Symantec Non-Federal Shared Service Provider PKI

Certification Practice Statement

A Symantec Trust Network CA

Version 2.0

September 15, 2017

(Portions of this document have been redacted.)

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043
+1 650.527.8000
www.symantec.com

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

Revision Date: September 15, 2017

Important – Acquisition Notice

On August 9, 2010, Symantec Corporation completed the acquisition of VeriSign Inc's Authentication division. As a result Symantec is now the registered owner of this Certificate Policy document and the PKI Services described within this document.

However a hybrid of references to both "VeriSign" and "Symantec" 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 as a corporate entity should be strictly considered to be legacy language that solely reflects the history of ownership.

Trademark Notices

Symantec Corporation.,
350 Ellis Street,
Mountain View, CA 94043 USA
Attn: Practices Development.
Tel: +1 650.527.8000
Fax: +1 650.527.8050
Email: ***practices@symantec.com***.

TABLE OF CONTENTS

1. INTRODUCTION

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

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

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

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

1.1 Overview

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

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

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

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

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

Authorized Symantec 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 State/Local government agencies or companies that purchase the Non-Federal SSP PKI services.

End-entities supported by the Non-Federal SSP PKI are State/Local employees, contractors and affiliates. The Non-Federal SSP PKI will issue X.509 Version 3 certificates compliant with the certificate profiles listed in Appendix A of this CPS. The certificates can be used by the subscribers and relying parties for both physical and logical access including use in a variety of applications such as secure electronic mail, signature of electronic forms and contract documents, secure document exchange, and secure web access and transmission.

1.1.1 Certificate Practices Statement (CPS)

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

This CPS describes a PKI for non-Federal entities which meets Federal information assurance levels and is cross certified with the FBCA to enable interoperability with Federal entities. This CPS describes the rights and obligations of persons and entities authorized under this CPS and the CP to fulfill any of the following roles: Certification Authority, Registration Authority, Trusted Agent, Repository, and the end-entity roles of Subscriber and Relying Party.

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

1.2 Document Name and Identification

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

STN Policy Object Identifiers	**Symantec Non-Federal SSP PKI Policy Object Identifiers:**
2.16.840.1.113733.1.7.23.1 STN Class 1	2.16.840.1.113733.1.7.23.1.1.2 SSP Rudimentary
2.16.840.1.113733.1.7.23.2 STN Class 2	2.16.840.1.113733.1.7.23.2.1.2 SSP Basic
2.16.840.1.113733.1.7.23.3 STN Class 3	2.16.840.1.113733.1.7.23.3.1.6 SSP Medium 2.16.840.1.113733.1.7.23.3.1.7 SSP MediumHardware 2.16.840.1.113733.1.7.23.3.1.8 SSP mediumDevices 2.16.840.1.113733.1.7.23.3.1.36 SSP mediumDevicesHardware 2.16.840.1.113733.1.7.23.3.1.13 SSP Auth (no longer issued, found in legacy certificates only) 2.16.840.1.113733.1.7.23.3.1.14 SSP Medium CBP 2.16.840.1.113733.1.7.23.3.1.15 SSP MediumHardware CBP 2.16.840.1.113733.1.7.23.3.1.17 SSP PIV-I cardAuth 2.16.840.1.113733.1.7.23.3.1.18 SSP PIV-I Hardware 2.16.840.1.113733.1.7.23.3.1.20 SSP PIV-I contentSigning

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

End-Entity certificates issued to devices after October 1, 2016 shall assert the *id-stn-ssp-mediumDevices*, *id-stn-ssp-mediumDevicesHardware,* or *id-stn-ssp-pivi-contentSigning* policy. All other policies defined in this document should be reserved for human subscribers when used in End-Entity certificates.

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

1.3 PKI Participants

1.3.1 PKI Authorities

1.3.1.1 Federal PKI Policy Authority (FPKIPA)

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

1.3.1.2 Symantec Policy Management Authority

The Symantec Trust Network Policy Management Authority (PMA) is responsible maintaining the CP, approving the CPS and Compliance Audit for each CA that issues certificates under the CP. The Symantec PMA is a management body responsible for maintaining this Symantec 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 FBCA CP regardless of by whom the PKI component is managed and operated.

