# DigiCert
# Shared Service Provider

# Certification Practices Statement

**Version 2.2**
**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 Shared Service Provider (SSP) Certification Practices Statement**

Printed in the United States of America.
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 Certificate Practices Statement document and the PKI Services described within this document.

However a hybrid of references to "VeriSign," "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

Symantec, the Symantec logo, and the Checkmark Logo are the registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. The VeriSign logo, VeriSign Trust and other related marks are the trademarks or registered marks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed by Symantec Corporation. Other names may be trademarks of their respective owners.

Without limiting the rights reserved above, and except as licensed below, no part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without prior written permission of DigiCert, Inc.

Notwithstanding the above, permission is granted to reproduce and distribute this SSP Certificate Practice Statement on a nonexclusive, royalty-free basis, provided that (i) the foregoing copyright notice and the beginning paragraphs are prominently displayed at the beginning of each copy, and (ii) this document is accurately reproduced in full, complete with attribution of the document to DigiCert, Inc.

Requests for any other permission to reproduce this SSP Certificate Practice Statement (as well as requests for copies from DigiCert) must be addressed to:

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

## TABLE OF CONTENTS

# 1. INTRODUCTION

The US Government has identified the need for Shared Service Providers (SSP) to provide PKI services for Federal employees, contractors and other affiliated individuals requiring PKI credentials for access to Federal systems. DigiCert is an approved Shared Service Provider operating under a Memorandum of Agreement (MOA) signed by the Federal PKI Policy Authority (PA). The DigiCert SSP Certification Practices Statement (CPS) and associated Compliance Audit have been approved by the FPKIPA.

This SSP CPS in conjunction with the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework (Common Policy, or simply, "CP") defines the practices that DigiCert will employ in issuing and managing certificates and in maintaining a certificate-based public key infrastructure (PKI) for the SSP. The SSP CPS is posted in the DigiCert repository at digicert.com/legal-repository.

## *1.1 Overview*

DigiCert has acquired the Symantec SSP Certification Authority (CA) that is subordinate to the US Government Federal Common Policy Root CA. The Federal Common Policy Root CA serves as the "trust anchor" for all certificates issued by the SSP CA.

The SSP PKI service offering provides complete certificate life-cycle support and certificate repository services for approved entities. The SSP PKI operates multiple assurance levels defined by the Common Certificate Policy (CP) as listed in section 1.1.2.

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

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 entities at Federal agencies that purchase the SSP PKI services. RAs may rely on a delegated in-person identity proofing process performed by authorized Trusted Agents.

End-entities supported by the SSP PKI are Federal employees, contractors and affiliates needing access to Federal facilities and IT systems. The SSP CA will issue X.509 Version 3 certificates compliant with the certificate profiles listed in the CP and Appendix A of this CPS. The certificates can be used by Subscribers and Relying Parties for both physical and logical access including use in a variety of secure commercial and government-developed applications such as 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 DigiCert will employ when issuing digital certificates as an approved SSP under the US Government Federal Common Certificate Policy. 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 Federal employees, individuals, contractors, and device sponsors to use in applications requiring communication between networked computer-based systems used for transacting business electronically with Federal agencies. These applications include, but are not limited to: electronic mail; transmission of unclassified information; signature of electronic forms; contract formation signatures; and authentication of humans and devices to infrastructure components such as web servers, firewall and directories as described. This CPS describes the rights and obligations of persons and entities authorized under this CPS and the Common 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.

### 1.1.2 Relationship between this CPS and the RPS

This CPS states what assurance can be placed in a certificate issued by DigiCert and each of its RAs. This certification practice statement (CPS) states how DigiCert establishes that assurance. Each RA that issues certificates under this CPS shall have a corresponding RPS (Registration Practices Statement) that includes its own Key Recovery Practices Statement (KRPS).

### 1.1.3 Scope

This CPS applies to certificates issued by DigiCert as the CA, to RAs, devices, and Federal employees, contractors and other affiliated personnel. This CPS does not apply to certificates issued to groups of people.

### 1.1.4 Interoperation with CAs Issuing under Different Policies

Interoperation with the Common CP and FPKI is achieved by DigiCert through policy mappings and cross-certifications through the Federal Bridge Certification Authority.

## *1.2 Document Name and Identification*

This CPS describes the practices for SSP PKI services delivered in accordance with the CP. The CP includes distinct certificate policies: a policy for users with software cryptographic modules, a policy for users with hardware cryptographic modules, a policy for devices with software cryptographic modules, a policy for devices with hardware cryptographic modules, a high assurance user policy, a user authentication policy, a card authentication policy, a policy for content signing, and a policy for derived PIV auth and derived PIV auth hardware. Certificates issued by the SSP PKI service will assert at least one of the following Policy Object Identifiers defined in the CP:

*id-fpki-common-policy* ::= {2 16 840 1 101 3 2 1 3 6}
For users with software cryptographic modules. Uses: digital signature, client authentication, encryption. Mutually exclusive of *id-fpki-common-hardware* and *id-fpki-common-High*.

*id-fpki-common-High* ::= {2 16 840 1 101 3 2 1 3 16}
For users with high identity assurance hardware cryptographic modules. Uses: digital signature, client authentication, encryption. Mutually exclusive of *id-fpki-common-hardware* and *id-fpki-common-policy*.

*id-fpki-common-hardware* ::= {2 16 840 1 101 3 2 1 3 7}
For users with hardware cryptographic modules (e.g., smart card). Uses: digital signature, client authentication, encryption. Mutually exclusive of *id-fpki-common-High* and id-*fpki-common-policy*.

*id-fpki-common-devices* ::= {2 16 840 1 101 3 2 1 3 8}
For devices (non-person entity) only; requires a human sponsor. Uses: device authentication, encryption.

*id-fpki-common-devicesHardware* ::= {2 16 840 1 101 3 2 1 3 36}
For devices (non-person entity) only; requires a human sponsor. Uses: device authentication, encryption.

*id-fpki-common-authentication* ::= {2 16 840 1 101 3 2 1 3 13}

For user authentication only, no digital signature capability (e.g., PIV authentication with *pivFASC-N* attribute specific to FIPS 201-2-2 Personal Identity Verification Card). Uses: client authentication for physical and logical access after private key activation; requires OCSP services.

*id-fpki-common-cardAuth* ::= {2 16 840 1 101 3 2 1 3 17}

For user authentication only, no digital signature capability (e.g., PIV authentication with *pivFASC-N* attribute specific to FIPS 201-2 Personal Identity Verification Card). Uses: client authentication for physical access – private key can be used without Subscriber activation; requires OCSP services

*id-fpki-common-piv-contentSigning* ::= {2 16 840 1 101 3 2 1 3 39}

Certificates are issued on PIV cards as defined in section 6.2.1. Uses: exclusively used by the Card Management System (CMS) to sign the PIV card security objects. Requirements associated with PIV Content Signing are identical to Medium Hardware except where specifically noted otherwise.

*id-fpki-common-derived-pivAuth* ::= {2 16 840 1 101 3 2 1 3 40}

Certificates issued to users supporting authentication, but not digital signature, where the corresponding private key is not stored on a PIV card. Requires OCSP services.

*id-fpki-common-derived-pivAuth-hardware* ::= {2 16 840 1 101 3 2 1 3 41}

Certificates issued to users supporting authentication, but not digital signature, where the corresponding private key is stored on a FIPS 140 validated cryptographic hardware device that is not the PIV card. Requires OCSP services.

Certificates issued from the 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-fpki-common-policy, id-fpki-common-hardware,* or *id-fpki-common-High*. Certificates issued to users supporting authentication but not digital signature may contain *id-fpki-common-authentication, id-fpki-common-derived-pivAuth* or *id-fpki-common-derived-pivAuth-hardware*. Certificates issued to users supporting token authentication where the private key can be used without user authentication may contain *id-fpki-common-cardAuth*. The devices policies apply to hardware devices and software applications (non-person entities) operated by or on behalf of federal agencies. Subscriber certificates issued to devices under this policy that use FIPS 140 Level 2 or higher cryptographic modules shall include either *id-fpki-common-devices, id-fpki-common-devicesHardware* or both. Subscriber certificates issued to devices under this policy using software cryptographic modules shall include *id-fpki-common-devices*. These 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 Policy Authority (FPKIPA) is a group of U.S. Federal Government Agencies (including cabinet-level Departments) established by the Federal CIO Council. The FPKIPA is responsible for maintaining the CP, approving the CPS and Compliance Audit for each CA that issues certificates under the CP.

#### 1.3.1.2 DigiCert Policy Authority

The DigiCert Policy Authority (DCPA) is a management body responsible for maintaining this 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 FPKI Common Policy regardless of by whom the PKI component is managed and operated. The DCPA is responsible for notifying customers, including Agencies that operate their own Policy Management Authorities.

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

An Agency PMA is responsible for ensuring that all agency-operated PKI components (e.g., CMSs and RAs) are operated in compliance with this CPS and the FPKI Common Policy and shall serve as the liaison for that agency to the DCPA. The DCPA is responsible for notifying its Agency PMAs and the FPKIPA of any change to the infrastructure that has the potential to affect the FPKI operational environment at least two weeks prior to implementation; all new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the change are provided to DigiCert and the FPKIPA within 24 hours following implementation.

#### 1.3.1.3 Certification Authority (CA)

The SSP CA is an entity authorized by the FPKIPA to create, sign and issue digital certificates that conform to the requirements of the CP and this CPS. The SSP CA is a Certification Authority subordinate to the US Government Federal Common Policy Root CA. This Root CA serves as the “trust anchor” for certificates issued by the SSP CA. The SSP CA issues all end-entity certificates within the SSP domain.

The 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 SSP certificates are performed in accordance with the requirements, representations, and warranties of this CPS.

#### 1.3.1.4 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. A Certificate Status Authority (CSA) shall assert all the policy OIDs for which it is authoritative.

### 1.3.2 Registration Authorities

#### 1.3.2.1 Registration Authority (RA)

Designated Federal Agency personnel will perform the RA functions for the SSP. The RA may rely on an in-person identity validation process performed by a Trusted Agent. DigiCert will establish a contractual relationship with a Federal Agency prior to the authorization of a Registration Authority or Trusted Agent to perform identity verification of employees/affiliates of the Agency. The Agency RA will be bound by contract to comply with the requirements of the CP and this CPS. DigiCert RAs enroll Agency RAs to perform RA functions on behalf of employees and affiliates of their Agency. For those agencies issuing Derived PIV credentials, DigiCert will confirm that the Agency currently has a NIST 800-79r2 ATO in place prior to allowing the RA function for that certificate type.

The SSP RA is a DigiCert trusted person operating a dedicated RA workstation within DigiCert’s secure facilities on DigiCert’s internal corporate network. The Agency RA is an external authority using trusted persons, referred to as RA personnel or Trusted Agents, operating a dedicated RA workstation on the Agency internal network. RA personnel will be issued public key certificates to enable secure authenticated access to the SSP CA. The associated RA private key is stored on a FIPS 140 Level 2 hardware token.

#### 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 its affiliates 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.

### 1.3.3 Subscribers

An SSP Subscriber is an entity whose name appears as the subject in an SSP certificate, and who asserts that it uses its key and certificate in accordance with SSP policy. Subscribers are limited to Federal employees, contractors and affiliated personnel. Subscribers may also be devices, such as workstations, firewalls, routers, and trusted servers (e.g., database, FTP, and WWW) under the control of humans, who accept the certificate and are responsible for the correct protection and use of the associated private key.

[There is a subset of human subscribers who will be issued role-based certificates. These certificates will identify a specific role on behalf of which the subscriber is authorized to act rather than the subscriber's name and are issued in the interest of supporting accepted business practices. The role-based certificate can be used in situations where non-repudiation is desired. Normally, it will be issued in addition to an individual subscriber certificate. A specific role may be identified in certificates issued to multiple subscribers, however, the key pair will be unique to each individual role-based certificate (i.e. there may be four individuals carrying a certificate issued in the role of "Secretary of Commerce" however, each of the four individual certificates will carry unique keys and certificate identifiers). Roles for which role-based certificates may be issued are limited to those that are held by a unique individual within an organization (e.g. Chief Information Officer, GSA is a unique individual whereas Program Analyst, GSA is not).]

Although the 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.

### 1.3.4 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 federal employee, contractor, affiliated personnel, or device.

### 1.3.5 Other Participants

#### 1.3.5.1 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. The SSP CPS is based on its existing commercial practices and controls. As such, the yearly independent SOC 2 and WebTrust for CA audits provide the assurance of DigiCert's compliance with the SSP CPS.

#### 1.3.5.2 Repository

DigiCert will operate the SSP Repository from its secure data facility located in [Text Removed]. This repository contains SSP Subscriber certificates, Certificate Revocation Lists (CRLs) and the SSP CA certificate and associated CRL. Updates to information contained in the SSP 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 certificate and CRL entries in the repository via an ldap query or using http URI queries.

## *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 Federal systems that have not been designated national security systems. While a validated public key is not generally sufficient to grant access, the key may be sufficient when supplemented by appropriate authorization mechanisms. Credentials issued under this 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.

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

Credentials issued under the *id-fpki-common-piv-contentSigning policy* are intended to meet the requirements in FIPS 201-2 and SP 800-157 as the digital signatory of the PIV Card Holder Unique IDentifier (CHUID) and associated PIV data objects.

In addition, this CPS may support signature and confidentiality requirements for Federal government processes.

### 1.4.2 Prohibited Certificate Uses

Certificates issued under this CPS shall not be used for access to Federal systems that have been designated national security systems. Certificates issued under this CPS shall not be used to support applications involving classified information pursuant to federal statutes and regulations.

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

## *1.5 Policy Administration*

### 1.5.1 Organization Administering the Document

The organization responsible for administering this CPS is the DigiCert Policy Authority. Questions or correspondence related to this CPS should be addressed as follows:

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

### 1.5.3 Person Determining CPS Suitability for the Policy

The Federal Policy Authority (FPKIPA) determines the suitability of the SSP CPS and its compliance with the Federal Common Policy CP after review, approval, and submission by the DigiCert Policy Authority (DCPA).

### 1.5.4 CPS Approval Procedures

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

## *1.6 Definitions and Acronyms*

See Appendix B and D for definitions and acronyms.

# 2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

## *2.1 Repositories*

The SSP Repository is accessible through Uniform Resource Identifier (URI) references asserted in valid certificates. The Repository is implemented in compliance with the standards contained in the Shared Service Provider Repository Service Requirements (SSP-REP). End users may search for SSP certificates as specified in section 1.3.5.2.

