInfo			
AlgorithmIdentifier			Public key algorithm associated with the public key. May be RSA.
algorithm		1.2.840.113549.1.1.1	RSA Encryption
		1.2.840.10045.2.1	Elliptic curve key
parameters			Format and meaning dependent upon algorithm
RSAParameters		NULL	For RSA, parameters field is populated with NULL.
subjectPublicKey		BIT STRING	For RSA public keys: certificates shall have a modulus of at least 2048 bits
required extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
keyUsage	TRUE		Use of a single certificate for both digital signatures and key management is deprecated, but may be used to support legacy applications that require the use of such certificates.
digitalSignature		1	may be asserted.
nonRepudiation		0	Must not be asserted in certificates issued to computing or communications devices.
keyEncipherment		1	May be asserted when public key is RSA.
dataEncipherment		0	
certificatePolicies	FALSE		

Field	Criticalit	Value	Comments
PolicyInformation			Other policy OIDs may be asserted in addition to the OID from the Common Certificate Policy.
policyIdentifier		2.16.840.1.113733.1.7.23.3.1.8	*id-stn-ssp-mediumDevices*
		2.16.840.1.113733.1.7.23.3.1.36	*id-stn-ssp-mediumDevicesHardware*
cRLDistributionPoints	FALSE		This extension is required in all end entity certificates and must contain at least one HTTP URI. The reasons and cRLIssuer fields must be omitted.
uniformResourceIdentifier		http://…	See preamble text on URIs.
extKeyUsage		BOOLEAN	This extension MUST appear in certificates issued after June 30, 2019. The extension should be noncritical and shall not include the anyExtendedKeyUsage value. The values listed below for keyPurposeID are recommended for inclusion. Additional keyPurposeIDs, consistent with key management purposes, may be specified. Note: For certificates issued prior to June 30, 2019, anyExtendedKeyUsage may be present or the entire extension may be absent.
authorityInfoAccess	FALSE		authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued under the FBCA Certificate Policy must include an authorityInfoAccess extension with at least one instance of the calssuers access method that specifies an HTTP URI. The OCSP access method may be included if status information for this certificate is available via OCSP.
accessMethod		id-ad-calssuers (1.3.6.1.5.5.7.48.2)	The access location shall include the URI name form to specify the location of an HTTP accessible Web server where certificates issued to the issuer of this certificate may be found.
accessLocation			
GeneralName			
uniformResourceIdentifier		http://…	See preamble text on URIs.
optional extensions			
KeyPurposeID		1.3.6.1.5.5.7.3.1	id-kp-serverAuth
		1.3.6.1.5.5.7.3.2	id-kp-clientAuth
issuerAltName	FALSE		Any name types may be present; only the most common are specified here.
rfc822Name		IA5String	Electronic mail address of the PKI administration
subjectAltName	FALSE		Any name types may be present; only the most common are specified here. Other names may be included to support local applications.
GeneralNames			
GeneralName			
dNSName		IA5String	This field contains the DNS name of the subject
iPAddress		IA5String	This field contains the IP address of the subject

A.6: Non-Federal SSP PIV-I Card Authentication Certificate Profile

Field	Criticality Flag	Value	Comments
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		INTEGER	Unique positive integer.
signature			
AlgorithmIdentifier			Must match Algorithm Identifier in signatureAlgorithm field. The parameters field is only populated when the algorithm is RSA.
algorithm		Choice of following algorithms:	
		1.2.840.113549.1.1.11	Sha256WithRSAEncryption
		1.2.840.10045.4.3.2	ecdsa-with-SHA256
parameters		NULL	
issuer			
Name			
RDNSequence			Must use one of the name forms specified in section 3.1.1 of the CPS.
validity			
notBefore		YYMMDDHHMMSSZ	
notAfter		YYMMDDHHMMSSZ	The notAfter time MUST not be after the PIV-I card expiration date.
subject			
Name			
RDNSequence			Must use one of the name form specified in section 3.1.1 of the CPS.
subjectPublicKeyInfo			
AlgorithmIdentifier			Public key algorithm associated with the public key. May be either RSA or elliptic curve.
algorithm		1.2.840.113549.1.1.1	RSA Encryption
		1.2.840.10045.2.1	Elliptic curve key
RSAParameters		NULL	For RSA, parameters field is populated with NULL.
subjectPublicKey		BIT STRING	For RSA public keys: certificates shall have a modulus of at least 2048 bits
required extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
keyUsage	TRUE		Only digitalSignature shall be set.
digitalSignature		1	
nonRepudiation		0	
keyEncipherment		0	
dataEncipherment		0	
extKeyUsage	TRUE		This extension shall assert only the *id-stn-ssp-pivi-cardAuth* keyPurposeID.

Field	Criticality Flag	Value	Comments
keyPurposeID		2.16.840.1.101.3.6.8	The *id-stn-ssp-pivi-cardAuth* keyPurposeID specifies that the public key is used to authenticate the PIV-I card rather than the PIV-I card holder.
certificatePolicies	FALSE		
PolicyInformation			One policy OID is specified for Card Authentication certificates. Other policy OIDs may be asserted and activated as well.
policyIdentifier		2.16.840.1.113733.1.7.23.3.1.17	*id-stn-ssp-pivi-cardAuth* (private key computations can be performed with the Card authentication key without user participation).
cRLDistributionPoints	FALSE		This extension is required in all end entity certificates and must contain at least one HTTP URI. The reasons and cRLIssuer fields must be omitted.
uniformResourceIdentifier		http://…	See preamble text on URIs.
authorityInfoAccess	FALSE		authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued for PIV-I must include an authorityInfoAccess extension with at least one instance of the caIssuers access method that specifies an HTTP URI. The OCSP access method must be included since the FBCA mandates OCSP distribution of status information for this certificate.
accessMethod		id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible Web server where certificates issued to the issuer of this certificate may be found.
accessLocation			
uniformResourceIdentifier		http://…	See preamble text on URIs.
accessMethod		id-ad-ocsp (1.3.6.1.5.5.7.48.1)	When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible OCSP server distributing status information for this certificate.
uniformResourceIdentifier		http://…	See preamble text on URIs.
subjectAltName	FALSE		
GeneralNames			Must only include UUID name form.
uniformResourceIdentifier		UUID	This field contains the UUID from the CHUID of the PIV-I card encoded as a URI as specified in Section 3 of RFC 4122.

A.7: Non-Federal SSP PIV-I Authentication Certificate Profile

Field	Criticality Flag	Value	Comments
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		INTEGER	Unique positive integer.
signatureAlgorithm		Choice of following algorithms:	
		1.2.840.113549.1.1.11	Sha256WithRSAEncryption
		1.2.840.10045.4.3.2	ecdsa-with-SHA256
issuerName			Must use one of the name forms specified in section 3.1.1 of the CPS.
validity			
notBefore		YYMMDDHHMMSSZ	
notAfter		YYMMDDHHMMSSZ	The notAfter time MUST not be after the PIV-interoperable card expiration date.
subjectName			This field must be populated with an X.500 distinguished name
RDNSequence			DN must use one of the name forms specified in section 3.1.1 of the CPS.
subjectPublicKeyInfo			
AlgorithmIdentifier			Public key algorithm associated with the public key.
algorithm		1.2.840.113549.1.1.1	RSA Encryption
		1.2.840.10045.2.1	Elliptic curve key
subjectPublicKey		BIT STRING	For RSA public keys: certificates shall have a modulus of at least 2048 bits.
required extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
keyUsage	TRUE		Only digitalSignature shall be set.
digitalSignature		1	
nonRepudiation		0	
keyEncipherment		0	
dataEncipherment		0	
keyAgreement		0	
keyCertSign		0	
cRLSign		0	
encipherOnly		0	
decipherOnly		0	
certificatePolicies	FALSE		
PolicyInformation			One policy OID for *id-stn-ssp-pivi-hardware* is specified for PIV-I Authentication certificates. Other policy OIDs may be asserted as well.
policyIdentifier		2.16.840.1.113733.1.7.23.3.1.18	*id-stn-ssp-pivi-hardware*