1.3.1.3 Organization Policy Management Authority

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

An Organization PMA is responsible for ensuring that all organization operated PKI components (e.g., CMSs and RAs) are operated in compliance with this CPS and the FBCA Policy and shall serve as the liaison for that organization to the Symantec PMA.

1.3.1.4 Certification Authority (CA)

The Symantec Non-Federal SSP PKI is a complex PKI with three segments each chaining to a different Symantec Trust Network Root CA. Symantec has established a separate Non-Federal SSP Intermediate Certification Authority (CA) subordinate to each of the Symantec Class 1, Class 2 and Class 3 Public Certification Authority Root CAs. The Class 1 Intermediate CA is for issuing FBCA Rudimentary Assurance certificates; The Class 2 Intermediate CA is for issuing FBCA Basic Assurance certificates; and the Class 3 Intermediate CA is for issuing Medium and Medium-Hardware certificates.

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

The Non-Federal SSP Intermediate CAs issue certificates to SSP CAs hosted and operated by Symantec on behalf of organizations such as government agencies, contractors, universities and other Non-Federal entities. Each of the Non-Federal SSP Intermediate CAs will be cross-certified with the Federal Bridge Certification Authority CA at the appropriate assurance levels. Non-Federal SSP CAs are entities authorized by the FPKIPA to create, sign and issue end-entity digital certificates that conform to the requirements of the CP and this CPS. Note: No other PKI services provided by the Symantec Trust Network are permitted in the Non-Federal SSP PKI hierarchy.

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

1.3.1.5 Certificate Status Authority/Certificate Status Server

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

1.3.2 Registration

1.3.2.1 Registration Authority (RA)

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

RA personnel will be issued Symantec Class 3 administrator certificates to enable secure authenticated access to their organization's Non-Federal SSP CA. The RA certificate is stored on a FIPS 140 Level 2 hardware token. Persons holding roles on the PIV-I CMS will be issued a PIV-I Authentication certificate on a PIV-I smartcard to authenticate to the CMS. The CMS will be issued a PIV-I Content signing certificate to perform the signing functions on the PIV-I cards being issued.

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

1.3.2.2 Trusted Agent

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

1.3.3 Card Management System (CMS)

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

The CMS is issued Symantec Class 3 administrator certificates to enable secure authenticated access to their organization's Non-Federal SSP CA. The CMS is issued a PIV-I certificate that expresses the PIV-I Content Signing policy OID only and shall not be issued certificates that express the PIV-I Hardware or PIV-I Card Authentication.

1.3.4 Subscribers

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

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

1.3.5 Affiliated Organization

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

1.3.6 Relying Parties

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

1.3.7 Other Related Participants

1.3.7.1 Compliance Auditor

Symantec retains the services of an independent security auditing firm, (e.g. KPMG), which conducts a yearly examination of the controls associated with Symantec's operations as set forth in Symantec'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 Symantec 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 Symantec's compliance with the SSP CPS.

1.3.7.2 Repository

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

1.4 Certificate Usage

The sensitivity of the information processed or protected using certificates issued by the CA will vary significantly. Organizations must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each organization for each application and is not controlled by this CPS.

1.4.1 Appropriate Certificate Uses

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

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

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

1.4.2 Prohibited Certificate Uses

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

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

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

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

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

1.5 Policy Administration

1.5.1 Organization Administering the Document

The organization responsible for administering this CPS is the Symantec Practices Development group. Questions or correspondence related to this CPS should be addressed as follows:

Symantec Corporation
350 Ellis Road
Mountain View, CA 94043 USA
Attn: Practices Development – CPS
+1 650-527-8000 (voice)
+1-650-527-8050 (fax)
practices@symantec.com

1.5.2 Contact Person

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

1.5.3 Person Determining CPS Suitability for the Policy

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

1.5.4 CPS Approval Procedures

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

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

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

1.6 Definitions and Acronyms

See sections 11 and 12 for definitions and acronyms.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

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

2.1.1 Repository Obligations

The Symantec 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 Symantec SSP Repository. Therefore, the Symantec SSP Repository provides unrestricted read-only access to subscribers, relying parties, and other interested parties. The Symantec SSP repository is accessible via methods described in Section 2.1.