### 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 (e.g. Federal agencies).

## *2.2 Publication of Certification Information*

### 2.2.1 Publication of Certificates and Certificate Status

The SSP will operate an online Repository available to Subscribers and Relying Parties. The SSP Repository shall maintain an availability of at least 99% per year and limit scheduled down-time to 0.5% per year for all components within its control. This Repository will contain or provide access to the following minimum information:

1. All CA certificates issued by or to the SSP CA;
2. Certificate status information, including revocation;
3. The most recently issued CRL;
4. The SSP certificate(s) needed to validate the signature on SSP Subscriber certificates; and
5. Any other relevant information the SSP considers relevant regarding the use of SSP certificates by its Subscribers or Relying Parties.

DigiCert and/or RAs will operate an online Repository available through secured methods for the following:
1. All valid and un-expired SSP Certificates.

The CSA shall maintain an availability of at least 99% per year and limit scheduled down-time to 0.5% per year for all components within its control.

### 2.2.2 Publication of CA Information

The Common Policy CP is made publicly available by the FPKIPA at *https://www.idmanagement.gov/fpki#certificate-policies*. The SSP document repository at *https://digicert.com/legal-repository* provides access to an abridged version of this CPS including at least the following topics covered under the CP:

- Section 1.4, SSP Contact Information;
- Section 3.1, Initial Registration;
- Section 4.9, Certificate Suspension and Revocation;
- Section 9, Other 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 Common Policy root or SSP certificate).

The SSP CPS is considered DigiCert Proprietary information.

DigiCert also publishes its annual PKI Compliance Audit Letter in the same legal repository as its CPS.

### 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 to the SSP. A redacted version of this CPS will be publicly available here: digicert.com/legal-repository as soon as reasonably possible following approval by the FPKIPA.

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

Upon revoking a certificate, the SSP 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/TLS and shall be limited to authorized SSP personnel.

# 3. IDENTIFICATION AND AUTHENTICATION

## *3.1 Naming*

### 3.1.1 Types of Names

For certificates issued by the SSP for *id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-High, id-fpki-common-authentication, id-fpki-common-devices, id-fpki-common-devicesHardware*, *id-fpki-common-derived-pivAuth-hardware,* and *id-fpki-common-derived-pivAuth* the CA shall use the X.500 DN name format for subject and issuer name fields. These distinguished names may be in either of two forms: an X.501 distinguished name specifying a geo-political name; or an Internet domain component name.
The Common PIV Content Signing certificate's subject DN shall indicate the organization administering the PIV card issuance system or device according to types of names for devices.

### 3.1.1.1 Geo-Political Name DN

CA and CSA distinguished names shall be a geo-political name composed of any combination of the following attributes: country; organization[1]; organizational unit; and common name.

Certificates issued under *id-fpki-common-authentication* shall include X.500 distinguished names and shall follow the rules specified for *id-fpki-common-hardware*. Certificates issued under *id-fpki-common-authentication* shall include a subject alternative name. The subject alternative name extension shall include a UUID and the pivFASC-N name type [FIPS 201-2]. The value for the pivFASC-N name shall be the FASC-N [PACS] of the subject's PIV card.

Certificates issued under *id-fpki-common-cardAuth* shall include a subject alternative name extension that includes the pivFASC-N name type. The value for this name shall be the FASC-N of the subject's PIV card. For certificates issued under *id-fpki-common-cardAuth* the subject alternative name extension shall also include a UUID [RFC 4122]. Certificates issued under *id-fpki-common-cardAuth* shall not include any other name in the subject alternative name extension but may include a non-NULL name in the subject field.

Certificates issued under *id-fpki-common-derived-pivAuth-hardware* and *id-fpki-common-derived-pivAuth* shall include a non-empty subject DN and shall also include a subject alternative name extension that includes a UUID, which shall be encoded as a URI. A unique UUID shall be created for each certificate issued under one of these policies.

The subject distinguished name of the *id-fpki-common-cardAuth* certificate shall take one of the following forms:

* C=US, o=U.S. Government, [ou=department], [ou=agency], serialNumber=FASC-N
* C=US, o=U.S. Government, [ou=department], [ou=agency], serialNumber=UUID (see Practice Note)

The FASC-N is encoded as a 25-byte binary value in the subject alternative name extension for certificates issued under *id-fpki-common-authentication* and *id-fpki-common-cardAuth*.

The FASC-N is encoded as a printable string decimal in a serialNumber attribute of certificates issued under *id-fpki-common-cardAuth*. Based on the detailed description provided in PACS Implementation Guidance Version 3.2, the five-tuples (4 bits plus 1 parity) are converted to decimal ignoring the parity bit. The start sentinel character in the FASC-N is ignored but the end sentinel and field separator characters are represented by space-

[1] While the SSP PKI is owned by DigiCert, Inc., legacy certificates may have been issued in the name of former owners, such as Verisign or Symantec. Any legacy certificate that indicates the Organization (O) as "VeriSign, Inc." of Symantec shall mean "DigiCert, Inc".

dash-space. When the serialNumber is printed each of the data elements in the FASC-N (e.g. Agency Code, System Code etc.) is readily identifiable.

The value of the subject alternative name of the *id-fpki-common-cardAuth* certificate shall take one of the following two forms:

- subjectAltname=FASC-N
- subjectAltName=UUID (see Practice Note)

> Practice Note: *When the UUID is included within the serial number attribute of the DN in a PIV 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 Authentication or PIV 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".*

Devices that are the subject of certificates issued under *id-fpki-common-devices* and *id-fpki-common-devicesHardware* may be assigned either a geo-political name or an Internet domain component name (see 3.1.1.2). For a geo-political name device names may take the following form:

- C=US, o=U.S. Government, [ou=department], [ou=agency], cn=device name

where [device name] is a descriptive name for the device.

All X.501 distinguished names assigned to federal employees shall be in the following directory information tree:

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

The organizational units department and agency appear when applicable and are used to specify the federal entity that employs the Subscriber. At least one organizational unit must appear in the DN. The distinguished name of the federal employee Subscriber will take one of the four following forms:

- C=US, o=U.S. Government, [ou=department], [ou=agency], cn=nickname lastname
- C=US, o=U.S. Government, [ou=department], [ou=agency], cn=firstname initial. lastname
- C=US, o=U.S. Government, [ou=department], [ou=agency], cn=firstname middlename lastname
- C=US, o=U.S. Government, [ou=department], [ou=agency], 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 makes the name unique. When a qualifier attribute is included, it may appear as part of a multi-valued relative distinguished name (RDN) with the common name or as a distinct RDN that follows the RDN containing the common name attribute. The last form shall be used only if the other three name forms have already been assigned to Subscribers.

X.501 distinguished names assigned to federal contractors and other affiliated persons shall be within the same directory information tree. The distinguished name of the federal contractor Subscribers and affiliate Subscribers will take one of the four following forms:

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

* C=US, o=U.S. Government, [ou=department], [ou=agency], cn=firstname middlename lastname (affiliate)
* C=US, o=U.S. Government, [ou=department], [ou=agency], cn=firstname middlename lastname (affiliate), dnQualifier=integer

Signature certificates issued under *id-fpki-common-hardware* or *id-fpki-common-High* may be issued with a common name that specifies an organizational role as follows:

* C=US, o=U.S. Government, [ou=department], [ou=agency], cn=role [, *department/agency*]

The combination of organizational role and agency must unambiguously identify a single person. A widely held role such as *Computer Scientist* or *Procurement Specialist* cannot be used since it does not identify a particular person. Where the role alone is ambiguous the [*department/agency*] suffix shall be present in the common name to uniquely specify a role held by a single person (eg, *Chief Information Officer*, *AgencyX*). Where the [*department/agency*] is implicit in the name of the role (e.g., Secretary of Commerce), it can be omitted. The organizational information in the common name shall match that in the organizational unit attributes. Common name fields shall be populated as specified above.

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

### 3.1.1.2 Internet Domain Component Name

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

* dc=gov, dc=org0, [dc=org1],…[ dc=orgN]
* dc=mil, dc=org0, [dc=org1],…[ dc=orgN]

Devices that are the subject of certificates issued under *id-fpki-common-devices* and *id-fpki-common-devicesHardware* may be assigned either a geo-political name (see 3.1.1.1) or an Internet domain component name. For an Internet domain component name, device names may take the following forms:

* dc=gov, dc=org0, [dc=org1], …[dc=orgN], [cn=device name]
* dc=mil, dc=org0, [dc=org1], …[dc=orgN], [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.

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

The distinguished name of the federal employee Subscriber may take one of the four following forms when their agency's Internet domain name ends in .gov:

* dc=gov, dc=org0, [dc=org1], …[dc=orgN], cn=nickname lastname
* dc=gov, dc=org0, [dc=org1],…[dc=orgN], cn=firstname initial. lastname
* dc=gov, dc=org0, [dc=org1],…[dc=orgN], cn=firstname middlename lastname
* dc=gov, dc=org0, [dc=org1],…[dc=orgN], cn=firstname middlename lastname, dnQualifier=integer

The distinguished name of the federal contractors and affiliated Subscribers may take one of the four following forms when the agency's Internet domain name ends in .gov:

* dc=gov, dc=org0, [dc=org1],…[dc=orgN], cn=nickname lastname (affiliate)

* dc=gov, dc=org0, [dc=org1],…[dc=orgN], cn=firstname initial. lastname (affiliate)
* dc=gov, dc=org0, [dc=org1],…[dc=orgN], cn=firstname middlename lastname (affiliate)
* dc=gov, dc=org0, [dc=org1],…[dc=orgN], cn=firstname middlename lastname (affiliate), dnQualifier=integer

The distinguished name of the federal employee Subscriber may take one of the four following forms when their agency's Internet domain name ends in .mil:

* dc=mil, dc=org0, [dc=org1], …[dc=orgN], cn=nickname lastname
* dc=mil, dc=org0, [dc=org1],…[dc=orgN], cn=firstname initial. lastname
* dc=mil, dc=org0, [dc=org1],…[dc=orgN], cn=firstname middlename lastname
* dc=mil, dc=org0, [dc=org1],…[dc=orgN], cn=firstname middlename lastname, dnQualifier=integer

The distinguished name of the federal contractors and affiliated Subscribers may take one of the four following forms when the agency's Internet domain name ends in .mil:

* dc=mil, dc=org0, [dc=org1],…[dc=orgN], cn=nickname lastname (affiliate)
* dc=mil, dc=org0, [dc=org1],…[dc=orgN], cn=firstname initial. lastname (affiliate)
* dc=mil, dc=org0, [dc=org1],…[dc=orgN], cn=firstname middlename lastname (affiliate)
* dc=mil, dc=org0, [dc=org1],…[dc=orgN], cn=firstname middlename lastname (affiliate), dnQualifier=integer

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

### 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

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=AgencyX 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 names in certificates.

DNs in certificates may contain a pseudonym (such as role names specified in section 3.1.1.1) as long as name space uniqueness requirements are met.

### 3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting distinguished name forms are contained in the applicable certificate profiles (See Section 7.1.2. and Appendix A). Rules for interpreting the pivFASC-N name type are specified in [PACS].

### 3.1.5 Uniqueness of Names

DigiCert and its associated RAs will ensure the uniqueness of names for all certificates issued in their respective systems for the SSP. Information contained in certificate enrollment requests will be automatically checked against the SSP database to prevent duplication and to ensure the uniqueness of SSP certificate distinguished names and serial numbers.

DigiCert shall investigate and correct, if necessary, any name collisions brought to its attention. If appropriate, DigiCert shall coordinate with and defer to the FPKIPA naming authority.

Agency PMAs shall resolve name collisions within their own space and describe that process in their RPS.

### 3.1.6 Recognition, Authentication, and Role of Trademarks

The SSP shall not knowingly issue a certificate including a name that a court of competent jurisdiction has determined infringes the trademark of another.

## *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 SSP 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 Agency smart card issuance, certificate enrollment requests are sent from an Agency RA workstation to the SSP CA as signed and encrypted messages (PKCS #7-enveloped PKCS #10 requests) over an HTTPS link. For software credentials, certificate enrollment requests are sent over an SSL/TLS 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 shall include the name of the Agency, 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 Agency.

### 3.2.3 Authentication of Individual Identity

The SSP certificate shall be issued only to a single entity. Certificates shall not be issued that contain a public key whose associate private key is shared.

#### 3.2.3.1 Authentication of Human Subscribers

Procedures used by agencies to issue identification to their own personnel and affiliates may be more stringent than the following. When this is the case, the agency procedures for authentication of personnel shall apply in addition to the guidance in this section.

The RA shall ensure that the applicant's identity information is verified. 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 agency identity badging requirements are otherwise satisfied. Minimal procedures for RA authentication and notarized authentication of employees and affiliated personnel are detailed below.

Federal Agencies using a SSP PKI to comply with the requirements of HSPD-12 must utilize the enrollment process, including identity proofing and background investigation procedures, specified in NIST FIPS 201-2. At a minimum, authentication procedures for employees must include the following steps:

1) Verify that a request for certificate issuance to the applicant was submitted by agency management;
2) Applicant's employment shall be verified through use of official agency records.
3) Applicant's identity shall be established by in-person proofing before the Registration Authority or Trusted Agent, based on either of the following processes:
    a) Process #1:
        i) The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and
        ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g. a photograph on the credential itself or a securely linked photograph of applicant), and
        iii) The credential presented in step 3) a) i) above shall be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid). Typically this is accomplished by querying a database maintained by the organization that issued the credential, but other equivalent methods may be used.
    b) Process #2:
        i) The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and
        ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a photograph of applicant securely stored and linked to the credential), and
        iii) The applicant presents current corroborating information (e.g., current credit card bill or recent utility bill) to the RA. The RA verifies the identifying information (e.g., name and address) on the credential presented in step 3) b) i) above and verifies the credential for currency and legitimacy (e.g., the agency ID is verified as valid). [Practice Note: This may be accomplished by querying a database maintained by the organization that issued the financial instrument or through use of a commercial credit database. In some instances, commercial credit card databases will validate name and address of current cardholders online; this validation is acceptable if the card is presented to the RA. Other methods may be accepted.]
4) A biometric of the applicant (e.g., a photograph or fingerprint) shall be recorded and maintained by the RA or CA. (Handwritten signatures and other behavioral characteristics are not accepted as biometrics for the purposes of this policy.) This establishes an audit trail for dispute resolution.