Field	Criticality Flag	Value	Comments
cRLDistributionPoints	FALSE		This extension is required in all end entity certificates and must contain at least one HTTP URI. The reasons and cRLIssuer fields must be omitted.
uniformResourceIdentifier		http://…	See preamble text on URIs.
authorityInfoAccess	FALSE		authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued for PIV-I must include an authorityInfoAccess extension with at least one instance of the caIssuers access method: that specifies an HTTP URI. The OCSP access method must be included since FBCA mandates OCSP distribution of status information for this certificate.
accessMethod		id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible Web server where certificates issued to the issuer of this certificate may be found.
uniformResourceIdentifier		http://…	See preamble text on URIs.
accessMethod		id-ad-ocsp (1.3.6.1.5.5.7.48.1)	When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible OCSP server distributing status information for this certificate.
uniformResourceIdentifier		http://…	See preamble text on URIs.
extKeyUsage		BOOLEAN	This extension MUST appear in certificates issued after June 30, 2018. The extension should be noncritical and shall not include the anyExtendedKeyUsage value. The values listed below for keyPurposeID are recommended for inclusion. Additional keyPurposeIds consistent with authentication purposes may be specified. Note: for certificates issued prior to June 30, 2018 anyExtendedKeyUsage may be present or the entire extension may be absent.
keyPurposeID		1.3.6.1.4.1.311.20.2.2	Microsoft Smart Card Logon
		1.3.6.1.5.5.7.3.2	TLS client authentication
		1.3.6.1.5.2.3.4	id-pkinit-KPClientAuth
subjectAltName	FALSE		
GeneralNames			This extension MUST include the UUID as specified below. Any additional name types may be present; only the most common are specified here. Other names may be included to support local applications.
GeneralName			
uniformResourceIdentifier		UUID	This field contains the UUID from the CHUID of the PIV-I card encoded as a URI as specified in Section 3 of RFC 4122.
otherName			Where supporting Microsoft *Smart Card Logon*, this name must be present
type-id		1.3.6.1.4.1.311.20.2.3	UPN OtherName OID
value		UTF8String	This field specifies Microsoft user principal name for use with Microsoft Windows logon.

Field	Criticality Flag	Value	Comments
optional extensions			

A.8: Non-Federal SSP PIV-I Digital Signature Certificate Profile

Field	Criticality Flag	Value	Comments
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		INTEGER	Unique positive integer.
signatureAlgorithm		Choice of following algorithms:	
		1.2.840.113549.1.1.11	Sha256WithRSAEncryption
		1.2.840.10045.4.3.2	ecdsa-with-SHA256
issuerName			Must use one of the name forms specified in section 3.1.1 of the CPS.
validity			
notBefore		YYMMDDHHMMSSZ	
notAfter		YYMMDDHHMMSSZ	The notAfter time MUST not be after the PIV-interoperable card expiration date.
subjectName			This field must be populated with an X.500 distinguished name
RDNSequence			If the DN is not NULL, must use one of the name forms specified in section 3.1.1 of the CPS.
subjectPublicKeyInfo			
AlgorithmIdentifier			Public key algorithm associated with the public key.
algorithm		1.2.840.113549.1.1.1	RSA Encryption
		1.2.840.10045.2.1	Elliptic curve key
subjectPublicKey		BIT STRING	For RSA public keys: certificates that expire on or after December 31, 2010 shall have a modulus of at least 2048 bits.
required extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
keyUsage	TRUE		digitalSignature and nonRepudiation shall be set.
digitalSignature		1	
nonRepudiation		1	
keyEncipherment		0	
dataEncipherment		0	
keyAgreement		0	
keyCertSign		0	
cRLSign		0	
encipherOnly		0	
decipherOnly		0	
certificatePolicies	FALSE		
PolicyInformation			One policy OID *id-stn-ssp-pivi-hardware* is specified for PIV-I Digital Signature certificates. Other policy OIDs may be asserted as well.
policyIdentifier		2.16.840.1.113733.1.7.23.3.1.18	*id-stn-ssp-pivi-hardware*

Field	Criticality Flag	Value	Comments
cRLDistributionPoints	FALSE		This extension is required in all end entity certificates and must contain at least one HTTP URI. The reasons and cRLIssuer fields must be omitted.
uniformResourceIdentifier		http://…	See preamble text on URIs.
extKeyUsage		BOOLEAN	This extension must appear in certificates issued after June 30, 2019. The extension should be noncritical and shall not include the anyExtendedKeyUsage value. The values listed below for keyPurposeID are recommended for inclusion. Additional keyPurposeIDs, consistent with signing purposes, may be specified. Note: For certificates issued prior to June 30, 2019, anyExtendedKeyUsage may be present or the entire extension may be absent.
keyPurposeID		1.3.6.1.5.5.7.3.4	id-kp-emailProtection
		1.3.6.1.4.1.311.10.3.12	MSFT Document Signing
authorityInfoAccess	FALSE		authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued for PIV-I must include an authorityInfoAccess extension with at least one instance of the caIssuers access method that specifies an HTTP URI. The OCSP access method must be included since FBCA mandates OCSP distribution of status information for this certificate.
accessMethod		id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible Web server where certificates issued to the issuer of this certificate may be found.
uniformResourceIdentifier		http://…	See preamble text on URIs.
accessMethod		id-ad-ocsp (1.3.6.1.5.5.7.48.1)	When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible OCSP server distributing status information for this certificate.
uniformResourceIdentifier		http://…	See preamble text on URIs.
optional extensions			
subjectAltName	FALSE		
GeneralName			
rfc822Name		IA5String	This field contains the electronic mail address of the subject.
AttributeType		OID	
AttributeValue			This field contains the electronic mail address of the subject.

A.9: Non-Federal SSP PIV-I Key Management Certificate Profile

Field	Criticality Flag	Value	Comments
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		INTEGER	Unique positive integer.
signatureAlgorithm		Choice of following algorithms:	
		1.2.840.113549.1.1.11	Sha256WithRSAEncryption
		1.2.840.10045.4.3.2	ecdsa-with-SHA256
issuerName			Must use one of the name forms specified in section 3.1.1 of the CPS.
validity			
notBefore		YYMMDDHHMMSSZ	
notAfter		YYMMDDHHMMSSZ	The notAfter time MUST not be after the PIV-interoperable card expiration date.
subjectName			This field must be populated with an X.500 distinguished name
RDNSequence			If the DN is not NULL, must use one of the name forms specified in section 3.1.1 of the CPS.
subjectPublicKeyInfo			
AlgorithmIdentifier			Public key algorithm associated with the public key.
algorithm		1.2.840.113549.1.1.1	RSA Encryption
		1.2.840.10045.2.1	Elliptic curve key
subjectPublicKey		BIT STRING	For RSA public keys: certificates shall have a modulus of at least 2048 bits.
required extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
keyUsage	TRUE		Only keyEncipherment shall be set.
digitalSignature		0	
nonRepudiation		0	
keyEncipherment		1	Asserted when public key is RSA.
dataEncipherment		0	
keyAgreement		1	Asserted when public key is elliptic curve.
keyCertSign		0	
cRLSign		0	
encipherOnly		0	
decipherOnly		0	
certificatePolicies	FALSE		
PolicyInformation			One policy OID *id-stn-ssp-pivi-hardware* must be present. Other policy OIDs may be asserted as well.
policyIdentifier		2.16.840.1.113733.1.7.23.3.1.18	*id-stn-ssp-pivi-hardware*

Field	Criticality Flag	Value	Comments
cRLDistributionPoints	FALSE		This extension is required in all end entity certificates and must contain at least one HTTP URI. The reasons and cRLIssuer fields must be omitted.
uniformResourceIdentifier		http://…	See preamble text on URIs.
extKeyUsage		BOOLEAN	This extension MUST appear in certificates issued after June 30, 2019. The extension should be noncritical and shall not include the anyExtendedKeyUsage value. The value listed below for keyPurposeID is recommended for inclusion. Additional keyPurposeIDs, consistent with key management purposes, may be specified. Note: For certificates issued prior to June 30, 2019, anyExtendedKeyUsage may be present or the entire extension may be absent.
keyPurposeID		1.3.6.1.5.5.7.3.4	Id-kp-emailProtection
authorityInfoAccess	FALSE		authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued for PIV-I must include an authorityInfoAccess extension with at least one instance of the caIssuers access method that specifies an HTTP URI. The OCSP access method must be included since FBCA mandates OCSP distribution of status information for this certificate.
accessMethod		id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible Web server where certificates issued to the issuer of this certificate may be found.
uniformResourceIdentifier		http://…	See preamble text on URIs.
accessMethod		id-ad-ocsp (1.3.6.1.5.5.7.48.1)	When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible OCSP server distributing status information for this certificate.
uniformResourceIdentifier		http://…	See preamble text on URIs.
optional extensions			
subjectAltName	FALSE		
GeneralNames			
GeneralName			
rfc822Name		IA5String	This field contains the email address of the subject.
AttributeType		OID	
AttributeValue			