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

2.2 Publication of Certification Information

2.2.1 Publication of Certificates and Certificate Status

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

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

1. All CA certificates issued by or to the Symantec SSP CA;
2. All valid and un-expired Symantec SSP Certificates, except for Certificates that contain the UUID in the subject alternative name extension, such as PIV-I Authentication certificates and Card Authentication certificates, shall not be distributed via public repositories (e.g. LDAP);
3. Certificate status information, including revocation;
4. The most recently issued CRL;
5. SSP CA certificate(s) needed to validate the signature on Symantec SSP subscriber certificates; and
6. Any other relevant information the Symantec SSP considers relevant regarding the use of Symantec SSP certificates by its subscribers or relying parties.

2.2.2 Publication of CA Information

The Symantec document repository at *www.symantec.com/about/profile/policies/repository.jsp* contains or provides access to a copy of the Symantec Trust Network Certificate Policy and an abridged version of this CPS including at least the following topics:

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

Applicable updates to this CPS that affect Subscribers and relying parties will be posted on the Symantec corporate web site.

The Symantec SSP CPS is considered Symantec Proprietary information.

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 Symantec SSP.

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

Upon revoking a certificate, the SSP CA shall immediately change the status of the certificate indicated in the Symantec 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 Symantec 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 LDAP queries.

The Symantec 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 Symantec SSP repository shall be controlled via certificate-based access over SSL and shall be limited to authorized Symantec SSP personnel.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

Certificates issued by a SSP CA shall have a non-null DN name and shall use the X.500 DN name format for subject and issuer name fields. These distinguished names shall be in the form of an X.501 distinguished name specifying a geo-political name.

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

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

The organizational units department and agency appear when applicable and are used to specify the entity that employs the subscriber. At least one organizational unit must appear in the DN. Normally the organizational unit agency will only be applicable for State/Local government agencies.

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

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

In the first name form, nickname may be the subscriber's first name, a form of the first name, middle name, or pseudonym (e.g., Buck) by which the subscriber is generally known. A generational qualifier, such as "Sr." or "III", may be appended to any of the common name forms specified above. In the last form, dnQualifier is an integer value that may be added to any name, primarily used to ensure name uniqueness.

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

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

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

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

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

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

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

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

PIV-I Certificates

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

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

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

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

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

The PIV-I Authentication certificate shall include a non-null subjectAltName value.

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

- Affiliated: {*Base DN*}, ou=[*Affiliated Organization Name*], serialNumber=UUID
- Unaffiliated: {*Base DN*}, ou=[*Entity CA's Name*], ou=Unaffiliated, serialNumber=UUID

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

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

3.1.2 Need for Names to be Meaningful

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

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

cn=firstname initial. lastname

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

cn=CMS name.

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

serialNumber=UUID (see Practice note).

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

subjectAltname=UUID (see Practice Note).

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

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

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

cn=Organization CA-3.

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

3.1.3 Anonymity or Pseudonymity of Subscribers

The SSP CAs shall not issue anonymous or pseudonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Names

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

3.1.6 Recognition, Authentication, and Role of Trademarks

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

The Symantec PMA shall investigate and correct, if necessary, any name collisions brought to its attention. If appropriate, Organization PMAs shall resolve name collisions within their own space.

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

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

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

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

3.2.2 Authentication of Organization Identity

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

3.2.3 Authentication of Identity

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

3.2.3.1 Authentication of Human Subscribers

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

The RA shall ensure that the applicant's identity information is verified. For certificates issued under medium assurance, identity shall be established no more than 30 days before initial certificate issuance. RAs may accept notarized authentication of an applicant's identity to support identity proofing of remote applicants, assuming organization identity badging requirements are otherwise satisfied. Minimal procedures for RA authentication and notarized authentication of employees and affiliated personnel are detailed below.

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

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

2) Applicant's employment shall be verified through use of official organization records.

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

   i) Identity source documents are presented as follows:
      - For non-PIV-I credentials, the applicant presents one Federal government-issued photo ID, one REAL ID Act compliant picture ID[3] or two non-Federal forms of ID, one of which must be a photo ID (e.g. non-REAL ID Act compliant driver's license) as proof of identity. A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement;
      - For PIV-I credentials, the applicant presents two identity source documents in original form. The identity source documents must come from the list of acceptable documents included in *Form I-9, OMB No. 1115-0136, Employment Eligibility Verification*. At least one document shall be a valid State or Federal Government-issued picture identification (ID). For PIV-I credentials, an in-person antecedent is not permitted;

      and,

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

   iii) The credential presented in step 3) i) above shall be verified by the RA for currency and legitimacy (e.g., the organization ID is verified as valid). Typically this is accomplished by querying a database[4] maintained by the organization that issued the credential, but other equivalent methods may be used. Any credentials presented must be unexpired.