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

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

2) Sponsoring Agency 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,

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

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

3) Applicant's identity shall be established by in-person proofing before the Registration Authority or Trusted Agent, based on either of the following processes:

   a) Process #1:

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

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

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

   b) Process #2:

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

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

      iii) The applicant presents current corroborating information (e.g., current credit card bill or recent utility bill) to the RA. The RA verifies the information (e.g., name and address) on the credential presented in step 3) b) i) above and verifies the credential for currency and legitimacy (e.g., the agency ID is verified as valid). Typically this is accomplished by querying a database maintained by the organization that issued the financial instrument or through use of a commercial credit database. In some instances, commercial credit card databases will validate name and address of current cardholders online; this validation is acceptable if the card is presented to the RA.

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

Additionally, the RA shall record the process that was followed for issuance of each certificate. The process documentation and authentication requirements 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);
- Unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- The biometric of the applicant;
- The date and time of the verification; and

- A declaration of identity signed by the applicant using a handwritten signature and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury).

FIPS 201-2 imposes a strict requirement of in-person registration for applicants for PIV cards. Applications enrolling for certificates where the corresponding private key is stored on a PIV Card (e.g. *id-fpki-common-authentication*) or under *id-fpki-common-High* must appear in person before the RA. Through the use of Registration Authority Agreements and Registration Practice Statements, DigiCert requires RAs to ensure that RA personnel are trained and that RA interfaces with the CA are securely managed. Except for applicants enrolling under *id-fpki-common-High*, where it is not possible for applicants to appear in person before the RA, 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 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.

### 3.2.3.2 Authentication of Component Identities

The SSP may provide device component certificates (e.g., for card management systems, routers, firewalls, servers, etc.) and software applications. 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 SSP, or approved Trusted Agent, correct information regarding:

- Device name (equipment identification (e.g., 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.

The SSP requires in-person registration of the PKI Sponsor, with the identity of the PKI Sponsor confirmed in accordance with the requirements of Section 3.2.3.1. 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.

### 3.2.3.3 Authentication for Derived PIV Credentials

For certificates issued under *id-fpki-common-derived-pivAuth-hardware* and *id-fpki-common-derived-pivAuth*, identity is verified in accordance with the requirements specified for issuing derived credentials in [SP 800-157]. The RA:

1) Verifies that the request for certificate issuance to the applicant was submitted by an authorized agency employee.

2) Uses the PKI-AUTH authentication mechanism from Section 6 of FIPS 201-2 to verify that the PIV Authentication certificate on the applicant's PIV Card is valid and that the applicant is in possession of the corresponding private key.
3) Maintains a copy of the applicant's PIV Authentication certificate.

Seven days after issuing the Derived credential, the RA issuer should recheck the revocation status of the PIV Authentication certificate. This step can detect use of a compromised PIV Card to obtain a derived credential. If an RA chooses to complete this recheck, they will describe this process in their respective RPS based on the instructions and manual for their CMS and this CPS.

For certificates issued under *id-fpki-common-derived-pivAuth-hardware*, the applicant appears at the RA in person to present the PIV Card and perform the PKI-AUTH authentication mechanism. The RA performs a one-to-one comparison of the applicant against biometric data stored on the PIV Card, in accordance with [SP 800-76], and records and maintains the biometric sample used to validate the applicant. In cases where a 1:1 biometric match against the biometrics available on the PIV Card or in the chain-of-trust, as defined in [FIPS201] is not possible:

1) The applicant presents a government-issued form of identification (e.g., a passport or driver's license) in addition to the PIV Card, and
2) The RA examines the presented credentials for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of the applicant), and
3) The process documentation for the issuance of the certificate includes the identity of the person performing the verification of the second (non-PIV) form of 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), a unique identifying number from the second form of identification or a facsimile of the ID, a biometric of the applicant, and the date and time of the verification.

### 3.2.4 Non-Verified Subscriber Information

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

### 3.2.5 Validation of Authority

CA certificates shall be issued only after the SSP verifies the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the CA.

Before issuing signature certificates that assert organizational authority, the SSP shall validate the individual's authority to act in the name of the organization. For certificates that identify Subscribers by their organizational roles, the CA shall validate that the individual either holds that role or has been delegated the authority to sign on behalf of the role.

DigiCert identifies the individuals who may request certificates that assert organizational authority. If an organization specifies, in writing, the individuals who may request a certificate, then the CA shall not accept any certificate requests that are outside this specification. The CA shall provide an Applicant with a list of the organization's authorized certificate requesters upon the Applicant's verified written request.

### 3.2.6 Criteria for Interoperation

All certificates and CRLs associated with the SSP PKI service will meet the certificate and CRL formats specified in the X.509 Certificate and Certificate Revocation List Extensions Profile for the Shared Service Providers Program [SSP-PROF].

## *3.3 Identification and Authentication for Re-Key Requests*

### 3.3.1 Identification and Authentication for Routine Re-Key

The SSP supports re-key for Subscribers and CAs.

Subscriber Re-Key:
For policies other than *id-fpki-common-High*, which requires re-authentication every three years, if it has been less than 9 years since a Subscriber was identified as required in Section 3.2, 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 currently valid Signature and Encryption certificates. The SSP provides separate SSL/TLS-protected web pages for re-keying of Signature and Encryption certificates (or other certificates as relevant to the Certificate profile and allowed by the Common CP).

The SSP may issue Subscriber certificates with one, two, or three-year lifetimes. A Subscriber certificate re-key shall follow the same procedures as initial certificate issuance as specified in section 3.2 once every nine years, and once every three years for *id-fpki-common-High*.

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

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

In addition, for re-key of subscriber certificates issued under *id-fpki-common-derived-pivAuth-hardware*, identity is established via mutual authentication between the issuer and the cryptographic module containing the current key, if the new key will be stored in the same cryptographic module as the current key. Identity is established through the initial registration process if the new key will be stored in a different cryptographic module than the current key.

CA Re-Key:
CA Certificate Re-key and Re-key of certificates issued under *id-fpki-common-High* are supported for circumstances where DigiCert cannot follow normal procedure of initial issuance. If a CA Certificate must be rekeyed to meet requirements, DigiCert will follow the same validation procedures as initial certificate issuance of a CA to ensure information to be included in the Re-key is still accurate.

### 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/TLS-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. Alternatively, the Subscriber may 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.

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

An Agency RA may revoke a Subscriber’s certificate only for Subscribers affiliated with his or her Agency.

The RA may revoke a Subscriber’s certificate for cause.

# 4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

## *4.1 Certificate Application*

### 4.1.1 Who Can Submit a Certificate Application

***4.1.1.1 CA Certificates***
An application for a CA certificate is submitted by an authorized representative of DigiCert in accordance with section 3.2.5.

***4.1.1.2 User Certificates***
An application for a user (subscriber) certificate is submitted by either the applicant or a trusted agent.

***4.1.1.3 Device Certificates***
An application for a device certificate is submitted by the human sponsor of the device.

***4.1.1.4 Code Signing Certificates***
Not offered by DigiCert or by any of its RAs.

### 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 agency) to obtain a certificate. (per Section 3.2)
- Establish and record identity of the applicant (per Section 3.2)
- 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 any role or authorization information requested for inclusion in the certificate.

All communications among SSP PKI Authorities in processing certification applications are electronic and are protected by SSL/TLS. Details of the certificate application process for each type of certificate issued by the SSP CA are as follows:

## *4.2 Certificate Application Processing*

### 4.2.1 Performing Identification and Authentication Functions

<u>Hardware Credential</u>

1) Applicants enrolling for a SSP certificate on a PIV smart card must appear before a designated Agency 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 Agency official.
2) The Applicant must appear before an Agency RA and present the enrollment authorization form. Applicants for Derived PIV will present their PIV credentials to the Agency RA. The Agency RA initiates the process for personalization of the secure hardware module, and after printing of the smart card or presenting the secure hardware module for derived PIV, the Agency RA enrolls on behalf of the Subscriber for the mandatory PIV Certificate. Alternatively, after issuance of the smart card the Subscriber receives a Passcode from the Agency RA which may be later presented to an Agency-hosted, SSL/TLS-protected web page for enrollment for the optional certificates types including Derived PIV.

3) Public/private key pairs for authentication certificates (based on the attributes specified in the relevant Certificate profile) are generated on the smart card/secure hardware module and a certificate signing request is generated which includes the public key, the Subscriber name, e-mail address and organizational data necessary to populate a certificate which meets one of the certificate profiles specified in Section 7. 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, posts the certificate to the SSP Repository and returns the certificate to the smart card issuance system where it is then downloaded onto the Subscriber's smart card.

4) An Agency-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/secure hardware module.

5) In order to perform key pair generation for a Derived PIV certificate, the applicant will take their existing PIV card to be read and validated. The RA or CMS will perform a user authentication with the PIV card to verify the owner's presence. After the PIV card and owner are verified, the applicant will present and identify the device that is to hold the Derived PIV private key and the CMS will establish a secure connection with the device based on the software and hardware process established in the CMS manufacturer's instructions. After authentication is completed, issuance is initiated and completed.

Software Credential

1) Applicants must appear before a designated Agency 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 Agency-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, the necessary key generation processes are initiated. First, the public-private key pair for the Authentication certificates (including digital signature, and/or other attributes as specified in the relevant Certificate profile) are generated locally on the Subscriber's workstation, and then the key pair for the Encryption certificate is generated in an Agency-hosted Key Manager (if applicable to the Certificate type). The associated 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 the certificates associated with the requested certificate type, posts them to the repository, and returns the certificates to the web browser for installation in the browser cache.

3) In order to perform key pair generation for a Derived PIV certificate, the Applicant will authenticate their existing PIV credentials through an encrypted SSL/TLS session or in-person with the RA. After the Applicant for the Derived PIV Certificate is verified with the existing PIV credentials (software or hardware), they will authenticate to the RA in-person or through an encrypted SSL/TLS session with their PIV Certificate. The derived PIV 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. Once verified, the Derived PIV certificates are generated on the Subscriber's browser.

### 4.2.2 Approval or Rejection of Certificate Applications

The SSP PKI will reject an application for a certificate if authentication of all required information in accordance with Section 3.2 cannot be completed.

For Device certificates, DigiCert will reject a certificate request if the requested Public Key has a known weak

Private Key

### 4.2.3 Time to Process Certificate Applications

Certificate applications must be processed and a certificate issued within 30 days of identity verification.

## *4.3 Certificate Issuance*

### 4.3.1 CA Actions during Certificate Issuance

Upon receiving the request, the SSP CA or RA shall:

- Verify the identity of the requester as described in section 4.2.1 and relevant requirements of section 3.2 of this CPS and the RPS for the Certificate requested;
- Verify the authority of the requester and the integrity of the information in the certificate request as specified in section 3.2 of this CPS and the RPS;
- Build and sign a certificate if all certificate requirements have been met (in the case of an RA, have the CA sign the certificate in accordance with section 7 and the guidance in the RPS to produce a test certificate that verifies to DigiCert that the attributes are in accordance with section 7 of this CP and the RPS); and
- Make the certificate available to the subscriber after confirming that the subscriber has formally acknowledged their obligations as described in section 9.6.3.

The certificate request to the CA may already contain certificate profile by input to the CMS application. This certificate will not be signed until all verifications and modifications, if any, have been completed to DigiCert's satisfaction in alignment with this CPS and the RPS as described above.

All authorization and other attribute information received from a prospective subscriber will be verified before inclusion in a certificate.

The SSP CA issues certificates 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 meeting FIPS 140 level 2 or higher. Subscribers with PIV cards can apply and use these credentials to authenticate to an RA for Derived PIV hardware certificates. After authenticating with the PIV card and presenting the FIPS-140 Level 2 or higher hardware intended for the Derived PIV, the certificate is issued.

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. Subscribers with PIV cards can apply and use these credentials to authenticate to an RA for Derived PIV auth certificates through a browser. After authenticating with the PIV credentials, the certificate is issued through a secure portal solution meeting FIPS-140 Level 1 or higher.

### 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 9.6.4. The Subscriber is also notified that the private key associated with their Encryption certificate is escrowed. After the Agency RA downloads the Subscriber's certificates to the smart card or Derived PIV hardware, the Subscriber takes possession of the smart card or hardware and signs a receipt.

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 and CA certificates as specified in section 2.2.1.

### 4.4.3 Notification of Certificate Issuance by the CA to Other Entities

DigiCert will notify the FPKIPA at least two weeks prior to the issuance of a new CA certificate. The notification will assert that the new CA 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 a private key for signature or authentication 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.

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. 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

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

## *4.7 Certificate Re-Key*

The SSP supports re-key for Subscriber certificates. DigiCert will perform Re-Key for CA certificates only when it is not possible to issue a new CA Certificate.

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 or modified.

When the SSP CA updates its private signature key and thus generates a new public key it will publish notification according to section 2.2.

### 4.7.1 Circumstances for Certificate Re-Key

The SSP certificate shall be 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

Subscribers with a currently valid certificate may request certification of a new public key. The SSP CA and RAs may request certification of a new public key on behalf of a subscriber. For device certificates, the human sponsor of the device may request certification of a new public key. The DCPA may request the Re-Key of a CA Certificate.

### 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 re-keyed 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

The SSP will inform any parties of subordinate CA certificates if they are maintained by an agency or authorized external party as specified in section 4.3.2 and 2.2.1.

### 4.8.4 Conduct Constituting Acceptance of Modified Certificate

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

### 4.8.5 Publication of the Modified Certificate by the CA

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

### 4.8.6. Notification of Certificate Issuance by the CA to Other Entities

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

Any subordinate CAs will be communicated as stated in section 4.4.3.

## *4.9 Certificate Revocation and Suspension*

The SSP CA shall issue CRLs covering all unexpired certificates issued under this policy except for OCSP responder certificates that include the *id-pkix-ocsp-nocheck* extension.

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:

- Identifying information including the organizational affiliation in the Subscriber’s certificate changes, the 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 of a Certificate or CA is suspected of compromise;
- The Subscriber or other authorized party asks for his/her certificate to be revoked; or
- A CA does not adhere to the requirements of this CPS or the FPKI CP.

The above circumstances also apply when Subscribers use hardware tokens. 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.

### 4.9.2 Who Can Request Revocation

The Subscriber is authorized to request the revocation of his or her own certificate.  The human sponsor of a device can request the revocation of the device's certificate.  The SSP 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. A Trusted Agent can only request revocation of a certificate for a Subscriber that is affiliated with the Trusted Agent's organization. Written notice including a reason for the revocation is also provided to a Subscriber whose certificate has been revoked.