A.10: Non-Federal SSP PIV-I Content Signing Certificate Profile

Field	Criticality Flag	Value	Comments
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		INTEGER	Unique positive integer.
signatureAlgorithm		Choice of following algorithms:	
		1.2.840.113549.1.1.11	Sha256WithRSAEncryption
		1.2.840.10045.4.3.2	ecdsa-with-SHA256
issuerName			Must use one of the name forms specified in section 3.1.1 of the CPS.
validity			
notBefore		YYMMDDHHMMSSZ	
notAfter		YYMMDDHHMMSSZ	The notAfter time MUST not be after the PIV-interoperable card expiration date.
subjectName			This field must be populated with an X.500 distinguished name
RDNSequence			If the DN is not NULL, must use one of the name forms specified in section 3.1.1 of the CPS.
subjectPublicKeyInfo			
AlgorithmIdentifier			Public key algorithm associated with the public key.
algorithm		1.2.840.113549.1.1.1	RSA Encryption
		1.2.840.10045.2.1	Elliptic curve key
subjectPublicKey		BIT STRING	For RSA public keys: certificates shall have a modulus of at least 2048 bits.
required extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
keyUsage	TRUE		
digitalSignature		1	digitalSignature must be asserted
nonRepudiation		0	
keyEncipherment		0	
dataEncipherment		0	
keyAgreement		0	
keyCertSign		0	
cRLSign		0	
encipherOnly		0	
decipherOnly		0	
extKeyUsage	YES		
KeyPurposeID		2.16.840.1.101.3.8.7	Id-fpki-pivi-content-signing
certificatePolicies	FALSE		
PolicyInformation			One policy OID *id-stn-ssp-pivi-contentSigning* must be present..
policyIdentifier		2.16.840.1.113733.1.7.23.3.1.20	*id-stn-ssp-pivi-contentSigning*

Field	Criticality Flag	Value	Comments
cRLDistributionPoints	FALSE		This extension is required in all end entity certificates and must contain at least one HTTP URI. The reasons and cRLIssuer fields must be omitted.
uniformResourceIdentifier		http://…	See preamble text on URIs.
authorityInfoAccess	FALSE		authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued for PIV-I must include an authorityInfoAccess extension with at least one instance of the calssuers access method: that specifies an HTTP URI. The OCSP access method must be included since FBCA mandates OCSP distribution of status information for this certificate.
accessMethod		id-ad-calssuers (1.3.6.1.5.5.7.48.2)	When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible Web server where certificates issued to the issuer of this certificate may be found.
uniformResourceIdentifier		http://…	See preamble text on URIs.
accessMethod		id-ad-ocsp (1.3.6.1.5.5.7.48.1)	When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible OCSP server distributing status information for this certificate.
uniformResourceIdentifier		http://…	See preamble text on URIs.
optional extensions			
subjectAltName	FALSE		If the subject name contains a DN, set criticality to FALSE. Otherwise set criticality to TRUE.
GeneralNames			This extension MUST include the UUID as specified below. Any additional name types may be present; only the most common are specified here. Other names may be included to support local applications.
GeneralName			
dNSName		IA5String	This field contains the DNS name of the subject
iPAddress		IA5String	This field contains the IP address of the subject
AttributeType		OID	
AttributeValue			

A.11: Non-Federal SSP OCSP Responder Certificate Profile

Field	Criticality Flag	Value	Comments
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		INTEGER	Unique positive integer.
signatureAlgorithm		Choice of following algorithms:	
		1.2.840.113549.1.1.11	Sha256WithRSAEncryption
		1.2.840.10045.4.3.2	ecdsa-with-SHA256
issuerName			Must use one of the name forms specified in section 3.1.1 of the CPS.
validity		No longer than 30 days from date of issue.	
subjectName			Unique X.500 OCSP Responder (subject) DN
subjectPublicKeyInfo			For RSA public keys: certificates shall have a modulus of at least 2048 bits.
algorithm		1.2.840.113549.1.1.1	RSA Encryption
		1.2.840.10045.2.1	Elliptic curve key
Required Extensions			
authorityKeyIdentifier	FALSE	OCTET STRING	Derived using the SHA-1 hash of the public key. Same as subject key identifier in Issuing CA certificate.
subjectKeyIdentifier	FALSE	OCTET STRING	Derived using the SHA-1 hash of the public key. Same as in PKCS-10 request or calculated by the Issuing CA
keyUsage	TRUE	digitalSignature	For SAFE, shall also include nonRepudiation.
certificatePolicies	FALSE		For SAFE, shall include all the certificate policy OIDs for which the Issuing CA issues certificates, and, a Policy Qualifier for the SAFE-mapped OID shall be present and express the following userNotice: "OCSP RESPONSE SUBJECT TO LIMITED LIABILITY/for SAFE use see SAFE CP at http://www.safe-biopharma.org/cp-pdf; other use see [COMPANY] CP at [URL]/CPs incorporated by reference":
authorityInfoAccess	FALSE	HTTP URL for the Issuing CA	id-ad-caIssuers (1.3.6.1.5.5.7.48.2)
subjectAltName		HTTP URL for the OCSP Responder	
extKeyUsage	BOOLEAN		
KeyPurposeID	TRUE	1.3.6.1.5.5.7.3.9	Id-kp-OCSPSigning
id-pkix-ocsp-nocheck	FALSE	NULL	OID=id-pkix-ocsp-nocheck, {1 3 6 1 5 5 7 48 1 5}

APPENDIX B: PIV-I CMS REQUIREMENTS

PIV-I Cards are issued and managed only through authorized Card Management Systems (CMSs). Organizations that deploy these systems have a responsibility to ensure a certain level of security from the CMSs that manage the token on which their certificates reside, and to which they issue certificates for the purpose of signing PIV-I Cards. This appendix provides requirements in addition to those found elsewhere that apply to CMSs within this CPS.

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

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

Individual personnel shall be specifically designated to the four Trusted Roles defined in section 5.2.1. Trusted Role eligibility and Rules for separation of duties follow the requirements for Medium assurance in section 5. All personnel who perform duties with respect to the operation of the CMS shall receive comprehensive training. Any significant change to CMS operations shall have a training (awareness) plan, and the execution of such plan shall be documented.

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

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

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

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

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

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- generate and archive audit records for all transactions; (see Section 5.4)
- enforce domain integrity boundaries for security critical processes; and
- support recovery from key or system failure.

APPENDIX C: PIV-I SMART CARD DEFINITION

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

The following requirements shall apply to PIV-I Cards:

1. To ensure interoperability with Federal systems, PIV-I Cards shall use a smart card platform that is on GSA's FIPS 201-2 Evaluation Program Approved Product List (APL) and uses the PIV application identifier (AID).
2. PIV-I Cards shall conform to [NIST SP 800-73[11]].
3. The mandatory X.509 Certificate for Authentication shall be issued under a policy that is cross certified with the FBCA PIV-I Hardware policy OID.
4. All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile].
5. PIV-I Cards shall contain an asymmetric X.509 Certificate for Card Authentication that:
    - Conforms to [PIV-I Profile];
    - Conforms to [NIST SP 800-73]; and
    - Is issued under the PIV-I Card Authentication policy.
6. PIV-I Cards shall contain an electronic representation (as specified in SP 800-73 and SP 800-76) of the Cardholder Facial Image printed on the card.
7. The X.509 Certificates for Digital Signature and Key Management described in [NIST SP 800-73] are optional for PIV-I Cards.
8. Visual distinction of a PIV-I Card from that of a Federal PIV Card is required to ensure no suggestion of attempting to create a fraudulent Federal PIV Card. At a minimum, images or logos on a PIV-I Card shall not be placed entirely within Zone 11, *Agency Seal*, as defined by [FIPS 201-2].
9. The PIV-I Card physical topography shall include, at a minimum, the following items on the front of the card:
    - Cardholder facial image;
    - Cardholder full name;
    - Organizational Affiliation, if exists; otherwise the issuer of the card; and
    - Card expiration date.
10. PIV-I Cards shall have an expiration date not to exceed 6 years of issuance.
11. Expiration of the PIV-I Card should not be later than expiration of PIV-I Content Signing certificate on the card.
12. The digital signature certificate that is used to sign objects on the PIV-I Card (e.g., CHUID, Security Object) shall contain a policy OID that has been mapped to the FBCA PIV-I Content Signing policy OID. The PIV-I Content Signing certificate shall conform to [PIV-I Profile].
13. The PIV-I Content Signing certificate and corresponding private key shall be managed within a trusted Card Management System as defined by Appendix B.
14. At issuance, the RA shall activate and release the PIV-I Card to the subscriber only after a successful 1:1 biometric match of the applicant against the biometrics collected in Section 3.2.3.1.