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

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

1) Verify that a request for certificate issuance to the applicant was submitted by an authorized sponsoring/Affiliated Organization employee. For PIV-I credentials, validation includes the authentication of organization identity as specified in section 3.2.2 and inclusion of the organization name within the subscriber DN.

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

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

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

[3] REAL ID Act compliant IDs are identified by the presence of the DHS REAL ID star.

[4] Databases or other sources that are used to confirm Subscriber attributes shall provide 1) an auditable chain of custody of information obtained, and 2) secure exchange of data in a confidential and tamper-evident manner, and 3) protection of data from unauthorized access.

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

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

   and,

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

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

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

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

- The identity of the person performing the identification;
- A signed declaration by that person that he or she verified the identity of the Applicant as required by the CPS using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury). The signature on the declaration may be either a handwritten or digital signature using a certificate that is of equal or higher level of assurance as the credential being issued;
- Unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- The date and time of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature or appropriate digital signature[5] using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury). Except for *id-stn-ssp-rudimentary* and *id-stn-ssp-basic* policies, this signature shall be performed in the presence of the person performing the identity authentication. The Subscriber shall also attest that he or she understands and acknowledges the obligations contained in the Subscriber Agreement including use and protection of the private key and the need to report suspicion of loss or compromise of the private key.

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

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 SSP RA either by first class postal mail, Federal Express or other similar means.

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

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

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

3.2.3.2 Authentication of Human Subscribers for Role-based Certificates

The Symantec SSP shall not issue certificates to a Subscriber identified by a role.

3.2.3.3 Authentication of Human Subscribers for Group Certificates

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

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

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

3.2.3.4 Authentication of Devices

The Symantec SSP CA may provide device component certificates (e.g., for card management systems, routers, firewalls, servers, etc.). Enrollment for the certificate must be performed by a human PKI Sponsor as described in Section 5.2.1.6. The PKI Sponsor is responsible for providing the RA, or approved Trusted Agent, correct information regarding:

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

For certificates issued at the *id-stn-ssp-mediumDevices* and *id-stn-ssp-mediumDevicesHardware* policies, registration shall be verified commensurate with the Medium assurance level. Acceptable methods include but are not limited to in person registration of the PKI Sponsor, with the identity of the PKI Sponsor confirmed in accordance with the requirements of Section 3.2.3 commensurate with the assurance level of the certificate requested. Alternatively, if the PKI Sponsor has a valid certificate issued by the SSP PKI, verification of the signature on a digitally signed message from the Sponsor is acceptable for identity authentication. In the case a human sponsor is changed, the new sponsor shall review the status of each device under his/her sponsorship to ensure it is still authorized to receive certificates.

3.2.4 Non-Verified Subscriber Information

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

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

3.2.5 Validation of Authority

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

3.2.6 Criteria for Interoperation

The Symantec SSP shall comply with the certificate and CRL profiles defined by the FPKIPA. The FPKIPA shall be responsible for all decisions to cross-certify the FBCA with an external PKI.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

The Symantec SSP supports re-key for Subscriber and CA certificates. If it has been less than six (6) years since a Subscriber was identified as required in Section 3.1, re-key requests for Subscriber certificates may be authenticated on the basis of existing subscriber certificates. A Subscriber, whose certificates have not expired and whose initial subscriber enrollment data has not changed, may re-key his or her certificates based on electronic authentication of a currently valid Signature and Encryption certificates. The SSP CA provides separate SSL-protected web pages for re-keying of Signature and Encryption certificates.

If the previous re-key authentication method was the same as original enrollment, then an alternate method may be used. Acceptable alternate methods are through proof of possession of the private key or through the use of a Challenge Phrase (or the equivalent thereof). During original enrollment, Subscribers choose and submit a Challenge Phrase (or the equivalent thereof). Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's reenrollment information, and

the enrollment information (including contact information) has not changed, a renewal Certificate is automatically issued.