### 4.9.3 Procedure for Revocation Request

The revocation request must 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 agency name, the subject name and the email address on the certificate. This information alone or combined is used to uniquely identify the correct Subject DN of the certificate to be revoked.
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 Agency RA. The message must include a reason for the revocation. The Agency 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 SSP RA, the SSP 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 Agency 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 immediately revoked, expressing reason code "key compromise".

*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 Agency 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 Agency RA will validate the request 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 Agency RA, the SSP 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 Agency RA may request revocation of any SSP Subscriber certificate affiliated with their organization. Access to the SSP to request revocation is protected using SSL/TLS and requires presentation of a valid RA certificate. The SSP validates the RA certificate and checks that the RA affiliation is the same as the Agency affiliation in the certificate to be revoked. If these checks are successful, the SSP 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 PKI Sponsor:* A PKI Sponsor may request revocation of the non-human entity for which the Sponsor is identified as the representative. The Sponsor shall initiate the request for revocation to either a Trusted Agent or Agency RA, uniquely identifying itself as described above, and uniquely identifying the component by subject name (e.g., DNS of the host). The RA and TA shall verify that requestor is the authorized Sponsor for the named Subscriber entity. The request is processed by the RA or TA using the relevant process variation described above, authenticating the identity of the Sponsor as representing the Subscriber.

Upon successful validation of the revocation request by the Agency RA, the request is submitted to the SSP. Access to the SSP to request revocation is protected using SSL/TLS and requires presentation of a valid RA certificate. The SSP will change the certificate status in the Repository from valid to revoked and the serial number of the revoked certificate will be placed on the next published CRL.

The SSP 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 his or her 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 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

The SSP will generate and issue CRLs at least every eighteen (18) hours. All 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, a CRL will be issued within six (6) hours of notification.

When a certificate issued under the *id-fpki-common-High* is revoked because of compromise or suspected compromise of a private key, a CRL must be issued within 6 hours of notification.

### 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 CSA to enable certificate status checking using the Online Certificate Status Protocol.

OCSP responses are compliant with RFC 5019 and/or RFC 6960 and are signed by an OCSP responder Certificate. OCSP responder Certificates are signed by the Issuing CA. Those OCSP responder Certificates sign OCSP responses for any inquiries about the revocation status of a Certificate issued by that CA.

The OCSP responder 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 HSM. 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 be at least as frequent as 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.

The CA shall operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

The CA shall maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA.

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

The SSP CA supports on-line status checking via OCSP for end entity certificates issued under *id-fpki-common-authentication, id-fpki-common-derived-pivAuth-hardware, id-fpki-common-derived-pivAuth,* and *d-fpki-common-cardAuth*.

### 4.9.10 On-line Revocation Checking Requirements

Agencies issuing end entity certificates under *id-fpki-common-authentication, id-fpki-common-derived-pivAuth-hardware, id-fpki-common-derived-pivAuth* and *id-fpki-common-cardAuth* are configured to utilize DigiCert OCSP services as the primary status checking mechanism for such certificates as described in section 4.9.9 of this CPS.

Client software using online status checking need not obtain or process CRLs but CRLs will still be available through the processes described in section 2.2.1 and 4.9.7 of this CPS.

### 4.9.11 Other Forms of Revocation Advertisements Available

No other form of Revocation status is available.

### 4.9.12 Special Requirements Regarding Key Compromise

In the event of a CA key compromise, the FPKIPA shall be immediately informed by the DCPA, as well as the US Government Root CA. 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.

CRL issuance for CA and Subscriber key compromise is described in section 4.9.7.

Agencies operating RAs are responsible for notification and revocation of subscriber certificates due to key compromise and will describe this process in their RPS. 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 by the RAs.

### 4.9.14 Who Can Request Suspension

The Subscriber is authorized to request the suspension of their own certificate. The RA, the Subscriber's authorizing organization, or other authorized party can request the suspension of a Subscriber's certificate on the Subscriber's behalf. 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 authentication of a valid RA certificate to the CMS. The RA checks that the RA affiliation is the same as the organizational affiliation in the certificate to be suspended. If these checks are successful, the RA will change the certificate status in the repository from "valid" to "suspended" and the CMS completes the suspension in order to 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. RAs are required to maintain this period and revoke or unsuspend the Certificate before the 30 day period ends. If the suspension remains in place through the 30 day period, the RA will either remove the suspension or revoke the Certificate prior to the end of the 30th day. The suspension process and the suspension period monitoring practices will be defined in the respective RPS if the CMS can perform suspension.

## *4.10 Certificate Status Services*

SSP CAs provide certificate status services via OCSP, via CRLs accessible by HTTP and direct HTTP query of the online repository. 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. CA private keys are never escrowed. 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 two-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 respective RA's RPS, Appendix E, 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 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 access while the cryptographic module is installed and activated. Physical security controls are implemented to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. 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 physically protected environments to deter, detect, and prevent unauthorized use of, access to, or disclosure of sensitive information. The primary site location is in [Text Removed], additional key storage in [Text Removed] (for backup key storage as described in section 5.1.2.2 and 5.1.2.3), and the DRF is at a facility in [Text Removed]. The facilities housing the primary and back-up CA and Repository provide extensive physical security and access control systems to limit access only to authorized personnel and authorized visitors (as described in Section 5.1.2.1). These facilities reside in geographically diverse areas.

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/or 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 and CSAs) and operation of the 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 situated within agency premises 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 alarm systems that are 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's alarm system is activated at a minimum when the building is unattended for periods greater than 8 hours. The datacenter 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 employees located in a security station monitor access to the buildings 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 anti-passback features 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 each building, the roofs, and sensitive areas of 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*

The SSP 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*

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

RAs must protect equipment from unauthorized access while the cryptographic module is installed and activated. RAs implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the RA equipment environment and described in the respective RPS to meet this section of the CPS and the Common CP.

### 5.1.2.3 Physical Access for CSS Equipment

Physical access control requirements for CSS equipment (if implemented), meets the CA physical access requirements specified in 5.1.2.1 in this CPS and in the Common CP.

### 5.1.3 Power and Air Conditioning

The SSP CA operates in a high availability configuration (i.e. redundant hot-standby systems at both the primary data center and the Disaster Recovery site datacenter). The SSP primary and backup facilities 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 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 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 SSP has a disaster recovery (hot) site in Virginia. Access to media is limited to authorized personnel and stored within the 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 five 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. In general, 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 role and their responsibilities 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 Agency RA in providing Subscriber identity verification during the registration process. Trusted Agents do not have automated interfaces with the SSP CA. 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 Agency RA 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, such as access to and management of Cryptographic Signing Units (CSU), CA key generation, CA signing key activation and CA private key backup require multiple trusted employees, one of which must be a holder of the Administrator role. Multiparty control of CA operations shall exclude personnel that serve in the Auditor Trusted Role.

RA 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 different RA Administrators, who control the password to the HSM and configures the CMS system for HSM access, and the other RA Administrator that utilizes the CMS RA private keys and the CMS PIV 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 SSP maintains a policy and rigorous control procedures to ensure segregation of duties based on job responsibilities. SSP RAs do not have any other roles on the SSP CA or CSA systems. A person holding the *CA Auditor* or *CSA Auditor* role may not hold any other role on the CA or the CSA.

No person assigned to a trusted role has more than one identity on the CA, the RA and the CSA.

## *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 for the 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

All persons filling trusted roles for the SSP shall be US citizens. All DigiCert persons filling trusted roles shall undergo a background investigation.  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 five (5) years:

1. Criminal history;
2. Previous employment;
3. Professional references;
4. Education (verification of highest or most relevant degree); and
5. Driver's license records[2] (violations and place of residence).

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 shall include all duties they are expected to perform, including, the operation of the SSP software and hardware, operational and security procedures, disaster recovery and business continuity operations, and requirements of this CPS.

[2] Place of residence check is limited to the last three (3) years.

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

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 personnel who violate the provisions of this CPS are subject to administrative and disciplinary action, including suspension or termination.

### 5.3.7 Independent Contractor Personnel Requirements

Any 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*

Audit log files shall be generated for all events relating to the security of the CA. Security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

### 5.4.1 Types of Events Recorded

All security auditing capabilities shall be enabled during installation of the SSP equipment to record events for the CA, RA, Agency 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)[3], 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 date and 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.

[3] 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 Common CP.

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
- IDENTIFICATION AND AUTHENTICATION:
  - Successful and unsuccessful attempts to assume a role
  - The value of maximum authentication attempts is changed
  - Maximum number of allowed 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 passwords
  - Attempts to modify passwords
  - Backing up CA internal database
  - Restoring CA internal database
  - File manipulation (e.g., creation, renaming, moving)
  - Posting of any material to a repository
  - Access to CA internal database
  - All certificate compromise notification requests
  - Loading tokens with certificates
  - Shipment of HSMs
    - Zeroizing HSMs
  - 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 digital media on a daily basis and labeled with a system-generated barcode to support digital 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.

For SSP CAs that issue *id-fpki-common-High* certificates, the review of the audit log will occur at least once every month.

### 5.4.3 Retention Period for Audit Log

All electronic audit data for the SSP CA, SSP RA, SSP CSA and Agency RA interaction with the SSP CAs is collected and maintained by the SSP. The SSP has the ability to recover audit log information from on-line and archive storage. SSP RAs and SSP CSAs are responsible to maintain their audit logs as stated in their individual RPS.

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 SSP currently relies on procedural (personnel and facility) controls to protect audit records from accidental or malicious overwrite. 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 Manager of Security provides an additional oversight and enforcement role.

The 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 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 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 and ATOs,
- 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 and ATOs,
- Certificate Policy
- Certification Practice Statement
- Contractual obligations
- Other agreements concerning operations of the CA
- System and equipment configuration
- Modifications and updates to system or configuration
- Certificate requests
- All certificates issued and/or published
- Record of Re-key
- Revocation requests
- Subscriber identity Authentication data as per Section 3.1.9
- Subscriber agreements
- Documentation of receipt of tokens
- All CARLs and CRLs issued and/or published
- Other data or applications to verify archive contents
- Compliance Auditor Reports
- Changes made to the Audit parameters, e.g. audit frequency, type of event audited
- Attempts to delete or modify the Audit logs
- CA key generation (not mandatory for single session or one-time use symmetric keys)
- Access to escrowed Subscriber private encryption keys escrowed for key recovery purposes
- Changes to the trusted public keys including additions and deletions
- Export of private and secret keys (with the exception of keys used for a single session or messages)
- 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 without loss of data in the event of a catastrophic system fault. System backups are stored at an offsite third party facility [Text Removed].

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

For SSP CAs that issue *id-fpki-common-High certificates*, archive records are retained as above for a period of at least twenty (20) years and six (6) months.

### 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 and in accordance with sections 9.3 and 9.4. 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. If the original media cannot retain the data for the required period, the archived data shall be transferred to new media. Applications needed 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 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, and other revocation database entries contain time and date information. Such time information is not cryptographic-based as described in section 6.8. The archives are time-stamped at the time of creation using Network Time Protocol based on atomic clock signals from the GPS system.

### 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 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 backup media. 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, Production 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 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.

CA certificate usage periods will be a maximum of 10 years to ensure that the validity interval of user certificates (up to 3 years) will expire before the validity interval of the CA certificate. The SSP will change its keys periodically according to the key usage periods in section 6.3.2 to ensure that no certificate is issued with a life beyond the expiration date of the CA certificate. The SSP CA does not support key rollover certificates. Key changeover of a CA requires a new CA certificate be issued. The SSP CA will continue to interoperate through cross-certification with the Common Policy Root CA following key rollover regardless whether the Common Policy Root CA DN is changed.

After an SSP CA performs a Key Changeover by issuing a new CA Certificate or performing a Re-Key per section 4.7, 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 passed. 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 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 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.

DigiCert will notify the FPKIPA if any CAs operating under the CPS experience the following:

- suspected or detected compromise of the CA systems;
- suspected or detected compromise of a certificate status server (CSS) if
  (1) the CSS certificate has a lifetime of more than 72 hours and
  (2) the CSS certificate cannot be revoked (e.g., an OCSP responder certificate with the id-pkix-ocsp-nocheck extension);
- physical or electronic penetration of CA systems;
- successful denial of service attacks on CA components; or
- any incident preventing the CA from issuing a CRL within 48 hours of the issuance of the previous CRL.

DigiCert will reestablish operational capabilities as quickly as possible in accordance with the procedures stated earlier in this section.

In the event of an incident, DigiCert will notify the FPKIPA within 24 hours of incident discovery, along with preliminary remediation analysis.

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

1. Which CA components were affected by the incident
2. The CA'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
6. A statement that the incident has been fully remediated

The notification provided directly to the FPKIPA will include detailed measures taken to remediate the incident. The FPKIPA will post the notices to idmanagement.gov and provide an announcement to all Federal Agencies and Bridge Affiliate PKIs.

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

Before returning to operation, the SSP CA shall ensure that the system's integrity has been restored as specified in section 13.6 of the DigiCert PKI SSP System Security Plan. 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 within the CRL issuance schedule specified in section 4.9.7.  If the CA signature keys are destroyed**,** CA operation shall be reestablished as quickly as possible, giving priority to the generation of a new CA key pair.

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, physical or electronic penetration of CA systems, the DCPA shall be immediately informed, as well as the FPKI PA and  US Government Root CA. The SSP Root CA 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 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

DigiCert maintains redundant hardware and backups of its CA and infrastructure system software at its disaster recovery facility. In addition, CA private keys are backed up and maintained for disaster recovery purposes in accordance with CPS section 6.2.4.   DigiCert maintains offsite backups of important CA information for SSP CAs, including, but not limited to: Certificate Application data, audit data (per Section 4.5), and database records for all Certificates issued.

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 the SSP 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 48 hours after the time specified in the next update field of the currently valid CRL, the FPKIPA shall be informed, as well as the Agency PMA(s) where appropriate. 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 the SSP signature key is destroyed as a result, the SSP will initiate certificate management operations from its Disaster Recovery site using the backup CA key pair or giving priority to the generation of a new CA key pair if the backup pair is not available.

In the case of a disaster whereby both the primary and DRF SSP CA installations are physically damaged and all copies of the SSP CA signature key are destroyed as a result, the FPKIPA shall be notified at the earliest feasible time, and the FPKIPA shall take whatever action it deems appropriate. Relying Parties may decide of their own volition whether to continue to use certificates signed with the destroyed private key pending reestablishment of CA operations with new certificates.

## *5.8 CA or RA Termination*

In the event of termination of the SSP CA before all certificates have expired, the CA signing keys shall be surrendered to the FPKIPA.