[11] *Special attention should be paid to UUID requirements for PIV-I.*

15. PIV-I Cards may support card activation by the card management system to support card personalization and post-issuance card update. To activate the card for personalization or update, the card management system shall perform a challenge response protocol using cryptographic keys stored on the card in accordance with [SP800-73].

    When cards are personalized, card management keys shall be set to be specific to each PIV-I Card. That is, each PIV-I Card shall contain a unique card management key. Card management keys shall meet the algorithm and key size requirements stated in Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification. [SP800-78]

KRPS Template

[Agency name]
Shared Service Provider PKI

Key Recovery
Practices Statement

Template Instructions:

This document provides a Key Recovery Practices Statement template that may be used by entities that conduct key management certificate decryption key escrow. If this KRPS template is used, it must be modified with the actual practices for key escrow and recovery used by the entity. Particularly when reference is made to requirements in the DigiCert SSP CPS the entity must use the example in the DigiCert NFI SSP CPS to know how to customize the entity's KRPS. In adapting this template, certain editorial changes must be made to personalize it, including: 1) change the Cover page to insert the name of the entity implementing a DigiCert-managed PKI, and 2) replace the "[RA name]" tags throughout the entire document.

1 INTRODUCTION

The idea of Key Recovery as espoused by the Federal Bridge PKI Key Recovery Policy (KRP) includes both key escrow, which is the archiving or escrowing of private keys, and the ability to recover escrowed private keys. The keys required under this policy to be escrowed are the decryption keys from a key management certificate. Since encryption keys are used to encrypt a variety of different data, entities need to have some way to recover these keys when required under special circumstances.

Any entity issuing key management certificates shall institute the KRP and escrow these decryption keys and have a process for recovering them. The system used for recovering keys is called the Key Recovery System (KRS). The KRS includes the Key Escrow Database (KED) and includes the Key Recovery Agent (KRA), the Key Recovery Officer (KRO), and the workstations used by KRAs and/or KROs to conduct recovery operations.

1.1 Overview

The purpose of this document is to describe the various systems, security practices, and personnel duties associated with an entity's key escrow and recovery activities. This Key Recovery Practices Statement Template requires that there are at least two KRAs present to recover any escrowed key from the KED. Subscribers may be permitted to recover their own keys from the KED, and do not need permission to do so as long as there is a process to require the Subscriber to authenticate to the KED. Entities are permitted to place the Historic key management decryption key(s) (previously issued, but now expired or not current for some other reason) onto the Subscriber's card at issuance.

1.2 Document name and identification

DigiCert Key Recovery Practices Statement *Template*

1.3 PKI Participants

1.3.1 PKI Authorities

The Federal Bridge PKI Policy Authority (FPKIPA) approves this [RA name] KRPS. The DigiCert PMA approves all changes to the *DigiCert NFI SSP KRPS Template*. Additional PKI Authorities include:

1.3.1.1 Key Escrow Database (KED)

The KED includes all the information systems used to provide key escrow and key recovery services for DigiCert NFI SSP Customers. It is comprised of the [RA name]-hosted Registration Authority (RA)[12] components and the DigiCert-hosted CA components, the Key Recovery Agent (KRA) Workstation and the Card Management System (CMS).

1.3.2 Key Recovery Authorities

1.3.2.1 Data Decryption Server

No stipulation
If an RA uses a Data Decryption Server the description goes here.

[12] *The KRS includes a component called an "RA component" dedicated to the key recovery operation. This component is not to be confused with the RA workstation used by RAs for enrollment of Subscribers for certificates.*

1.3.2.2 Key Recovery Agent (KRA)

[RA name] appoints trusted personnel as KRAs who are authorized, as specified in this KRPS Template to interact with the KRS in order to recover an escrowed key.

KRAs are Trusted Roles and subject to the requirements the subset of controls in section 5.2 for Procedural Controls. The full set of requirements for all Trusted Roles are found in the *DigiCert NFI SSP CPS* section 5.
[RA name] KRAs will:

- Acknowledge receipt of the KRPS and their responsibility to operate in accordance with the provisions of this KRPS.
- A KRA in coordination with a second KRA use multi-party access to the KED to recover an escrowed key.
- Protect Subscribers' escrowed keys from unauthorized disclosure, including the encrypted files and associated PKCS#12 passwords.
- Protect Subscribers' recovered keys from compromise. After providing the Requestor with the encrypted key, the KRA shall destroy the copy of the encrypted key and associated PKCS #12 password in his/her system.
- Protect all information, including the KRA key(s) that could be used to recover Subscribers' escrowed keys.
- Initiate the process to recover a Subscriber's escrowed key only upon receipt of a request from an authorized Requestor. The KRA shall authenticate the identity of the Requestor prior to initiating the key recovery.
- Validate the authorization for key recovery requests, to include consultation with legal counsel when appropriate.
- Release Subscribers' escrowed keys only for properly authenticated and authorized requests from Requestors.
- Protect all information regarding all occurrences of key recovery. KRAs shall communicate knowledge of a recovery process only to the Requestor involved in the key recovery. KRAs shall not communicate any information concerning a key recovery to the Subscriber except when the Subscriber is the Requestor.
- Keep records of all key recovery requests and dispositions, including acknowledgement of receipt by the Requestor. The audit records shall not contain Subscribers' keys in any form: plaintext, split, encrypted, etc.

1.3.2.3 Key Recovery Officer (KRO)

If a KRO is used by the RA, KROs are authorized to validate identity of a requestor. The KRO conducts identity verification and authorization validation tasks. They authenticate the Requestor. If the KRO has access to the KED, they shall be Trusted Roles, and adhere to the subset of requirements found in Section 5.2 Procedural Controls. The full set of requirements for all Trusted Roles are found in the *DigiCert NFI SSP CPS* section 5.

[RA name] KROs will:

- Acknowledge receipt of the KRPS and their responsibility to operate in accordance with the provisions of this KRPS.
- The KRO shall authenticate the identity of the Requestor prior to initiating the key recovery.
- Validate the authorization for key recovery requests, to include consultation with legal counsel when appropriate.

- Protect Subscribers' escrowed keys from unauthorized disclosure, including the encrypted files and associated PKCS#12 passwords.
- Protect Subscribers' recovered keys from compromise. After providing the Requestor with the encrypted key, the KRO shall destroy the copy of the encrypted key and associated PKCS #12 password in his/her system.

1.3.3 Trusted Agents

See the *DigiCert NFI SSP CPS* section 5.2. Trusted Agents validate identity of a Requestor for certificate issuance, and that is the job of the KRO or KRA in key recovery operations.

1.3.4 Key Recovery Requestors

A Requestor is the person who requests the recovery of a private encryption key. A Requestor is the Subscriber of the certificate or a third party (e.g., supervisor, corporate officer or law enforcement officer) who is authorized to request recovery of a Subscriber's escrowed key.

1.3.4.1 Subscriber

A Subscriber is the individual named in the Subject DN in the certificate to be recovered. For devices the human Sponsor becomes the Subscriber.

1.3.4.2 Internal Requestor

An Internal Requestor is the Subscriber or anyone who is in the Subscriber's supervisory chain or otherwise authorized to obtain the Subscriber's key for the organization. The intent of the KRPS is not to change the policy and procedures of the organization. [RA name] identifies authorized Requestors to ensure that its existing organization policy regarding access and release of sensitive information can be met.

1.3.4.3 External Requestor

An External Requestor is an investigator or someone outside of [RA name] with an authorized court order to obtain the private encryption key of the Subscriber. Such court orders shall be validated by the KRA prior to recovering a key. An external Requestor must work with an internal Requestor unless the law requires the organization to release the Subscriber's private key without approval of the Subscriber and [RA name]. The intent of the KRPS is not to change the current procedures for obtaining information about individuals in connection with such requests. [RA name] appoints authorized personnel and implements the KRPS so that the existing organization policy can be met while releasing the escrowed private key.

A KRA validates the authorization of the Requestor in consultation with management and legal counsel, as appropriate.