The SSP CA may issue Subscriber certificates with a maximum of three (3) year lifetime. If more than six (6) years have passed since a Subscriber's identity was authenticated as specified in Section 3.1, a Subscriber certificate re-key shall follow the same procedures as initial certificate issuance.

3.3.2 Identification and Authentication for Re-Key After Revocation

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

3.4 Identification and Authentication for Revocation Request

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

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

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

A Trusted Agent may request revocation of an affiliated Subscriber's certificate by sending a digitally signed e-mail message to Symantec. The Organization 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 organization.

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

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

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Submission of Certificate Application

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

4.1.2 Enrolment Process and Responsibilities

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

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

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

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

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Hardware Credential

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

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

3) Public/private key pairs for authentication certificates are generated on the smart card 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 Appendix A. The certificate signing request is submitted over an SSL session to the SSP CA, which checks for proof of possession of the private key.

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

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

Software Credential

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

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

4.2.2 Approval or Rejection of Certificate Applications

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

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

4.2.3 Time to Process Certificate Applications

Symantec begins processing certificate applications within a reasonable time of receipt. There is no time stipulation to complete the processing of an application unless otherwise indicated in the relevant Subscriber Agreement, CPS or other Agreement between STN participants. A certificate application remains active until rejected.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

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

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

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

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

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

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

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Hardware Credential
The Subscriber signs a statement declaring that he/she has read the Subscriber Agreement and understands and 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. After the Subscriber's certificates are downloaded to the smart card, the Subscriber takes possession of the smart card and signs a receipt. For acceptance of a PIV-I Card, the RA shall activate and release the PIV-I Card to the subscriber only after a successful 1:1 biometric match of the applicant against the biometrics collected in Section 3.2.3.1.

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

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

4.4.2 Publication of the Certificate by the CA

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

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

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

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

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

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

Symantec 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. Certification modification means creating a new certificate with the same key as the old one, but with a new name or authorization. The Symantec SSP does not implement certificate renewal or modification for Subscriber certificates. Modification of SSP CA certificates is permitted after the SSP RA verifies proof of any subject information changes. Following renewal or modification, the old renewed or modified CA certificate may not be further renewed, re-keyed, or modified. SSP CAs may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the Subscriber name and attributes are unchanged.

In the event of a CA compromise, Subscribers shall be required to repeat the initial certificate application process.

4.7 Certificate Re-Key

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

4.7.1 Circumstances for Certificate Re-Key

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

4.7.2 Who May Request Certification of a New Public Key

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

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.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

See section 4.4.1.

4.7.6 Publication of the Re-Keyed Certificate by the CA

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

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

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

4.8 Certificate Modification

The Symantec SSP does not implement certificate update 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.

When the SSP CA updates its private signature key and thus generates a new public key, it shall notify by e-mail all CAs, RAs and Subscribers that rely on the CA's certificate that it has been changed and shall provide instructions for how to obtain and validate the updated SSP CA certificate. The old SSP CA certificate shall not be further re-keyed or updated.

4.9 Certificate Revocation and Suspension

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

4.9.1 Circumstances for Revocation

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

- Identifying information including the organizational affiliation in the Subscriber's certificate changes, affiliation is terminated, or the organization no longer authorizes the affiliation before the certificate expires;
- Privilege attributes asserted in the Subscriber's certificate are reduced;
- The certificate subject can be shown to have violated the requirements of this CPS or the subscriber agreement;
- The private key is suspected of compromise, e.g. due to loss or theft;

- The subscriber fails to sign the declaration of identity during registration in accordance with section 3.2.3.1;
- The subscriber or other authorized party asks for his/her certificate to be revoked; or
- The continued use of the certificate may be harmful to the Non-Federal SSP PKI.

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

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

4.9.2 Who Can Request Revocation

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

4.9.3 Procedure for Revocation Request

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

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

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

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

Certificate Revocation Request by Trusted Agent: A Trusted Agent may request revocation of a Subscriber's certificate by sending a digitally signed message to the Organization RA. The TA shall receive a request from a

Subscriber uniquely identifying the Subscriber whose certificate(s) is to be revoked and the reason for the revocation. The TA shall authenticate the Subscriber's request for revocation either by validating the Subscriber's signature on a digitally signed-e-mail, by validating the Subscriber's identity in person, or by consulting an appropriate entity in the Subscriber's organization.