Before the keys are surrendered, the following actions are taken:

- Notice shall be provided to all Subscribers and according to section 5.7 prior to termination;
- Whenever possible, the FPKIPA shall be notified at least two weeks prior to the termination of the SSP CA;
- Any actions needed to ensure continued support for certificates issued by the SSP CA shall be taken in accordance with agreements;
- All unexpired 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 past. After the final CRL has been issued, the private signing key of the SSP CA will be destroyed or taken offline, designated as "not in use", and protected as stipulated in section 5.1.2;Dissemination of revocation notice will be achieved as discussed in CPS section 5.7.1 and 5.7.3.; and
- The SSP CA also transfers its archival records to an Agency PMA approved archival facility. Currently DigiCert uses the services of Iron Mountain for offsite storage and archival.

Note: This section does not apply to CAs that have ceased issuing new certificates but are continuing to issue CRLs until all certificates have expired. Such CAs are required to continue to conform with all relevant aspects of this policy (e.g., audit logging and archives).

# 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 modules. The ceremony is recorded and a full audit trail record is created to ensure that all security requirements, including separation of roles were followed. Key ceremonies are performed under dual control of a Key Ceremony Administrator and witnessed by another trusted employee. 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. Subscriber key pairs for encryption certificates are generated by the SSP Key Management System. Subscriber Derived PIV certificates are generated on a Subscriber's local system/device (after authenticating to an SSP or RA (as specified in section 4.2.1). Subscriber Derived PIV hardware certificates are generated on Subscriber's hardware that meets the cryptographic standards (FIPS 140 Level 2 or higher), after authenticating to the SSP or an RA (as specified in section 4.2.1) PIV content Signing Certificates are generated through the operating system of a CMS to a cryptographic module. At no time does the Subscriber private key appear in plain-text form outside the hardware protection boundary of the cryptographic module.

The 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-fpki-common-policy, id-fpki-common-derived-pivAuth,* or *id-fpki-common-devices* certificates, Subscriber signature key pairs are generated in a FIPS 140 Level 1 cryptographic module (i.e., browser software).

For *id-fpki-common-hardware, id-fpki-common-devicesHardware, id-fpki-common-High, id-fpki-common-authentication, id-fpki-common-derived-pivAuth-hardware* or *id-fpki-common-cardAuth*, Subscriber signature key pairs are generated in a FIPS 140 Level 2 cryptographic 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.

DigiCert RA and Agency RA keys are generated in a FIPS 140 Level 2 validated cryptographic module.

#### 6.1.1.3 CSS Key Pair Generation

Cryptographic keying material used by CSSes to sign status information are generated in FIPS 140 validated cryptographic modules. For the DigiCert SSP, the module(s) meet or exceed FIPS 140 Level 2.

#### 6.1.1.4 PIV Content Signing Key Pair Generation

Cryptographic keying material used by PIV issuing systems or devices for Common PIV Content Signing must be generated in FIPS 140 validated cryptographic modules. The module(s) maintained by RAs for the DigiCert SSP meet or exceed FIPS 140 Level 2. Key generation procedures are documented in the respective RPS for the RAs.

### 6.1.2 Private Key Delivery to Subscriber

The SSP CA shall only issue certificates to a single Subscriber. Certificates shall not be issued that contain a public key whose associated private key is shared. Subscriber private keys are delivered as follows:

Hardware Credential

Key generation for authentication certificates are stored and generated on hardware secure modules. 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 module is in the possession of the Agency RA who is responsible for accountability of the module until the Subscriber accepts possession of it (with the exception of Derived PIV credential implementation that may be performed through authenticating an existing PIV credential at a self-service CMS station solution)The Subscriber acknowledges receipt of the hardware secure module and the SSP CA requires a record of the subscriber acknowledgment through the RA records.

Private Encryption keys are generated in an Agency hosted Key Manager which delivers the keys to the issuance system for downloading to the Subscriber’s hardware security 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 security module. After the private Encryption key is injected into the hardware security module, the PKCS#12 file and password are erased by the card management software.

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 Agency 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/TLS-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/TLS-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.

The unlock password for the PKCS #12 file is provided to the Subscriber on an SSL/TLS-protected web page. Passwords for access to the hardware tokens are chosen by the Subscriber at the time of installation of the token manager software.

### 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 shall 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 is 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 is 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.

## 6.1.3 Public Key Delivery to Certificate Issuer

Secure delivery uses a cryptographic algorithm and key size at least as strong as the private key. The Subscriber's identity information and public key are securely delivered to the certificate issuer as follows.

<u>Hardware Credential</u>

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.

<u>Software Credential</u>

The Subscriber's identity information and public key are delivered in a certificate signing request to the SSP CA over an SSL/TLS-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

Relying Parties will be required to compare the SSP Root Certificate hash against the hash value received from a Trusted Agent, DigiCert RA or Agency RA.

Alternatively, these certificates may be imported onto the Subscriber smart card at the time of certificate enrollment by the Agency RA.

## 6.1.5 Key Sizes and Signature Algorithms

Signature algorithms shall conform to RSA PKCS#1. Key sizes and hash algorithms are detailed below:

- The key pairs for SSP CAs are 2048-bit RSA key pairs and those that expire after 12/31/2030 shall be at least 3072 bits for RSA or 256 bits for elliptic curve algorithms.
- The key pairs for all end entity certificates are at least 2048-bit RSA key pairs.
  The key pairs for end entity certificates issued under *id-fpki-common-devices* and *id-fpki-common-*

*devicesHardware* that expire after December 31, 2030 shall be at least 3072 bits for RSA or 256 bits for elliptic curve algorithms.

- All SSP CAs, including the SSP Intermediate CA and the Agency SSP CAs shall use SHA-256 for digital signature. The CSAs use the same signature algorithm, key size and hash algorithm used by the CA to sign CRLs. Signatures on certificates and CRLs shall be generated using SHA-256.
- SSP CA-issued Transport Layer Security (TLS) or Secure Socket Layer (SSL) certificates currently use AES (128 bits) for symmetric keys and 2048 bit RSA for asymmetric keys. After December 31, 2030 asymmetric keys shall be at least 3072 bit for RSA or at least 256 bit for elliptic curve algorithms.

### 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]. Public key parameters for signature algorithms defined in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186-4.

Parameter Quality Checking
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)

All certificates include a critical key usage extension. The SSP CA issues client Signature certificates with the key usage extension for signing and client authentication and issues encryption certificates with the key usage extension for encryption.

Public keys that are bound into human Subscriber certificates are used only for signing or encrypting, but not both. Subscriber certificates that assert *id-fpki-common-authentication* or *id-fpki-common-cardAuth* only assert the *digitalSignature* bit. Other human 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. Certificates that contain elliptic curve public keys that are used for key agreement assert the *keyAgreement* bit.

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 assert 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) Certificates 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) shall 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 that contain elliptic curve public keys that are used for key agreement assert the *keyAgreement* bit. Device certificates do not assert the *nonRepudiation* bit.

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

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

Signing certificates issued under the CPS for *id-fpki-common-piv-contentSigning* shall include an extended key usage of *id-PIV-content-signing*

The *dataEncipherment*, *encipherOnly*, and *decipherOnly* bits shall not be asserted in certificates issued per this CPS. All certificates shall 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-fpki-common-policy, id-fpki-common-devices, id-fpki-common-derived-pivAuth*) 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-fpki-common-hardware, id-fpki-common-devicesHardware, id-fpki-common-authentication, id-fpki-common-cardAuth, id-fpki-common-High, id-fpki-common-derived-pivAuth-hardware*) are obligated to use cryptographic modules that meet at least the criteria for FIPS 140 Level 2 hardware for all cryptographic operations.

The SSP RA and Agency 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.

PIV Cards are PKI tokens that have private keys associated with certificates asserting *id-fpki-common-authentication* or *id-fpki-common-cardAuth*. PIV 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). On an annual basis, for each PCI configuration used (as defined by the FIPS 201-2 Evaluation Program), one populated, representative sample PIV Card shall be submitted to the FIPS 201-2 Evaluation Program for testing.

All cryptographic modules dedicated to management of 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 Agency RA, is physically separated from the SSP which is located within the DigiCert datacenters described in section 5.1.2.1.

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

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

When the SSP certificate signing key pair is generated in DigiCert’s Key Ceremony rooms in 5.1.2.3, the PIN required to activate the associated hardware HSM 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 storage 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 HSM is so initialized, the key pair generated and the associated CA certificate signed by its superior CA, the HSM is ultimately moved to a separate Secure Data Center room for activation into an operational state. Activation of the HSM 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 Key

CA private keys are not escrowed.

### 6.2.3.3 Escrow of Subscriber Private Signature Key

Subscriber private signature keys are not escrowed.

### 6.2.3.4 Escrow of Subscriber Encryption Key

DigiCert 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 which is hosted at the Agency 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 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 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 five (5) copies of the SSP CA and CSA private keys. There is no need to backup 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 usually made during the original key ceremony process using a secure process specifically designed for cloning of key pairs.

#### 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 ensuring security controls consistent with the protection provided by the Subscriber's cryptographic module.

Subscriber private Signature keys are never escrowed.

For 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-fpki-common-authentication*
- *id-fpki-common-cardAuth*
- *id-fpki-common-High*
- *id-fpki-common-derived-pivAuth-hardware*

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

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 CSA Private Key

See 6.2.4.1.

#### 6.2.4.5 Backup of Device Private Key

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.

#### 6.2.4.6 Backup of Common PIV Content Signing Key

The Common PIV Content Signing private signature keys is backed up under multi-person control. At least one copy of the private signature key shall be stored in a secondary location. All copies of the Common PIV Content Signing private signature key are accounted for and protected in the same manner as the original. Backed up Common PIV Content private signature keys are not exported or stored in plaintext form outside the cryptographic module. Backup procedures are documented in the RPS of the respective RA.

### 6.2.5 Private Key Archival

CA private Signature keys and Subscriber private Signature keys are not archived. The SSP provides archive of escrowed 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 CA makes a backup copy of its private key, the key is transferred to the backup hardware HSM 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 in 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-fpki-common-authentication, id-fpki-common-cardAuth, id-fpki-common-hardware, id-fpki-common devicesHardware* or *id-fpki-common-High* policy may use the secure export/import capability in the latest versions of the browsers 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 in accordance with section 6.2.1.

### 6.2.8 Method of Activating Private Key

The SSP 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.

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-fpki-common-authentication, id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-derived-pivAuth, id-fpki-common-derived-pivAuth-hardware* or *id-fpki-common-High* 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.

For certificates issued under *id-fpki-common-devices* and *id-fpki-common devicesHardware*, 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-fpki-common-piv-contentSigning*, key activation requires multi-party control as stipulated in section 5.2.2.

For certificates issued under *id-fpki-common-cardAuth*, Subscriber authentication is not required to use the associated private key.

### 6.2.9 Method of Deactivating Private Key

The SSP and CSA hardware tokens are operated in a five-tiered secured 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 no greater than 5 minutes or by removing them from the smart card reader.

The department or agency shall implement technical or administrative controls to enforce this policy.

### 6.2.10 Method of Destroying Private Key

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 Agency 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 all SSP CA key pairs is a maximum of ten (10) years. The SSP CA private key may be used to generate certificates for at most four (4) years, and the public key may be used to validate certificates for the entire usage period. If the CA private key is used to sign CRLs, it may be used to sign CRLs for the entire usage period. All certificates signed by a specific CA key pair must expire before the end of that key pair's usage period.

Subscriber public keys in certificates that assert the *id-PIV-content-signing* OID in the extended key usage extension have a maximum usage period of nine (9) years. The private keys corresponding to the public keys in these certificates have a maximum usage period of three (3) years. Expiration of the *id-fpki-common-piv-contentSigning* certificate shall be later than the expiration of the *id-fpki-common-authentication, id-fpki-common-derived-pivAuth-hardware*, or *id-fpki-common-derived-pivAuth* certificates.

OCSP responders and all other subscriber public keys have a maximum usage period of three (3) years. Subscriber Signature private keys have the same usage period as their corresponding public key. The usage period for Subscriber key management private keys is not restricted.

## *6.4 Activation Data*

### 6.4.1 Activation Data Generation and Installation

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

RAs are also required to choose their own PINs with an appropriate level of strength to protect their private key.

The PIV Content Signing key pairs shall be generated by an operating system component of the CMS and put on a FIPS 140 Level 2 or higher Cryptographic Module and conform to [NIST SP 800-78] requirements, including PIN generation requirements to protect the PIV content signing private key.

The PINs used to protect the SSP and CSA tokens are randomly and automatically generated. Activation data protecting access to the SSP hardware token is generated within the FIPS 140 Level 3 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 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. Each individual so trusted maintains a separate secure lock box where the share under their control is stored when not in use. At no time is the value of a share, or the PIN, written down. The SSP CA and SSP CSA PINs are not changed for the life of the keys because they are stored as shares on hardware tokens. The RA or Subscriber activation PIN is only known by the holder of the token.

### 6.4.3 Other Aspects of Activation Data

See Section 6.4.1.

## *6.5 Computer Security Controls*

### 6.5.1 Specific Computer Security Technical Requirements

The SSP and CSA employ operating systems that have been evaluated for security functionality, including audit requirements, identification and authentication, and discretionary access controls. [Text Removed]

The SSP operator accounts are implemented to provide individual authentication. 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. This is accomplished through strict personnel and procedural controls to limit these accounts to a few trusted individuals, and is augmented by manual and automated perimeter controls that monitor (via active badges) which individuals have access to the system at any particular time.

Remote workstations used to administer the CAs implement the following security functions:

- 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 in accordance with section 5.4;
- enforce domain integrity boundaries for security critical processes; and
- support recovery from key or system failure.

All communications between any PKI Trusted Role and the CA are authenticated and protected from modification.

### 6.5.2 Computer Security Rating

[Text Removed]

[Text Removed]

The 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 CA, 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 SSP 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 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, uninitialized 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 enveloped 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 Agency 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 is encrypted using the TLS protocol. All communications between the Agency 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].

For the purposes of administration, the SSP CA shall allow connection establishment with a remote workstation only after successful authentication of the remote workstation at a level of assurance commensurate with that of the CA.

[Text Removed] The 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 which log password hashes, for verifying password strength
  - [Text Removed], for checking file integrity and malicious code detection
  - [Text Removed]
- Security monitoring tools used on the network including, but not limited to:
  - [Text Removed]for internal and external network scanning
  - [Text Removed]for network IDS.

- Security monitoring tools [Text Removed] including, but not limited to:
    - Virus scanners

## 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

Certificates issued by a CA under this policy shall conform to the X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program [SSP-PROF].