1.3.5 Relying Parties

Not Applicable

1.3.6 Other Participants

Not Applicable

1.3.7 Relationship to PKI Authorities from CP

The applicable requirements for physical security, personnel, technical security controls, and the procedural security controls are found in the *DigiCert NFI SSP CPS* in sections 5 and 6 and are not discussed in detail in this KRPS. These requirements apply to the following key escrow and recovery systems:

- CA requirements are applied to the KED and to the Data Encryption Server [maintained by the RA];
- RA requirements are applied to the KRA and automated KRA systems; and
- RA requirements are applied to the KRO and automated KRO systems when the KRO has access to the KED.

1.4 Certificate Usage

Not Applicable

1.5 Policy Administration

The DigiCert PMA is responsible for approving this KRPS.

1.6 Definitions and Acronyms

See the *DigiCert SSP CPS* Appendixes B and C

2 Publication and Repository Responsibilities

Not Applicable

3 IDENTIFICATION AND AUTHENTICATION

The Requestor's identity and authorization to access the requested escrowed key is verified prior to recovering an escrowed key. The Requestor's authenticated identity is used as the basis for determining access permissions and providing Requestor accountability.

3.1 Naming

Not Applicable

3.2 Identity Validation

Identity authentication is based on the activities specified by section 3.2 in the *DigiCert NFI SSP CPS* for authentication of individual identity during initial certificate enrollment or will be based on digital signatures that can be verified using [RA name] public key certificates.

A Requestor may appear before a KRA for in-person identity proofing. If identity authentication is based on digital signatures, the assurance level of a certificate used for identity authentication of a Requestor will be commensurate with the assurance level of the NFI SSP certificate associated with the key being recovered.

3.2.1 Method to Prove Possession of Private Key

Not Applicable

3.2.2 Authentication of Organization Identity

Any third-party Requestor must prove his or her authority to request a key on behalf of the organization he or she represents during identity proofing according to section 3.2.3.1 below.

3.2.3 Authentication of Individual Identity

3.2.3.1 Third-Party Requestor Authentication

A third-party Requestor is an individual other than the Subscriber and may be a representative of [RA name] (i.e., an internal requestor), or, for example, a representative of a law enforcement agency (i.e., an external requestor).

The following subsections identify the requirements for authentication and authorization of a third-party Requestor.

Organization Representative
All organization representatives must appear before a KRA prior to requesting recovery of a private key belonging to a Subscriber in this organization. The Requestor must establish his or her identity to a KRA who will personally verify the identity of the Requestor using the procedures defined in section 3.2 of the *DigiCert NFI SSP CPS* for initial Subscriber enrollment.

Law Enforcement Representative
If the Requestor is a representative of a law enforcement agency, the Requestor must establish his or her identity to a KRA who will personally verify the identity of the Requestor using the procedures defined in section 3.2 of the *DigiCert NFI SSP CPS* for initial Subscriber enrollment.

3.2.3.1.1 Requestor Authorization Verification

The KRA that performs identity authentication of a Requestor also performs the authorization verification of the Requestor.

If the Requestor is an authorized representative of the Subscriber's organization, the KRA validates their authorization in accordance with the procedures specified in the [RA name]'s policy to verify that the Requestor is authorized to request recovery of the Subscriber's key.

If the Requestor is not an authorized representative of the Subscriber's organization, the KRA reviews the Requestor-submitted court-issued subpoena or order and will validate the authorization of the Requestor in consultation with management and legal counsel, as appropriate. Any consultation with the Legal or Human Resources department [RA name] is subject to applicable law.

3.2.3.2 Subscriber Authentication

If the Subscriber has a current, valid [RA name] certificate, he/she may authenticate by sending a digitally signed message directly to a KRA. The assurance level of the authentication certificate used shall be equal to or greater than that of the certificate whose corresponding private key is being recovered. A KRA will authenticate the identity of the Subscriber by validating the digital signature on the message.

If the Subscriber does not have a current or valid [RA name] certificate or chooses not to authenticate by sending a digitally signed message, the Subscriber must establish his or her identity by personally appearing before a KRA for personal presence identity proofing in accordance with identity authentication specified in section 3.2 of the *DigiCert NFI SSP CPS.*

For automated self-recovery the Subscriber will authenticate to the KED using a valid (i.e. not revoked or expired) digital certificate issued at an assurance level equal to or greater than the key management key being recovered.

3.2.3.3 KRA Authentication

KRAs are trusted organizational personnel as stipulated in section 5.3 of the *DigiCert NFI SSP CPS*.
The KRA authenticates to the KRA workstation using a [RA name] certificate with the KRA key pair generated and stored on FIPS 140-1 Level 2 hardware token. The KRA also authenticates to the CMS using a certificate stored on FIPS 140-1 Level 2 hardware token.

Identity proofing of the KRA is done as defined in section 3.2 of the *DigiCert NFI SSP CPS*.

3.2.3.4 KRO Authentication

A KRO that is authorized to access the [RA name] KED, must adhere to all the requirements for authentication levied on the KRA in the previous section 3.2.3.3 above.

3.2.3.5 Data Decryption Server Authentication

If the RA deploys and uses a Data Decryption Server this server shall authenticate to the KED using a public key certificate issued by the RA, and the assurance level of this public key certificate shall be of an assurance level equal to or greater than all certificates issued by the RA PKI.

3.2.4 Non-Verified Subscriber Information

Not Applicable

3.2.5 Validation of Authority

3.2.5.1 Requestor Authorization Validation

The KRA, or the KRO acting on behalf of the KRA will validate the authorization of the Requestor, in coordination with [RA name] management and/or legal counsel as appropriate.

3.2.5.2 Subscriber Authorization Validation

Subscribers with proper affiliation with the organization may recover their own escrowed key management keys.

3.2.5.3 KRA Authorization Validation

The KED verifies that the authenticating KRA has appropriate privileges to obtain the keys for the [RA name] Subscriber.

3.2.5.4 KRO Authorization Validation

The KED or the KRA will verify that the KRO is authorized to request keying material for the authorized Subscriber.

3.2.5.5 Data Decryption Server Authorization Validation

If a data decryption server is utilized in the organization, the KED shall verify that it is within the scope for which the data decryption server was established to conduct key operations for the organization.

3.2.6 Criteria for Interoperation

Not Applicable

3.3 Identification and Authentication for Rekey Requests

Not Applicable

3.4 Identification and Authentication for Rekey After Revocation

Not Applicable

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Key Recovery Application

4.1.1 Who Can Submit a Key Recovery Application

Subscribers may request recovery of their own escrowed keys. Key recovery may also be requested by the personnel permitted by the [RA name] organization policy and by law enforcement personnel with court order from a competent court.

4.1.2 Key Escrow Process and Responsibilities

Subscriber private decryption keys associated with a key management certificate are securely escrowed by [RA name]. DigiCert ensures the keys are successfully escrowed prior to issuance.

Escrowed keys are protected during delivery to the Requestor by [RA name] defined process.

4.1.3 Key Recovery Process and Responsibilities

Persons requesting recovery of escrowed keys are required to provide sufficient information that can be used to verify their identity and authorization according to section 3 Identification and Authentication of the *DigiCert NFI SSP CPS*.

Subscribers may use electronic or manual means to request their own escrowed keys. If the request is made electronically, the Subscriber will digitally sign the request using a [RA name] certificate of assurance level equal to or greater than that of the escrowed key. Manual requests must be in writing and be signed by hand. Third party Requestors may use electronic or manual means to request recovery of a Subscribers' escrowed key. The Requestor must submit the request to a KRA. If the request is made electronically, the Requestor must digitally sign the request using an NFI SSP Certificate of assurance level equal to or greater than that of the escrowed key. Manual requests must be in writing and be signed by hand.

Requests from law enforcement must be under cover of a court-issued subpoena or order authorizing a particular law enforcement official or department to recover a Subscriber's encryption key.

4.2 Certificate Application Processing

Not Applicable

4.3 Certificate Issuance

Not Applicable

4.4 Certificate Acceptance

Not Applicable

4.5 Key Pair and Certificate Usage

Not Applicable

4.6 Certificate Renewal

Not Applicable

4.7 Certificate Rekey

Not Applicable

4.8 Certificate Modification

Not Applicable

4.9 Certificate Revocation and Suspension

The key management certificates associated with a [RA name] recovered decryption key shall not be revoked simply because the key was recovered. See the *DigiCert NFI SSP CPS* for all other reasons and example practices for revocation.