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

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

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

4.9.4 Revocation Request Grace Period

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

4.9.5 Time within Which CA Must Process the Revocation Request

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

Revocation requests received within two hours of CRL issuance shall be processed before the next CRL is published.

4.9.6 Revocation Checking Requirement for Relying Parties

The Symantec 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 (If Applicable)

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

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

Symantec Root CAs are operated offline and are used only for issuing certificates to other CAs and signing CRLs. CRLs for offline CAs shall be published every 30 days.

4.9.8 Maximum Latency for CRLs

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

4.9.9 On-Line Revocation/Status Checking Availability

The Symantec SSP will provide an online CSA to enable certificate status checking using the Online Certificate Status Protocol (OCSP compliant with RFC 5019). The OCSP responder certificate will be issued on a FIPS 140 Level 3 hardware token. The OCSP responder certificate is signed by the same CA using the same key that signed the certificates whose status is to be checked. The OCSP responder shall ensure that accurate and up-to-date information is provided in the revocation status response and shall digitally sign all responses. Distribution of OCSP status information will meet or exceed the CRL issuance requirements specified in section 4.9.7.

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

4.9.10 On-line Revocation Checking Requirements

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

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

4.9.11 Other Forms of Revocation Advertisements Available

The Symantec SSP will also provide a Web page protected with a Symantec Class 3 service certificate at which relying parties may query the revocation status of a subscriber certificate. Certificate status information will meet or exceed the CRL issuance requirements specified in section 4.9.7.

4.9.12 Special Requirements Regarding Key Compromise

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

Subscriber key compromise is described in section 4.9.7.

4.9.13 Circumstances for Suspension

For CA certificates, suspension is not permitted. For end-entity certificates, suspension is not supported.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

SSP CAs provide certificate status services via OCSP, via CRLs accessible by HTTP, and optionally by direct LDAP query of the online repository. See sections 4.9.7 to 4.9.11 inclusive.

4.11 End of Subscription

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

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

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

Escrowed keys shall be protected at no less than the level of security in which they are generated, delivered, and protected by the subscriber. Recovery of the private encryption key is under dual-person control. The methods, procedures and controls which apply to the storage, request for, extraction and/or retrieval, delivery, protections and destruction of the requested copy of an escrowed SSP Subscriber private encryption key are described in the Symantec SSP Key Recovery Practices Statement (KRPS).

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

The Non-Federal SSP PKI does not support session key encapsulation and recovery.

5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 Physical Controls

The Symantec SSP equipment is dedicated to CA functions and does not perform non-CA related functions.

5.2 Procedural Controls

5.2.1 Trusted Roles

All employees, contractors, and consultants of the Symantec 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.

5.2.1.2 Officer

The Officer role as defined in the CP is fulfilled by the following entities for the Symantec SSP:

The *Symantec SSP RA* is responsible for validating subscriber identity and processing subscriber certificate enrollment requests. The SSP RA approves certificate enrollment requests, processes certificate revocation requests and also assists Subscribers during the enrollment process (as required). All persons filling the *Symantec SSP RA* role shall be US citizens.

An *Organization RA* is a representative of an organization that has entered into a contract with Symantec for SSP PKI services. The Organization RA performs the equivalent functions of the Symantec SSP RA. The Organization RA has a secure, remote interface to the SSP CA. All communications between the Organization RA and the SSP CA are via an SSL session with certificate-based access control. The Organization RA certificate is stored on a FIPS 140 Level 2 hardware token. Organization RA personnel for Federal Agency PKIs must be US citizens. Organization RA personnel for other organization PKIs may be citizens of the country where the RA is located.

5.2.1.5 Trusted Agent

A *Trusted Agent* is a person authorized to act as a representative of the SSP RA in providing Subscriber identity verification during the registration process. Trusted Agents do not have automated interfaces with the SSP CA. Trusted Agents for Federal Agency PKIs must be US citizens. Trusted Agents for other organization PKIs may be citizens of the country where the RA they are representing is located.

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 identify 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 9.6.3, and that Subscribers are informed of the consequences of not complying with those obligations.

5.2.1.6 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 SSP 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.