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

## *7.1 Certificate Profile*

### 7.1.1 Version Number(s)

The 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 are based on the X.509 Certificate and Certificate Revocation List Extensions Profile for the Shared Service Providers Program [SSP-PROF].

### 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 } |

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 responses.

### 7.1.4 Name Forms

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

Each RDN contains a single attribute type, value pair. DirectoryString values are encoded as printable string.

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 certificates issued under *id-fpki-common-authentication* and *id-fpki-common-cardAuth* the subject alternative name extension shall be present and include the pivFASC-N name type and a UUID encoded as a URI. In certificates issued under *id-fpki-common-derived-pivAuth-hardware* and *id-fpki-common-derived-pivAuth*, the subject alternative name extension shall be present and include a UUID encoded as a URI.

### 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. Certificates that express the *id-fpki-common-piv-contentSigning* shall not express any other policy OIDs.

### 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 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 SSP CA shall conform to the CRL profile specified in [SSP-PROF].

### 7.2.1 Version Number(s)

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

### 7.2.2 CRL and CRL Entry Extensions

The SSP CA shall issue CRLs that comply with the extensions specified in the CRL profiles detailed in [SSP-PROF].

## *7.3 OCSP Profile*

SSP CSAs shall sign responses using algorithms designated for CRL signing. SSP CSAs shall use OCSP version 1. Critical OCSP extensions are not used.

# 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The DCPA is responsible for ensuring audits are conducted for all PKI functions regardless of how or by whom the PKI components are managed and operated.

## 8.1 Frequency or Circumstances of Assessment

The SSP CA, CSA and RA shall undergo an annual compliance audit as part of the DigiCert annual PKI audit, and will make itself available for additional compliance audits that may be required by the PA. The Agency RAs 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 Assessor

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

The Agency PMA is responsible for identifying and engaging a qualified auditor of Agency 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 Common Policy.
- 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 Assessed Entity

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 SSP auditor has not served in developing or maintaining DigiCert’s CA facility or Certification Practices Statement.

The Agency’s RA and/or CMS auditor shall be an independent organization[4] engaged through a contractual relationship for audit services and may not have any other role or responsibility relating to the agency’s SSP operation.

## 8.4 Topics Covered by Assessment

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 SSP CA/RA operations and the Agency RA/CMS

[4] 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.

operations shall be subject to compliance audit inspections in accordance with this CPS and any corresponding Registration Practices Statement (RPS).

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.

## 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 and appropriate Agency PMA.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the FPKIPA and DCPA may decide to temporarily halt operation of the CA, RA or CMS, to 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 Agency CMS compliance auditor shall report the results of a compliance audit to the Agency and supply a signed Auditor Letter of Compliance addressed to the DCPA. The Agency shall supply the signed Auditor Letter of Compliance to the DCPA. Additionally, on request from the FPKIPA, the Agency shall supply the full audit results report.

On an annual basis, the DCPA shall submit an annual review package to the FPKI PA. 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 DCPA, 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

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

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 1.5.

### 9.2.3 Insurance or Warranty Coverage for End-Entities

The SSP does not offer warranty protection.

## *9.3 Confidentiality of Business Information*

Information deemed confidential is protected in accordance with section 9.4. CA information not requiring protection is made publicly available through an online Repository as described in Section 2.2.

### 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 repository 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 SSP 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. However, certificates that contain the FASC-N in the subject alternative name extension, such as PIV Authentication Certificates, shall not be distributed via public repositories (e.g., via 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.

Sensitive information is stored securely, and released only in accordance with other stipulations in section 9.4.

### 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 private keys are the personal property of DigiCert, Inc.
- DigiCert Public Keys: SSP 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;
- 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 9.6.4; and
- Operating or providing for the services of an online repository that satisfies the obligations under Section 2, and informing the repository service provider of their obligations if applicable.

### 9.6.2 RA Representations and Warranties

An RA or TA who performs registration functions as described in this CPS shall comply with the stipulations of this CPS and the CP. An RA or TA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA/TA responsibilities.

An RA supporting this policy shall conform to the stipulations of this document, including:

- Performing in-person identity 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 9.6.4, and that Subscribers are informed of the consequences of not complying with those obligations.

### 9.6.3 Trusted Agent Representations and Warranties

A Trusted Agent who performs identification and authentication functions as described in this CPS shall comply with the stipulations of this CPS and CP. A Trusted Agent who is found to have acted in a manner inconsistent with these obligations is subject to revocation of Trusted Agent responsibilities.

A Trusted Agent supporting this CPS shall conform to the stipulations of this document, including:

- Performing in-person identity verification of certificate applicants in accordance with Section 3.2.3;
- 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 9.6.4, and that Subscribers are informed of the consequences of not complying with those obligations.

### 9.6.4 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 Section 9.9;
- 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.

Subscribers shall:

- Accurately represent themselves and ensure the accuracy of information provided in all communications with the SSP CA, RA, and/or TA;
- Protect their private keys at all times, in accordance with this CPS, and as set forth in the applicable Subscriber agreements;
- Prevent unauthorized disclosure of their private keys and activation data in accordance with Sections 6.2.4.2 and 6.2.8;
- Notify the SSP, 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;

- Abide by all the terms, conditions, and restrictions levied upon the use of their private keys and certificates;
- 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 SSP 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.
If the human sponsor for a device is not physically located near the sponsored device, and/or does not have sufficient administrative privileges on the sponsored device to protect the device's private key and ensure that the device's certificate is only used for authorized purposes, the device sponsor may delegate these responsibilities to an authorized administrator for the device. The delegation shall be documented and signed by both the device sponsor and the authorized administrator for the device. Delegation does not relieve the device sponsor of his or her accountability for these responsibilities.

### 9.6.5 Relying Party Representations and Warranties

The following summarizes the obligations and responsibilities of parties who rely upon a certificate received from the SSP 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.

### 9.6.6 Representations and Warranties of Other Participants

#### 9.6.6.1 DigiCert PA Obligations

The DCPA 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.

#### 9.6.6.2 Agency PMA Obligations

The Agency PMA shall—

- Review periodic compliance audits to ensure that RAs and other components operated by the agency 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; and
- Review name space control procedures to ensure that distinguished names are uniquely assigned within their agency.
- Notify appropriate entities in the event of RA compromise or termination.

## *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 "non-repudiation" for any DigiCert certificate or any message (because non-repudiation 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 Section 9.7.3 (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 Relationship

The SSP CA or RA 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*

The U.S. Government shall not be liable to any party, except as determined pursuant to the Federal Tort Claims Act (FTCA), 28 U.S.C. 2671-2680, or as determined through a valid express written contract between the Government and another party.

### 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 SSP, its RAs or Trusted Agents in connection with a single transaction involving the use or reliance on a certificate shall be limited to one thousand dollars ($1,000 USD).

Furthermore, DigiCert's total liability for any incident (aggregate of all transactions) involving the use or reliance on a certificate shall be limited to fifty thousand ($50,000 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 5.8.

### 9.10.3 Effect of Termination and Survival

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 (Individual Notices and Communications with Participants), 9.13 (Dispute Resolution Provisions), 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 at:
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 of the person on file with DigiCert, Inc.

If any planned change to the infrastructure has the potential to affect the FPKI operational environment, that change will 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 will be provided to the FPKI PA 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 1.5 of this document.

The DCPA, 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 DigiCert SSP CPS will be published on the legal repository and available for relying parties as soon as feasible.

This SSP CPS is published as described in Section 2.2.2. Applicable updates to this CPS that affect Subscribers and Relying Parties will be published as described in Section 2.2.2.

### 9.12.3 Circumstances under Which OID must be Changed

If the FPKI determines that a change is necessary in the object identifier corresponding to its Certificate policy, the amendment shall contain new object identifiers for the Certificate policies corresponding to each type 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 FPKIPA shall facilitate the resolution between entities when conflicts arise as a result of the use of certificates issued under this CPS. When the dispute is between Federal agencies, and the FPKIPA is unable to facilitate resolution, dispute resolution may be escalated to OMB or U.S. Department of Justice, Office of Legal Counsel as necessary.

DigiCert shall investigate and correct if necessary any name collisions brought to its attention. If appropriate, DigiCert shall coordinate with and defer to the EPMA (External Policy Management Authority) 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 Utah 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 and the MOA between DigiCert and the FPKIPA shall be governed by the laws of the United States of America.

If you are an individual or entity within the United States Government and have purchased the services associated with this CPS, this Agreement, and the interpretation of it, will be governed, as applicable, by the Contract Disputes Act of 1978, as amended (codified at 41 U.S.C. § 601 et seq.).

## *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 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 Section 5.8, 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 Federal Common Policy CP and this CPS, the Federal Common Policy CP 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.

# APPENDIX A:  CERTIFICATE AND CRL FORMATS

All certificates and CRLs associated with the SSP PKI service will meet the certificate and CRL formats specified in the X.509 Certificate and Certificate Revocation List Extensions Profile for the Shared Service Providers Program available here:

Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile:
http://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-x509-cert-profile-ssp.pdf

# APPENDIX B: DEFINITIONS

| | |
|---|---|
| access | Ability to make use of any information system (IS) resource. |
| access control | Process of granting access to information system resources only to authorized users, programs, processes, or other systems. |
| accreditation | Formal declaration by a Designated Approving Authority that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. |
| 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. |
| crypto period | Time span during which each key setting remains in effect. |
| data integrity | Assurance that the data are unchanged from creation to reception |
| 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). |
| Legacy Federal PKI | A PKI implementation owned and managed by a Federal Agency and cross-certified with the Federal Bridge prior to 12/31/2005. |
| 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. |
| 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 Common CP and in 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, (2) holds a private key that corresponds to a public key listed in that certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual, an application or network device. 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. |
| 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. They provide 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 C: REFERENCES

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

| Number | Title | Date |
|---|---|---|
| ABADSG | *Digital Signature Guidelines* <br> *http://www.abanet.org/scitech/ec/isc/dsgfree.html* | 1 August 1996 |
| SSP-PROF | *X.509 Certificate and CRL Extensions Profile for the Shared Service Providers (SSP) Program* *http://www.cio.gov/fpkipac/documents/CertCRLprofileForCP.pdf* | |
| E-Auth | *E-Authentication Guidance for Federal Agencies, M-04-04* | 16 December 2003 |
| FIPS140 | *Security Requirements for Cryptographic Modules* <br> *http://csrc.nist.gov/publications/index.html* | 21 May 2001 |
| FIPS112 | *Password Usage* <br> *http://csrc.nist.gov/* | 5 May 1985 |
| FIPS186-4 | *Digital Signature Standard* <br> https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf | July 2013 |
| FIPS201-2 | *Personal Identity Verification (PIV) of Federal Employees and Contractors* <br> https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf | August 2013 |
| FOIAACT | *5 U.S.C. 552, Freedom of Information Act* <br> *http://www4.law.cornell.edu/uscode/5/552.html* | |
| NS4009 | *NSTISSI 4009, National Information Systems Security Glossary* | January 1999 |
| PACS | *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems* *http://smart.gov/information/TIG_SCEPACS_v2.2.pdf* | 27 July 2004 |
| PKCS-1 | *PKCS #1 v2.1: RSA Cryptography Standard* <br> *http://www.rsasecurity.com/rsalabs/node.asp?id=2125* | 14 June 2002 |
| PKCS-12 | *Personal Information Exchange Syntax Standard* <br> *http://www.rsasecurity.com/rsalabs/node.asp?id=2138* | 24 June 1999 |
| 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 |
| RFC 6960 | *X509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP,* https://tools.ietf.org/html/rfc6960 | June 2013 |
| RFC3647 | *Certificate Policy and Certification Practices Framework, Chokhani and Ford.* <br> *http://www.ietf.org/rfc/rfc3647.txt* | November 2003 |
| RFC 4122 | *A Universally Unique IDentifier (UUID) URN Namespace, Paul J. Leach, Michael Mealling, and Rich Salz. http://www.ietf.org/rfc/rfc4122.txt* | July 2005 |
| RFC 5280 | *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* | May 2008 |
| SP 800-73-3(1) | *Interfaces for Personal Identity Verification – Part 1: End-Point PIV Card Application Namespace, Data Model and Representation, NIST Special Publication 800-73-3.* | February 2010 |

# APPENDIX D: ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| AES | Advanced Encryption Standard |
| CA | Certification Authority |
| CMA | Certificate Management Authority |
| CMS | Cryptographic Message Syntax |
| CP | Certificate Policy |
| CPS | Certification Practice Statement |
| CRL | Certificate Revocation List |
| CSA | Certificate Status Authority |
| 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 Standards |
| FPKI | (US) Federal Public Key Infrastructure |
| GSA | General Services Administration |
| HTTP | HyperText Transfer Protocol |
| HSM | Hardware Security Module |
| I&A | Identification and Authentication |
| ICA | Intermediate Certificate |
| ID | Identity (also, a credential asserting an identity) |
| ISO | International Organization for Standards |
| 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 (also referred to as Policy Management Authority (PMA)) |
| PIN | Personal Identification Number |
| PIV | Personal Identity Verification |
| PKCS | Public Key Certificate Standard |
| PKI | Public Key Infrastructure |
| PMA | Policy Management Authority (also referred to as Policy Authority (PA)) |
| 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 Services Provider |
| TA | Trusted Agent |
| TLS | Transport Layer Security |
| USD | United States Dollar |
| UUID | Universal Unique Identifier |

*APPENDIX E: KEY ESCROW AND RECOVERY*

# *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 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 "[Agency 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 [Agency name] KRPS. The DigiCert PMA approves all changes to the *DigiCert 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 SSP Customers. It is comprised of the [Agency name]-hosted Registration Authority (RA)[5] 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 Agency uses a Data Decryption Server the description goes here.*

[5] 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)

[Agency 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 SSP CPS* section 5. [Agency 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 Agency, 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 SSP CPS* section 5.

[Agency 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 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. [Agency 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 [Agency 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 [Agency name]. The intent of the KRPS is not to change the current procedures for obtaining information about individuals in connection with such requests. [Agency 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 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 SSP CPS* for authentication of individual identity during initial certificate enrollment or will be based on digital signatures that can be verified using [Agency 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 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 [Agency 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 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 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 [Agency 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 [Agency name] is subject to applicable law.

#### 3.2.3.2 Subscriber Authentication

If the Subscriber has a current, valid [Agency 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 [Agency 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 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 SSP CPS*.
The KRA authenticates to the KRA workstation using a [Agency 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 SSP CPS*.