4.10 Certificate Status Services

Not Applicable

4.11 End of Subscription

Not Applicable

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

Refer to the Template Instructions at the start of this KRPS Template regarding frequent references to the DigiCert NFI SSP CPS from here on out. Much of the next two sections 5 and 6 are not particular to the KRS and the roles using it, so **[RA name]** ***is directed to insert its own practices*** *in these sections.*

5.1 Physical Controls

The KRS is protected with physical controls to minimize unauthorized access in accordance with RA protections specified in the *DigiCert NFI SSP CPS*.

PIV-I CMS equipment containing the PIV-I Content Signing key meets the physical access requirements specified in section 5.1 in the *DigiCert NFI SSP CPS*.

5.2 Procedural Controls

5.2.1 Trusted Roles

It is acceptable for the same person to hold multiple trusted roles on the PKI and the KRS. For example, a person may be a system administrator on the PKI and the KED, and an RA may also serve as a KRA or KRO. The audit administrator for the PKI may also audit the KED and data decryption server in the [RA name] KRS.

5.2.1.1 KED Roles

5.2.1.1.1 System Administrator

[RA name] System Administrators are authorized to configure and maintain the various KRS operating systems including the hypervisors. They can create and maintain system and user accounts, configure operating system audit logging, and perform system backup and recovery.

5.2.1.1.2 Application Administrator

[RA name] Application Administrators are authorized to install, configure and maintain the various KRS application software. They are the only role that may generate KED keys. Additionally, this role will configure and maintain access controls to the KRS and configure audit logging.

5.2.1.1.3 Audit Administrator

[RA name] Audit Administrators are authorized to review, maintain, and archive KRS audit logs.

5.2.1.2 Data Decryption Server Roles

If applicable the RA shall utilize the same roles as for the rest of the KRS and the same persons may perform the same duties on both.

5.2.1.2.1 System Administrator

See KED Roles.

5.2.1.2.2 Application Administrator

See KED Roles

5.2.1.2.3 Audit Administrator

See KED Roles

5.2.1.3 Key Recovery Agent

KRAs are subject to the provisions in this KRPS. Their role and the corresponding procedures include:

- Authenticating a request for key recovery;
- Validating the requestor's authorization;
- Requesting the escrowed key from the KRS using the KRA workstation or optionally the CMS; and
- Securely delivering the key to the Requestor.

5.2.1.4 Key Recovery Official

[RA name] KROs are subject to the stipulations under this KRPS. KROs are responsible only for verifying and authenticating Requestor identity and may participate in distributing recovered keys in accordance with the KRA. KROs are given the following functions:

- Verify a Requestor's identity and authorization;
- Build key recovery requests on behalf of a Requestor;
- Securely communicate key recovery requests to the KRA and responses from the KRA; and
- Participate in the distribution of recovered keys to the Requestor in accordance with the KRA.

5.2.2 Number of Persons Required per Task

Two or more persons are required for the following tasks:

- KED key generation
- Data decryption server key generation
- KED private key backup
- Data decryption server private key backup

Where multiparty control is required, other than for key recovery operations which particularly require two KRAs, at least one of the parties is a System Administrator. All persons serving in the KRS environment are trusted roles as per section 5.2.1 Trusted Roles in the *DigiCert NFI SSP CPS*. Auditors do not serve in a capacity to provide multiparty control.

[RA name] KRAs/KROs do not perform any duties performed by the System Administrator, Application Administrator or System Auditor.

Two KRAs are required to perform a third-party key recovery.

5.2.3 Identification and Authentication for Each Role

All [RA name] KRS Trusted Roles securely identify himself or herself before performing any action permitted for that role.

5.2.4 Roles Requiring Separation of Duties

In the [RA name] KRS, no one individual performs more than one role at a time. One individual serves in only one of the roles listed in 5.2.1 Trusted Roles above. None of these roles may perform the same role on both the KED and data decryption server (if applicable).

5.3 Personnel Controls

See section 5.3 Personnel Controls in the *DigiCert NFI SSP CPS*.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

See section 5.4.1 Types of Events Recorded in the *DigiCert NFI SSP CPS* for more details.

The Trusted Role of KRA is similar to that of RA so all controls for the RA and CMS meet the requirements for the KRA and KED

5.4.2 Frequency of Processing Logs

Conducting audits of the KED and KRS environment is done in correlation with other audit duties found in section 5.4.2 Frequency of Processing Logs in the *DigiCert NFI SSP CPS.*

5.4.3 Retention Period for Audit Log

Audit logs for the KED and KRA and/or KRO are retained in the same manner as described in section 5.4.3 Retention Period of Audit Log in the *DigiCert NFI SSP CPS.*

5.4.4 Protection of Audit Logs

Audit logs for the KED and KRA and/or KRO are protected in the same manner as described in section 5.4.4 Protection of Audit Logs in the *DigiCert NFI SSP CPS.*

5.4.5 Audit Log Backup Procedures

Audit logs for the KED and KRA and/or KRO are backed up in the same manner as described in section 5.4.5 Audit Log Backup Procedures in the *DigiCert NFI SSP CPS.*

5.4.6 Audit Collection System (internal vs. external)

The [RA name] audit log collection system for the KED and KRA and/or KRO is the same as described in the *DigiCert NFI SSP CPS* in the same section.

5.4.7 Notification to Event-causing Subject

There is no requirement to notify anyone of any event and no one including the Subscriber shall be notified of a third-party key recovery operation.

5.4.8 Vulnerability Assessments

[RA name] conducts vulnerability assessments across the enterprise and includes all components of the KRS including KRA and/or KRO workstations. Practices are aligned to those included in the *DigiCert NFI SSP CPS* in the same section.

5.5 Records Archival

KRS Records are archived in accordance with the practices stated in section 5.5 subsections Records Archival in the *DigiCert NFI SSP CPS.*

5.5.1 Types of Information Recorded

[RA name] archives the following information from the KRS:

- This KRPS
- Agreements with all KRAs/KROs, and key recovery request forms
- Audit data
- Escrowed keys

Any software needed to read or execute any archived information, including escrowed keys is maintained for the entire retention period required in the next section.

5.5.2 Retention Period for Archive

[RA name] retains KRS artefacts for ten (10) years six (6) months in accordance with the section 5.5.2 Retention Period for Archive in the *DigiCert NFI SSP CPS.*

5.5.3 Protection of Archive

Protection of the [RA name] KED archive conforms with the requirements found in the same section 5.5.3 Protection of Archive in the *DigiCert NFI SSP CPS* section 5.5.3.

5.5.4 Archive Backup Procedures

[RA name] does not perform any other archive backups than that required in the *DigiCert NFI SSP CPS.*

5.5.5 Requirements for Time-Stamping of Records

[RA name] has configured KRS records to be time-stamped as they are created, as appropriate; for instance, paper records will contain a written date and time. Digital records are time-stamped at creation using Network Time Protocol based on atomic clock signals through GPS.

5.5.6 Archive Collection System (internal vs external)

The RA shall give details on how archives are collected. Examples may include utilization of some log collection utility such as Splunk.

5.5.7 Procedures to Obtain and Verify Archive Information

[RA name] will refer to the *DigiCert NFI SSP CPS* for requirements on how archive information is obtained and verified.

5.6 Key Changeover

[RA name] has a process that ensures KED keys are changed over when necessary to ensure they are as strong as the keys being protected.

The KRA/KRO and the data decryption server (if applicable) are considered end entities when issued certificates and their keys are changed in accordance with the requirements found in the *DigiCert NFI SSP CPS*.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

[RA name] will refer to the *DigiCert NFI SSP CPS* for requirements on incident and compromise handling procedures.

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

[RA name] will refer to the *DigiCert NFI SSP CPS* for requirements associated with the corruption of KRS computing resources, software, and/or data.

`5.7.3 Agency (KRS) Private Key Compromise Procedures

[RA name] will refer to the *DigiCert NFI SSP CPS* for requirements on private key compromise procedures, in section 5.7.3 RA Private Key Compromise Procedures.

5.7.4 Business Continuity Capabilities After a Disaster

[RA name] will refer to the *DigiCert NFI SSP CPS* for requirements on business continuity capabilities to restore the KRS after a disaster.

5.8 Authority Termination

5.8.1 KED Termination

Upon terminating the KED the KRS will archive appropriate KED records in accordance with 5.5 Records Archival above.

5.8.2 KRA Termination

When a KRA is terminated the KRS takes possession of all KRA records.

5.8.3 KRO Termination

When a KRO is terminated the KRS takes possession of all KRO records.

5.8.4 Data Decryption Server Termination

If applicable: When the data decryption server is terminated, the KRS takes possession of all data decryption server records.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

[RA name] will refer to the *DigiCert NFI SSP CPS* for key pair generation requirements beyond that required in key escrow and recovery operations.