#### 3.2.3.4 KRO Authentication

A KRO that is authorized to access the [Agency 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 Agency deploys and uses a Data Decryption Server this server shall authenticate to the KED using a public key certificate issued by the Agency, 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 Agency 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 [Agency 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 [Agency 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 [Agency 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 [Agency name]. DigiCert ensures the keys are successfully escrowed prior to issuance.

**Escrowed keys are protected during delivery to the Requestor by [Agency 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 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 [Agency 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 a 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 [Agency name] recovered decryption key shall not be revoked simply because the key was recovered. See the *DigiCert 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 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* **[Agency 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 SSP CPS*.

PIV CMS equipment containing the PIV Content Signing key meets the physical access requirements specified in section 5.1 in the *DigiCert 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 [Agency name] KRS.

#### 5.2.1.1 KED Roles

***5.2.1.1.1 System Administrator***
[Agency 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***
[Agency 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***
[Agency name] Audit Administrators are authorized to review, maintain, and archive KRS audit logs.

#### 5.2.1.2 Data Decryption Server Roles

*If applicable the Agency 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

[Agency 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 SSP CPS*. Auditors do not serve in a capacity to provide multiparty control.

[Agency 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 [Agency 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 [Agency 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 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 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 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 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 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 SSP CPS.*

### 5.4.6 Audit Collection System (internal vs. external)

The [Agency name] audit log collection system for the KED and KRA and/or KRO is the same as described in the *DigiCert 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

[Agency 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 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 SSP CPS.*

### 5.5.1 Types of Information Recorded

[Agency 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

[Agency 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 SSP CPS.*

### 5.5.3 Protection of Archive

Protection of the [Agency name] KED archive conforms with the requirements found in the same section 5.5.3 Protection of Archive in the *DigiCert SSP CPS* section 5.5.3.

### 5.5.4 Archive Backup Procedures

[Agency name] does not perform any other archive backups than that required in the *DigiCert SSP CPS.*

### 5.5.5 Requirements for Time-Stamping of Records

[Agency 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 Agency 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

[Agency name] will refer to the *DigiCert SSP CPS* for requirements on how archive information is obtained and verified.

## *5.6 Key Changeover*

[Agency 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 SSP CPS.*

## *5.7 Compromise and Disaster Recovery*

### 5.7.1 Incident and Compromise Handling Procedures

[Agency name] will refer to the *DigiCert SSP CPS* for requirements on incident and compromise handling procedures.

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

[Agency name] will refer to the *DigiCert 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

[Agency name] will refer to the *DigiCert SSP CPS* for requirements on private key compromise procedures, in section 5.7.3 Agency Private Key Compromise Procedures.

### 5.7.4 Business Continuity Capabilities After a Disaster

[Agency name] will refer to the *DigiCert 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

[Agency name] will refer to the *DigiCert SSP CPS* for key pair generation requirements beyond that required in key escrow and recovery operations.

### 6.1.2 Private Key Delivery to Subscriber

[Agency name] will refer to section 6.1.2 Private Key Delivery to Subscriber in the *DigiCert 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

[Agency name] will refer to section 6.2 Private Key Protection in the *DigiCert SSP CPS* for private key protection requirements that also pertain to key escrow and recovery operations.

## 6.3 Other Aspects of Key Pair Management

[Agency name] will refer to section 6.3 Other Aspects of Key Pair Management in the *DigiCert SSP CPS* for key pair management requirements that also pertain to key escrow and recovery operations.

## 6.4 Activation Data

[Agency name] will refer to section 6.4 Activation Data in the *DigiCert SSP CPS* for activation data requirements that also pertain to key escrow and recovery operations.

## 6.5 Computer Security Controls

[Agency name] will refer to the *DigiCert SSP CPS* for complete requirements for computer security controls in the KED.

*If the Agency uses remote administration for the KED and/or Data Decryption Server, the Agency shall not eliminate the requirement for two-person access control to the environment.*

[Agency 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

[Agency name] will use the *DigiCert SSP CPS* in the same section for details on Life Cycle Technical Controls.

## 6.7 Network Security Controls

[Agency name] will use the *DigiCert 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: *Agency 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

[Agency name] will use the *DigiCert 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

[Agency name] will use the *DigiCert Certificate Policy* and the *DigiCert 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

[Agency name] will use the *DigiCert Certificate Policy* and the *DigiCert SSP CPS* for details on Section 9.2.

## 9.3 Confidentiality of Business Information

[Agency name] will use the *DigiCert Certificate Policy* and the *DigiCert SSP CPS* for details on Section 9.3.

## 9.4 Privacy of Personal Information

[Agency name] will use the *DigiCert Certificate Policy* and the *DigiCert SSP CPS* for details on Section 9.4.

## 9.5 Intellectual Property Rights

[Agency name] will use the *DigiCert Certificate Policy* and the *DigiCert SSP CPS* in the same section for details on Section 9.5.

## 9.6 Representations and Warranties.

[Agency name] will use the *DigiCert Certificate Policy* and the *DigiCert 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 [Agency 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 sign an attestation to the effect: "I hereby state that I have legitimate and official need to recover this key in order to obtain (recover) the encrypted data that I have authorization to access. I acknowledge receipt of a recovered encryption key associated with the Subscriber identified here *[Subscriber Name]*. I certify that I have accurately identified myself to 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

[Agency name] will use the *DigiCert Certificate Policy* and the *DigiCert SSP CPS* in the same section for details on Section 9.8

## 9.9 Indemnities

[Agency name] will use the *DigiCert Certificate Policy* and the *DigiCert 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

[Agency name] will use the *DigiCert Certificate Policy* and the *DigiCert 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 SSP CPS* in the same section for details on Section 9.12.

## 9.13 Dispute Resolution Provisions

[Agency name] will use the *DigiCert Certificate Policy* and the *DigiCert SSP CPS* in the same section for details on Section 9.13.

## 9.14 Governing Law

[Agency name] will use the *DigiCert Certificate Policy* and the *DigiCert SSP CPS* in the same section for details on Section 9.14.

## 9.15 Compliance with Applicable Law

[Agency name] will use the *DigiCert Certificate Policy* and the *DigiCert SSP CPS* in the same section for details on Section 9.15.

## 9.16 Miscellaneous Provisions

[Agency name] will use the *DigiCert Certificate Policy* and the *DigiCert SSP CPS* in the same section for details on Section 9.16.

## 9.17 Other Provisions

[Agency name] will use the *DigiCert Certificate Policy* and the *DigiCert SSP CPS* in the same section for details on Section 9.17.

## *APPENDIX F: REVISION HISTORY*

| Version | Date / Status | Revision Details |
|---|---|---|
| 2.2 | April 2020 | Changes to address FPKI Comments from 2019 Annual SSP NFI Review. |
| 2.1 | May 2018 | 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 |

| Section | Changes made |
|---|---|
| Various | Specified PA throughout the document as either FPKIPA or DigiCert PMA (DCPA);<br>Corrected some typos;<br>Replaced http queries with ldap queries in some instances<br>Correct a few typos. |
| 1. INTRODUCTION | Removed:<br>The Symantec SSP PKI is also certified as an approved service by the GSA FIPS 201 Evaluation Program. |
| 1.1 Overview | Replaced “SSP” with “Federal” in “Federal Common Policy Root CA” |
| 1.2 Document Name and Identification | Added definition of id-pki-contentSigning polidy.<br>Removed Sha-1 OIDs and references |
| 1.3.1.2 Policy Management Authority | Removed the Federal PKI PA in this context |
| 1.4.1 Appropriate Certificate Uses | Removed Sha-1 references |
| 2.2.2 Publication of CA Information | Updated the link |
| 3.1.1 Types of Names | Added:<br>The Common PIV Content Signing certificate’s subject DN shall indicate the organization administering the PIV card issuance system or device according to types of names for devices. |
| 3.1.1.1 Geo-Political Name DN | Made the following changes:<br>At a minimum, tThe subject alternative name extension shall include a UUID and the pivFASC-N name type [FIPS 201]. The value for theis pivFASC-N name shall be the FASC-N [PACS] of the subject’s PIV card.<br><br>For certificates issued under id-fpki-common-cardAuth the subject alternative name extension shall also may alternatively include a UUID [RFC 4122].<br><br>Devices that are the subject of certificates issued under id-fpki-common-devices and id-fpki-common-devicesHardware may be assigned either a geo-political name or an Internet domain component name (see 3.1.1.2). |
| 3.1.1.2 Internet Domain Component Name | Added “id-fpki-common-devicesHardware” to the paragraph referring to device certificates. |
| 3.2.3.1 Authentication of Human Subscribers | Added the following note to point 4 for contractors and other affiliate personnel: |

| Section | Changes made |
|---|---|
| | (Handwritten signatures and other behavioral characteristics are not accepted as biometrics for the purposes of this policy.) |
| 4.2.1 Performing Identification and Authentication Functions | Added “Card Authentication certificate” and “Encryption certificate and Digital Signature certificate for cardholders with a government-issued email account at the time of credential issuance” to the applicable types of certificates. |
| 4.7.4 Notification of New Certificate Issuance to Subscriber | Replaced “No Stipulation” with:<br>Notification of issuance of a re-keyed certificate to the Subscriber is in accordance with Section 4.3.2 |
| 4.7.7 Notification of New Certificate Issuance by the CA to Other Entities | Replaced “No Stipulation” with:<br>RAs may receive notification of the issuance of certificates they approve |
| 4.9.9 On-Line Revocation/Status Checking Availability | Changed “token” to “HSM”.<br>Changed “FIPS level from 2 to 3.<br>Added the following:<br>The CA shall operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.<br>The CA shall maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA.<br>The CA shall maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint. |
| 4.12.2 Session Key Encapsulation and Recovery Policy and Practices | Removed “Non’” from “Non-Federal SSP PKI” |
| 5.2.1 Trusted Roles | Modified Trusted Roles to reflect responsibilities and requirements of the CP. |
| 5.3.1 Qualifications, Experience, and Clearance Requirements | Modifications added for roles and responsibilities for citizenship requirements. |
| 5.4.1 Types of Events Recorded | Added “date and time”<br>Corrected wording of one bullet point.<br>Replaced “tokens” with “HSMs” |
| 5.5.2 Retention Period for Archive | Added “without loss of data”.<br>Added reference ‘as above’ to specifications for common-High certificates |
| 5.5.6 Archive Collection System (Internal vs. External) | Replaced “No stipulation” with:<br>Symantec archive collection systems are internal, except for RA Customers. Symantec assists its RAs in preserving an audit trail. Such an archive collection system therefore is external to that RA |
| 5.6 Key Changeover | Replaced “every 3 years” with “periodically according to the key usage periods in section 6.3.2”<br>Added “OCSO responder certificates to reasons replaced keys will be retained for. |

| Section | Changes made |
|---|---|
| 5.7.3 Entity (CA) Private Key Compromise Procedures | Removed “add the certificate serial number to a CRL” for compromised OCSP responders. |
| 5.8 CA or RA Termination | Added in regards to Symantec SSP CA termination:<br>“before all certificates have expired, the CA signing keys shall be surrendered to the FPKIPA.”<br><br>Added:<br>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 past.<br>After the final CRL has been issued, the private signing key of the SSP CA will be destroyed.<br><br>Note: This section does not apply to CAs that have ceased issuing new certificates but are continuing to issue CRLs until all certificates have expired. Such CAs are required to continue to conform with all relevant aspects of this policy (e.g., audit logging and archives).<br><br>Corrected reference to section 5.7.3 |
| 6.1.1.1 CA Key Pair Generation | Replaced “tokens” with “modules”.<br>Replaced “video taped” with “recorded.<br>Removed reference to specific model of crypto hardware.<br>Added:<br>The corresponding key ceremony documentation is reviewed by an independent third party on an annual basis. |
| 6.1.5 Key Sizes and Signature Algorithms | Removed Sha-1 references.<br>Added:<br>The key pairs for end entity certificates issued under id-fpki-common-devices and id-fpki-common-devicesHardware that expire after December 31, 2030 shall be at least 3072 bits for RSA or 256 bits for elliptic curve algorithms.<br><br>Added:<br>After December 31, 2030 asymmetric keys shall be at least 3072 bit for RSA or at least 256 bit for elliptic curve algorithms. |
| 6.2.1 Cryptographic Module Standards and Controls | Added “hardware” to the crypto module requirement for specified subscriber certificates.<br>Added “minimum” to the crypto module requirement for CA and CSA.<br>Removed reference to specific model of crypto hardware.<br>Added:<br>PIV Cards are PKI tokens that have private keys associated with certificates asserting id-fpki-common-authentication or id-fpki-common-cardAuth. PIV Cards shall only be issued using card stock that has been tested and approved by the FIPS 201 Evaluation Program and listed on the GSA Approved Products List (APL). On an annual basis, for each PCI configuration used (as defined by the FIPS 201 Evaluation Program), one |

| Section | Changes made |
|---|---|
| | populated, representative sample PIV Card shall be submitted to the FIPS 201 Evaluation Program for testing. |
| 6.2.2 Private key (n out of m) Multi-Person Control | Replaced "token" with "HSM" throughout this section.<br>Replaced "magnetic media" with "storage media". |
| 6.2.4.1 Backup of CA Private Signature Key | Changed total of copies maintained from "four (4)" to "five (5)".<br>Added:<br>Backup copies of the Symantec SSP CA key pair are usually made during the original key ceremony process using a secure process specifically designed for cloning of key pairs.<br><br>Removed the detailed description of cloning keys specific to only one type of HSM |
| 6.2.4.2 Backup of Subscriber Private Signature Key | Re-phrased the references to the policies that either allow or do not allow backups. |
| 6.2.6 Private Key Transfer Into or From a Cryptographic Module | Replaced "token" with "HSM" |
| 6.2.9 Method of Deactivating Private Key | Specified time out period to be "no greater than 5 minutes".<br>Added:<br>The department or agency shall implement technical or administrative controls to enforce this policy. |
| 6.2.10 Method of Destroying Private Key | Added "by individuals to trusted roles" in two places. |
| 6.4.1 Activation Data generation and Installation | Added "with an appropriate level of strength" to the password/PIN requirement for subscribers.<br>Removed reference to guidance provided during enrollment process for subscribers.<br>Added "with an appropriate level of strength" to the password/PIN requirement for RAs.<br>Removed reference to guidance provided during the enrollment process for RAs. |
| 6.7 Network Security Controls | Changed key size from 1024 to 2048 bit RSA.<br>Added "at a level of assurance commensurate with that of the CA." to remote workstation authentication. |
| 7.1.3 Algorithm Object Identifiers | Removed Sha-1 references |
| 7.1.4 Name Forms | Re-phrased the requirement for the subject alt name extension and added UUID encoded as a URI. |
| 7.1.6 Certificate Policy Object Identifier | Added:<br>Certificates that express the id-fpki-common-piv-contentSigning shall not express any other policy OIDs. |
| 7.2 CRL Profile | Removed Sha-1 references |
| 8.1 Frequency of Circumstances of Assessment | Updated link. |
| 9.1.4 Fees for Other Services | Removed that Symantec may charge a fee for OCSP access to certificate status information. |

| Section | Changes made |
|---|---|
| 9.2.3 Insurance or Warranty Coverage for End-Entities | Replaced "No stipulation" with:<br>The Symantec Federal SSP does not offer warranty protection |
| 9.3.1 Scope of Confidential Information | Replaced "No stipulation" with:<br>The following records of Subscribers shall, subject to Section 9.3.2, be kept confidential and private ("Confidential/Private Information"):<br>CA application records, whether approved or disapproved,<br>Certificate Application records,<br>Private keys held by Customers,<br>Transactional records (both full records and the audit trail of transactions),<br>Audit trail records created or retained by Symantec or a Customer,<br>Audit reports created by Symantec or a Customer (to the extent such reports are maintained), or their respective auditors (whether internal or public),<br>Contingency planning and disaster recovery plans, and<br>Security measures controlling the operations of Symantec hardware and software and the administration of Certificate services and designated enrollment services. |
| 9.3.2 Information Not Within the Scope of Confidential Information | Replaced "No stipulation" with:<br>Certificates, Certificate revocation and other status information, Symantec 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 | Replaced "No stipulation" with:<br>Symantec secures private information it receives from compromise and disclosure to third parties |
| 9.6.4 Subscriber Representations and Warranties | Added:<br>If the human sponsor for a device is not physically located near the sponsored device, and/or does not have sufficient administrative privileges on the sponsored device to protect the device's private key and ensure that the device's certificate is only used for authorized purposes, the device sponsor may delegate these responsibilities to an authorized administrator for the device. The delegation shall be documented and signed by both the device sponsor and the authorized administrator for the device. Delegation does not relieve the device sponsor of his or her accountability for these responsibilities. |
| 9.12.3 Circumstances under Which OID must be Changed | Replaced "No stipulation" with:<br>If the Symantec PMA 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 type of Certificate. Otherwise, amendments shall not require a change in Certificate policy object identifier. |

| **Version** | **Date / Status** | **Revision Details** |
|---|---|---|
| 2.2 | April 2020 | Changes to address FPKI Comments from 2019 Annual SSP NFI Review. |
| 2.1 | May 2018 | 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 | |
| 1.14 | | **Updates addressing Change Proposals:**<br>**Sections:** | **Description**: |
| | October 2012 | 1.3.1.2, 8.0-8.6, glossary | 2012-01 – updates for RA & CMS audits |
| | February 2012 | 1.3.5.2, 2.1, 2.4, 4.10, 9.4.1, 9.4.3 | 2011-03 – Removed LDAP services |
| | | 1.2, 3.1.1, 3.2.3.2, 3.3.1, 6.1.1.2, 6.2.1, 6.2.4.5, 6.2.6, 6.2.8, 7.1.4 | 2011-02 – Added policy for *id-fpki-common-devicesHardware* |
| | | 1.3.1.4 | 2011-01 – CAs assert policy OIDs in OCSP responder certs for which the OCSP responder is authoritative. |
| | | 5.3.2 | DMV check includes check for violations & 3 years of place of residence. |
| | | 6.1.7 | All certificates shall include a critical key usage extension. |
| | | 6.4.1 | Password rules for RAs & Subscribers provided during the enrollment process shall reflect strength commensurate with FIPS 140-2 Level 2. |
| | | Throughout the doc – administrative changes reflecting Symantec ownership, rebranded name of the PKI, new contact info & URLs. | |
| | 06 Jan 2011 | **Updates addressing Change Proposals:**<br>**Sections:** | **Description**: |
| | | 1.2, 1.4.1, 6.1.5, 7.2 | 2010-07 – SHA-1 OIDs & policies for continued use of the deprecated SHA-1 algorithm. |
| | | | 2010-06 – no changes. |
| | | 5.5.1 | 2010-05 – Added list of additional audited events identified by CP. |
| | | | 2010-04 – no changes needed. |
| | | 3.1.1.1 | 2010-03 – Added UUID as alternative value for serial number & *subjAltName*. |
| | | 6.5.1 & 6.7 | 2010-02 – Remote Admin requirements. |
| | | 6.1.5 | 2010-01 – -CA key pairs expiring after 12/31/2030 shall be either 3072 RSA or 256 ECC.<br>-all end entity certs are at least 2048 RSA<br>-TLS/SSL certs use 128-bit AES symmetric keys<br>-removed all transition timelines prior/up to Dec 31, 2010 (date is now passed). |
| | | 3.2.3.1 | 2009-02 – A sponsoring employee may present a valid PIV Auth certificate as proof of identity & employment. |
| | | | 2009-01 – no change. |
| | | | 2008-02 – no change. |
| | | 8.3 | 2008-01 – Added: the auditor is not allowed to have served in developing or maintaining the implementation or CPS docs. |
| | | 1.4.2 | Clarification of prohibited uses (as per Common Policy) |
| | | 2.2.1 | Changed availability as permitted by Common Policy. |
| | | 3.1.1.1 | Added use of generational qualifier as part of common name. |
| | 27 Dec 2010 | **Symantec maintenance updates**<br>**Sections:** | **Description**: |
| | | 2.1, 4.9.11, 9.2.2 | Corrected URLs |
| | | 2.2.2 | Provided URL for obtaining Common Policy instead of publishing it ourselves. |
| | | 3.1.3 | Clarification – no anonymous or pseudonymous names are permitted. |
| | | 3.2.2 & 3.2.5 | Clarification – Authentication for a CA certificate requires authentication of the Agency for which the CA is named. |
| | | 3.2.3.2 | Tighten security – upon changes in device sponsorship, the new sponsor shall review the status of the devices under their sponsorship to confirm their authorization for certificates. |

|  |  |  |  |
|---|---|---|---|
|  |  | 4.3.1 | Added “or other comparable certificate store”. |
|  |  | 4.1.1 & 4.3.2 | Clarification of who can submit certificate applications & how certificate generation is notified. |
|  |  | 4.5.1 & 4.5.2 | Clarification of certificate usage restrictions. |
|  |  | 4.7–4.7.6 | Clarification of certificate re-key.<br>-After re-key the old certificate may optionally be revoked but may not be further re-keyed, renewed or modified.<br>-a re-key request may be authenticated either electronically or in-person |
|  |  | 4.9.3 | Tighten the process for revocation:<br>-clarified the process for identifying the certificate to be revoked.<br>-upon departure of a subscriber, h/w tokens must be surrendered & zeroized. Any un-retrieved tokens must be immediately revoked as “key compromise”.<br>-clarified the TA’s process for authentication of a request.<br>-Added process (previously missing) for revocation request by a PKI Sponsor for revocation of a device cert. |
|  |  | 1.3.2.1, 3.4, 4.9.3, 5.2.1.5, 5.2.1.6 | Correction: The Agency (not VeriSign) performs the RA functions. |
|  |  | 4.9.7 & 4.9.8 | Changed CRL validity interval from 18 to 24-hours & clarified that the maximum latency for publishing is 4 hours. |
|  |  | 4.9.9 & 4.10 | -OCSP compliance changed from RFC 2560 to RFC 5019 (lightweight OCSP).<br>-clarification of the specific CA certificate that is used to sign the specific CRL. |
|  |  | 4.9.13 | Correction: only CA certificate suspension is not permitted. |
|  |  | 4.11 | End of subscription is synonymous with certificate validity period. |
|  |  | 4.12.1 & 4.12.2 | Added clarification language about Key escrow processes. |
|  |  | 5.1.2 | Correction to safes – removed “government-approved” & changed from 2 to 3 persons required for access. |
|  |  | 5.1.3 | Added UPS system with sufficient power to complete any pending actions following loss of all power. |
|  |  | 5.2.1.3 | Clarified IT Audit Manager trusted role to comply with Common Policy. |
|  |  | 5.2.2 & 5.2.4 | Added detail for dual-person controls & separation of duties to comply with Common Policy. |
|  |  | 5.3.2 | Clarified description of background checks performed – similar to DoD Industrial Secret & 7 yrs of history investigated (instead of Top Secret). |
|  |  | 5.3.3 | Removed the exact detail about the training programs. |
|  |  | 5.4.2 | -corrected the threshold for generating capacity alerts (warning at 70% & critical at 90%)<br>-added barcode labeling of tape media<br>-copy of audit logs is retained onsite for reviews |
|  |  | 5.4.1 & 5.4.3 | -clarified specific components generating audit log data<br>-the RA audit data collected by the CA is limited to RA interaction with the CA. |
|  |  | 5.4.8 | Added: audit data is checked for gaps in audit logs. |
|  |  | 5.5.2 & 5.5.7 | Added:<br>-barcode labeling of media & database for referencing archives<br>-testing of backup completeness & media viability<br>-restoration tested twice a year<br>-use of media & software app that survives the period of archive retention<br>Added description of accuracy of archived data:<br>-Veritas NetBackup obtains logs directly from OS via secure channel.<br>-capability to verify the integrity of data on tape & data being restored |
|  |  | 5.6 | Clarified: Re-key of CA requires generation of a new certificate & the old certificate is retained to issue CRLs for certificates signed by that old cert. |
|  |  | 5.7.2 | Clarified Disaster Recovery gives “priority to the generation of a new CA key pair”. |

|  |  |  |  |
|---|---|---|---|
|  |  | 5.8 | Clarified that notice shall be given prior to CA termination & continued support of issued certificates shall be performed in accordance with agreements. |
|  |  | 6.1.1.1 & 6.2.4.1 | -Clarified dual controls & witnessing of CA key generation ceremonies.<br>-Backup copies are created via secure cloning process during the key ceremony. |
|  |  | 6.1.6 | Public key parameters are generated in accordance with FIPS186. |
|  |  | 6.2.1 | Removed VeriSign smart card issuance system (not provided by VeriSign). |
|  |  | 6.2.2 | Changed from 12 to 16 shares. |
|  |  | 6.2.4.2 & 6.2.4.3 | Backup of Key Management (ie, Encryption) Private key is moved to new section (6.2.4.3). Signature keys are not escrowed but Encryption keys are. Storage of backup copies ensure security is consistent with the protection provided by the Subscriber's crypto module. |
|  |  | 6.3.2 | -Corrected: CA key pair usage period from 6 yrs to max of 10 yrs & generation period from 3 yrs to 4 yrs. Subscriber cert max usage is 3 yrs.<br>-Added: usage periods for certs asserting the PIV-contentSigning extension to max usage of 8 yrs for public keys & max of 3 yrs for private keys. |
|  |  | 6.6.2 | -Changed name of CBO to PKI Ops<br>-corrected delivery packaging from tamper-resistant to tamper-evident.<br>-corrected delivery services (removed 'registered mail & constant surveillance courier') |
|  |  | 6.7 | Added secure comms between the KMS & KMD & SSP |
|  |  | 7.1.3 | Added ECC algorithms |
|  |  | 7.1.5 | RAs are limited to the jurisdictional name space assigned |
|  |  | 8.1 | Added annual audit requirement for the Agency. |
|  |  | 9.1.1 | Correction: VeriSign is entitled to charge fees (but removed the statement that we publish our fees on our website). |
|  |  | 9.4.1, 9.4.3 | Added description of our privacy practices for compliance with policy |
|  |  | 9.6.2 | Added missing responsibility – the RA performs in-person identity verification |
|  |  | 9.6.4 | Added missing responsibility – the Subscriber shall prevent disclosure of their private keys & activation data. |
|  |  | 9.6.6.1 | Added missing responsibility – the PA shall provide notifications in the event of disaster, compromise or termination. |
|  |  | 9.10.1 & 9.10.3 | -the term of the CPS extends through the end of the archive period<br>-corrected section reference #'s of obligations that survive termination of the CA. |
|  |  | 9.13.2, 9.14 & 9.15 | Governing law & dispute resolution changed from Santa Clara CA to Virginia (in effect under the legacy owner, VeriSign – the next revision will correct this for the new owner, Symantec) |
|  |  | Appx B, C & D | Corrected definitions, acronyms & references as required |
| 1.13.1 | 12 Nov 2010 | Convert to RFC3647 sequence |  |
| 1.13.1 | 30 March 2010 | Maintenance updates: |  |
|  |  | **Sections:** | **Description**: |
|  |  | 1.1, 1.3.2.1, 1.3.5.2, 5.1.1, 5.7.1 | Updated location of Primary Facility from MV to Delaware & DRF from Virginia to CA. |
|  |  | 1.3.2.1 | RAs are no longer co-located with Primary site. |
|  |  | 5.1.1 | -Removed reference to Army regs 389-5<br>-Removed 'metal-clad construction' of perimeter doors. |
|  |  | 6.7 | -Changed security monitoring tools to: Bladelogic, security audit scripts, Qualys, Sourcefire, Win-based virus scanners.<br>-Changed firewall to: Checkpoint NGX-R55 and NGX-R62<br>-Changed primary IDS to: NS2000 and 3D2100 IDS appliances running OS version 4.8.02, with RNA enabled |
|  |  | 6.5.1 & 6.5.2 | -[Text Removed]<br>-Removed EAL-4 certification of the VeriSign CA |
| 1.13 | Ready for submission to EPMA Review after upcoming release of Common Policy |  |  |

| | | |
|---|---|---|
| | 12 Nov, 2009 – PWG Approval | This CPS replaces Version 1.12 dated March 10, 2008 to reflect the changes to the VeriSign PKI infrastructure resulting from planned evolution and internal compliance monitoring. |
| 1.12 | Mar 10, 2008 | This revision incorporates changes to comply with the U.S. Federal PKI Common Policy Framework modification 2007-02 dated 12 Sep 2007 and to address comments from a review of the CPS by the Federal Policy Authority and the external annual audit. |
| 1.1 | Feb 2, 2007 | This revision incorporates changes to comply with the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework Version 2.5, dated 16 Oct 2006 |
| 1.1 | Jul 19, 2006 | This CPS replaces version 1.0 dated June 30, 2004. Changes to this CPS are to align with the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework Version 2.4, dated 15 Feb 2006. These changes are required for compliance with NIST FIPS 201. |