6.1.2 Private Key Delivery to Subscriber

[RA name] will refer to section 6.1.2 Private Key Delivery to Subscriber in the *DigiCert NFI SSP CPS* for private key delivery requirements beyond that required in key escrow and recovery operations.

6.1.3 Public Key Delivery to Certificate Issuer

Not Applicable

6.1.4 CA Public Key Delivery to Relying Parties

Not Applicable

6.1.5 Key Sizes

Not Applicable

6.1.6 Public Key Parameters Generation and Quality Checking

Not Applicable

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

Not Applicable

6.2 Private Key Protection and Cryptographic Module Engineering Controls

[RA name] will refer to section 6.2 Private Key Protection in the *DigiCert NFI SSP CPS* for private key protection requirements that also pertain to key escrow and recovery operations.

6.3 Other Aspects of Key Pair Management

[RA name] will refer to section 6.3 Other Aspects of Key Pair Management in the *DigiCert NFI SSP CPS* for key pair management requirements that also pertain to key escrow and recovery operations.

6.4 Activation Data

[RA name] will refer to section 6.4 Activation Data in the *DigiCert NFI SSP CPS* for activation data requirements that also pertain to key escrow and recovery operations.

6.5 Computer Security Controls

[RA name] will refer to the *DigiCert NFI SSP CPS* for complete requirements for computer security controls in the KED.

If the RA uses remote administration for the KED and/or Data Decryption Server, the RA shall not eliminate the requirement for two-person access control to the environment.

[RA name] utilizes KRA and KRO workstation controls that include the following:

- Discretionary access controls (DAC);
- Internal audit;
- Authentication and authorization of logins;
- A trusted path for authentication and authorization of logins;
- Protection for storage objects such as memory, disk sectors, and device registers;
- Operating system self-protection; and
- Domain isolation for application processes.

6.6 Life Cycle Technical Controls

[RA name] will use the *DigiCert NFI SSP CPS* in the same section for details on Life Cycle Technical Controls.

6.7 Network Security Controls

[RA name] will use the *DigiCert NFI SSP CPS* in the same section for details on Network Security Controls. This includes protection against network access to a KRA/KRO workstation using these controls: the *RA shall choose one or more as applicable to its environment.*

- *Network guard*
- *Firewall*
- *Filtering router*

These devices are configured to limit services to and from the KRA/KRO workstation to only those required to perform the KRA and/or KRO functions. The KRA/KRO workstation is protected against:

- currently known network attacks
- Unused network ports and services are turned off
- Only network software required for the function of the KRA/KRO duties is allowed on the workstation

6.8 Time Stamping

[RA name] will use the *DigiCert NFI SSP CPS* in the same section for details on Time Stamping.

7 Certificate, CRL, and OCSP Profiles

Not Applicable

8 Compliance Audit and Other Assessments

[RA name] will use the *DigiCert Certificate Policy* and the *DigiCert NFI SSP CPS* in the same section for details on Compliance Audit.

9 Other Business and Legal Matters

9.1 Fees

No stipulation for key escrow and key recovery services.

9.2 Financial Responsibility

[RA name] will use the *DigiCert Certificate Policy* and the *DigiCert NFI SSP CPS* for details on Section 9.2.

9.3 Confidentiality of Business Information

[RA name] will use the *DigiCert Certificate Policy* and the *DigiCert NFI SSP CPS* for details on Section 9.3.

9.4 Privacy of Personal Information

[RA name] will use the *DigiCert Certificate Policy* and the *DigiCert NFI SSP CPS* for details on Section 9.4.

9.5 Intellectual Property Rights

[RA name] will use the *DigiCert Certificate Policy* and the *DigiCert NFI SSP CPS* in the same section for details on Section 9.5.

9.6 Representations and Warranties.

[RA name] will use the *DigiCert Certificate Policy* and the *DigiCert NFI SSP CPS* in the same section for details on Section 9.6.

9.6.1 KED Representations and Warranties

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

- The DigiCert PMA shall approve the KRPS prior to key escrow.
- The KED shall operate in accordance with the stipulations of this KRPS.
- The KED shall automatically notify the subscribers when their private keys have been escrowed (e.g., a dialog box may appear on a subscriber's screen during the certificate request process).

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

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

9.6.2 KRA/KRO Representations and Warranties

9.6.2.1 KRA Obligations:

KRAs that submit requests as described in this KRPS shall comply with the stipulations of this KRPS. In particular, the following stipulations apply:

- KRAs shall keep a copy of this KRPS.
- KRAs shall operate in accordance with the stipulations of this KRPS.
- KRAs shall protect subscribers' escrowed keys from unauthorized disclosure, including the encrypted files and associated decryption keys.

- KRAs shall protect all information associated with key recovery, including the KRA's own key(s), that could be used to recover subscribers' escrowed keys.
- KRAs may rely upon the KROs for authentication and verification of the identity and authority of the Requestor. However, KRAs shall also authenticate the identity of the Requestor when the Requestor digital signature is available.
- KRAs shall release Subscribers' escrowed keys only for properly authenticated and authorized requests from Requestors.
- When applicable, KRAs shall authenticate the KROs using strong authentication techniques.
- KRAs shall validate the authorization of the KRO by ensuring that the KRO is an authorized KRO for the Subscriber for whom key recovery has been requested.
- KRAs shall protect all information regarding all occurrences of key recovery.
- KRAs shall communicate knowledge of a recovery process only to the KRO and Requestor involved in the key recovery.
- KRAs shall not communicate any information concerning a key recovery to the Subscriber except when the Subscriber is the Requestor.
- KRAs shall monitor KRO activity for patterns of potentially anomalous behavior as indicators of possible problems in the infrastructure, and initiate inquiries or investigations as appropriate.

9.6.2.2 KRO Obligations

A KRO initiates a key recovery request for a Requestor. When using the services of a KRO, the Requestor is generally a third party, but this KRPS does not preclude the Subscriber from seeking the assistance of a KRO to recover the Subscriber's private key.

- The KRO shall protect Subscribers' recovered keys from compromise.
- After providing the Requestor with the encrypted key, the KRO shall destroy the copy of the key in his/her system.
- The KRO shall request the Subscriber's keys only upon receipt of a request from an authorized Requestor.
- The KRO, as an intermediary for the KRA, shall validate the identity of any Requestor seeking a key recovery.
- When the Requestor is authenticated on the basis of digital signature, the KRO shall forward the Requestor's digitally signed object to the KRA in a form verifiable by the KRA.
- In the case of persons other than the Subscriber seeking a key recovery, the KRO shall ensure that the Requestor has the authority to request the Subscriber's private decryption key.
- The KRO, as an intermediary for the KRA, shall validate the authorization for the request, to include consultation with legal counsel when appropriate.
- The KRO shall protect all information associated with key recovery, including the KRO's own private key(s), that could be used to obtain the Subscriber's recovered private decryption key(s).
- The KRO shall protect all information regarding all occurrences of key recovery.
- The KRO shall communicate knowledge of any recovery process only to the Requestor.
- The KRO shall not communicate any information concerning a key recovery to the Subscriber except when the Subscriber is the Requestor.
- The KRO shall accurately represent himself when requesting key recovery services.
- The KRO shall keep records of all recovery requests and disposition, including acknowledgement of receipt by the Requestor.

If an Issuing Organization chooses not to implement the KRO role, then these obligations become the responsibility of the KRA in addition to the obligations in Section 9.6.2.1 above.

9.6.3 Subscriber Representations and Warranties

Subscribers shall comply with the following:

- Subscribers shall provide accurate identification and authentication information during initial and subsequent key recovery requests.
- When the Subscriber is notified that his or her escrowed key has been recovered, the Subscriber shall determine whether revocation of the pubic key certificate associated with the recovered key is necessary. The Subscriber shall request the revocation, if necessary.

9.6.4 Requestor Representations and Warranties

- Prior to receiving a recovered key, the Requestor must formally acknowledge and agree to the obligations described here.
- Requestors shall protect Subscribers' recovered key(s) from compromise. Requestors shall use a combination of computer security, cryptographic, network security, physical security, personnel security, and procedural security controls to protect their keys and recovered Subscribers' keys.
- Third-party Requestors shall destroy Subscribers' keys when no longer required (i.e., when the data has been recovered).
- Requestors shall request and use the Subscriber's escrowed key(s) only to recover Subscriber's data they are authorized to access.
- Requestors shall accurately represent themselves to all entities during any key recovery service.
- When the request is made to a KRO, the Requestor shall provide accurate identification and authentication information at least to the same level required for issuing new PKI certificates at the level of the key being requested (e.g. the Requestor sends a digitally signed request using the credential issued by the [RA name] PKI at the same or higher assurance level as the key being recovered).
- The Third-Party Requestor shall protect information concerning each key recovery operation.
- The Third-Party Requestor shall communicate information concerning the recovery to the Subscriber when appropriate as determined by the reason for the recovery. The decision to notify the Subscriber shall be based on the law and 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 shall consult with the Subscriber to determine whether or not the recovery circumstances warrant revoking the associated public key certificate.
- As a condition of receiving a recovered key, a Requestor shall sign an acknowledgement of agreement to follow the law and 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 shall signıan 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 the KRO, and truthfully described all reasons that I require access to data protected by the recovered key. I acknowledge my responsibility to use this recovered key only for the stated purposes, to protect it from further exposure, and to destroy all key materials or return them to the KRO 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."

9.6.5 Representations and Warranties of Other Participants

9.6.5.1 Data Decryption Server Representations and Warranties

If Applicable:

Prior to the beginning of the operation of a data decryption server, the Issuing Organization shall formally acknowledge and agree to the obligations described here by signing an appropriate document.

- The data decryption server shall protect Subscribers' recovered key(s) from compromise. The data decryption server shall use a combination of computer security, cryptographic, network security, physical security, personnel security, and procedural security controls to protect their keys and recovered subscribers' keys.
- The data decryption server shall destroy Subscribers' keys when no longer required (i.e., when the data has been recovered).
- The data decryption server shall request the Subscriber's escrowed key(s) only upon receiving a request to decrypt subscriber data from an authenticated authorized Enterprise system (e.g., an e-mail Server)
- The data decryption server shall use the Subscriber's recovered keys only to recover Subscriber's data requested from an authenticated authorized Enterprise system (e.g., an e-mail Server)
- The data decryption server shall provide accurate identification and authentication information at the same or higher assurance level as required for issuing new PKI certificates at the assurance level of the key being requested.

9.7 Disclaimers of Warranties

This KRS operating under this KRPS may not disclaim any responsibilities described in the Federal Bridge KRP.

9.8 Limitations of Liability

[RA name] will use the *DigiCert Certificate Policy* and the *DigiCert NFI SSP CPS* in the same section for details on Section 9.8

9.9 Indemnities

[RA name] will use the *DigiCert Certificate Policy* and the *DigiCert NFI SSP CPS* in the same section for details on Section 9.9

9.10 Term and Termination

9.10.1 Term

This KRPS becomes effective when approved by the DigiCert PMA. This KRPS has no specified term.

9.10.2 Termination

Termination of this KRPS is at the discretion of the DigiCert PMA.

9.10.3 Effect of Termination and Survival

The requirements of this KRPS remain in effect through the end of the archive period for the certificate corresponding to the last escrowed key.

9.11 Individual Notices and Communications with Participants

[RA name] will use the *DigiCert Certificate Policy* and the *DigiCert NFI SSP CPS* in the same section for details on Section 9.11.

9.12 Amendments

This KRPS shall be subject to the requirements set forth for the *DigiCert Certificate Policy* and the *DigiCert NFI SSP CPS* in the same section for details on Section 9.12.

9.13 Dispute Resolution Provisions

[RA name] will use the *DigiCert Certificate Policy* and the *DigiCert NFI SSP CPS* in the same section for details on Section 9.13.

9.14 Governing Law

[RA name] will use the *DigiCert Certificate Policy* and the *DigiCert NFI SSP CPS* in the same section for details on Section 9.14.

9.15 Compliance with Applicable Law

[RA name] will use the *DigiCert Certificate Policy* and the *DigiCert NFI SSP CPS* in the same section for details on Section 9.15.

9.16 Miscellaneous Provisions

[RA name] will use the *DigiCert Certificate Policy* and the *DigiCert NFI SSP CPS* in the same section for details on Section 9.16.

9.17 Other Provisions

[RA name] will use the *DigiCert Certificate Policy* and the *DigiCert NFI SSP CPS* in the same section for details on Section 9.17.

Appendix E: Revision History

Version	Date / Status	Revision Details
2.3	April 2020	Changes to address FPKI Comments from 2019 Annual SSP NFI Review.
2.2	May 2018	Comprehensive changes to address corporate ownership change from Symantec to DigiCert
2.1	November 2017	Initial changes to address corporate ownership change from Symantec to DigiCert
2.0	February 2017	Changes to Address Symantec 2016 Annual Review Comments from FPKI
1.24	October 2012	2012-01 – updates for RA & CMS audits (sections 1.3.1.2, 1.3.1.3, 8.0-8.6, glossary)
	March 2012	Modifications to comply with Change Proposals: 2010-05 –Section 3.2.3.1 - REAL ID credential accepted for identity proofing 2010-06 – Section 3.2.3.1 & 4.9.1 – Declaration of identity signature may be digitally signed. 2011-01 – section 3.2.3.1 – controls for databases supporting validation of subscriber attributes. 2011-02 – section 5.3.2 – Trusted Roles background check shall be refreshed every 10 years. 2011-03 – section 6.1.1.2 – clarification that for PIV-I certs used for digital sig or authentication, keys shall be generated in a h/w token (not generated by the CA). 2011-04 – Appx B - CMS system personnel are governed by the Trusted Roles eligibility & separation of duties in section 5. 2011-05 – n/a. 2011-06 – throughout doc – removed all references to LDAP services. 2011-07 – sections 1.1, 1.2, 1.3.4, 3.1.1, 3.2.3.4, 6.1.1.2, 6.2.1, 6.2.3.4, 6.2.4.6, 6.2.6, 6.2.8, A.1, A.5 – added policy for *id-fpki-mediumDevicesHardware*
		Section 4.9.9 & 10: Changed from RFC2560 OCSP to RFC5019 OCSP Section 6.1.5: Removed all Dec 31, 2011 deadlines for 2048 RSA asymmetric keys & 128 AES symmetric keys. Section 9.8.1: Addition to Limitation of Liability Throughout doc – changed ownership and branding from VeriSign to Symantec.
1.23	13 December 2010	Addition of deprecated SHA-1 OIDs which are in effect from 1/1/2011 until 1/1/2014. Sections: 1.2, 1.4.1, 6.1.5, 6.5.1, 6.6.2, 6.7, A, A.1, A.3, A.4, A.5, A.6, A.7, A.10.
1.23	27 September 2010	This CPS (RFC3647 format) replaces Version 1.10 dated November 6, 2008 and incorporates changes to comply with the U.S. Federal Bridge PKI Certificate Policy version 2.16, dated May 14, 2010.
1.22	28 May 2010	Updated for compliance with PIV-I assurance levels as specified by CP changes (# 2010-03, May 11, 2010), sections: 1.0, 1.2, 1.3.1.5, 1.3.3, 1.3.5, 1.4.1, 3.1.1, 3.1.2, 3.1.4, 3.2.2, 3.2.3, 3.2.3.1, 4.2.1, 4.9.1, 4.9.2, 4.9.10, 4.10, 5.1.2.1, 5.2.2, 5.2.4, 6.1.1.2, 6.1.2, 6.1.5, 6.1.7, 6.2.1, 6.2.4.2, 6.2.4.5, 6.2.8, 6.3.2, 6.4.3, 7.1.3, 7.1.4, 7.1.10, 8.1, 8.4, 8.5, 9.6.1, 9.6.5.3, 10, 11,12, Appx A, Appx B, Appx C. Added Medium-CBP & MediumHardware-CBP policies, sections 1.2, 5.3.2.

1.21	10 May 2010	Updated location of Primary & DR Facility: Primary changed [Text Removed] (sections 1.1, 1.3.6.2. 5.7.1, 5.1.1). Section 5.1.1 – removed reference to Army Regs 380-5. Section 6.7 – clarified tools by systems & network; changed network scanning tools from [Text Removed] Section 6.5.2 – updated to [Text Removed]
1.21	30 April 2010	Converted from rfc2527 to rfc3647 format.
1.20	12 Nov, 2009	This CPS replaces Version 1.10 dated Nov 6, 2008 to incorporate all changes resulting from the policy mapping against the SAFE CP. This revision further incorporates changes to the VeriSign PKI infrastructure resulting from planned evolution and internal compliance monitoring.
1.10	06 November, 2008	Incorporates all changes resulting from the policy mapping against the Federal Bridge CP.

* * * End of Document * * *