5.3 Personnel Controls

5.3.1 Qualifications, Experience and Clearance Requirements

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

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

Personnel appointed to operate CMA equipment shall:

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

5.3.3 Training Requirements

Operations personnel are sufficiently trained prior to performing independent, unattended duties.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Symantec SSP equipment will record events for the CA, RAs and the CSA.

5.4.7 Notification to Event-Causing Subject

No notification is provided to an event-causing subject.

5.4.8 Vulnerability Assessments

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

Symantec conducts quarterly vulnerability assessments to determine its ability to protect against external network threats. Symantec personnel, in addition to external consultants, perform this routine assessment. Finally, Symantec undergoes a yearly extensive SOC 2 security audit and 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 Symantec SSP audit process records the following information, in either paper or electronic record format, upon initialization of a CA key pair:

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

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

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

5.5.2 Retention Period for Archive

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

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

5.6 Key Changeover

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

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Symantec has created and maintains business continuity plans so that in the event of a business disruption, critical business functions may be resumed. Symantec maintains a Disaster Recovery Facility (DRF) located at a Symantec-owned 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 Symantec's security standards.

5.8 CA or RA Termination

In the event of termination of the SSP CA, notice shall be provided to all Subscribers and any cross-certified CAs prior to termination. Any actions needed to ensure continued support for certificates issued by the SSP CA shall be taken in accordance with agreements with the cross-certified CAs. All certificates signed by the SSP CA will be revoked. The SSP Cryptographic Device Manager, when informed of SSP CA termination, shall initiate the issuance of a final long term CRL with a nextUpdate time past the validity period of all issued certificates. This final CRL shall be available for all relying parties until the validity period of all issued certificates has past. After the final CRL has been issued, the private signing key of the SSP CA will be destroyed. Dissemination of revocation notice will be achieved as discussed in CPS section 5.7.2.

In the event of termination of an SSP RA, the RA certificate shall be revoked and the RA shall provide all archived data to the archival facility specified by Symantec.

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 Symantec's secure Key Ceremony room on hardware tokens. The ceremony is recorded and a full audit record is created to ensure that all security requirements, including separation of roles were followed.

6.1.1.2 Subscriber Key Pair Generation

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

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

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

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

The PIV-I Content Signing certificate and corresponding private key shall be maintained within a cryptographic module that meets the requirements of a PIV-I Card as described in Appendix C and managed within a trusted CMS as described in Appendix B.

6.1.2 Private Key Delivery to Subscriber

Subscriber private keys are delivered as follows:

Hardware Credential

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

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

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

Software Credential

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

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

6.1.2.1 Acknowledgement of Private Key Delivery

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

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

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

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

6.1.3 Public Key Delivery to Certificate Issuer

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

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

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

6.1.4 CA Public Key Delivery to Relying Parties

The Root CA Certificates and the Symantec Non-Federal SSP CA certificates shall be delivered to users and relying parties by downloading the certificates from a web site secured with a Symantec Class 3 web server certificate. Subscribers will be required to compare the STN Root CA Certificate hash against the hash value received from a Trusted Agent, Symantec RA or Organization RA. Alternatively, these certificates may be imported onto the Subscriber smart card at the time of certificate enrollment by the Organization RA.

6.1.5 Key Sizes

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

- The key pairs for the SSP CAs, which are the Symantec STN Class 1, Class 2 and Class 3 Root CAs, that expire before 12/31/2030 are 2048-bit RSA key pairs and those that expire after 12/31/2030 shall be at least 3072 bit RSA or 256 bits for elliptic curve algorithms.
- The key pairs for the Symantec Non-Federal SSP CAs, including the Symantec Non-Federal SSP Intermediate CAs and the Non-Federal Entity SSP CAs that expire before 12/31/2030 are 2048-bit RSA key pairs and those that expire after 12/31/2030 shall be at least 3072 bit RSA or 256 bits for elliptic curve algorithms.
- The key pairs for all end entity certificates are at least 2048-bit RSA key pairs.
- All Symantec Non-Federal SSP CAs, including the Symantec Non-Federal SSP Intermediate CAs and the Non-Federal Entity SSP CAs shall use SHA-256 for digital signature. Signatures on certificates and CRLs shall be generated using SHA-256.
- SSP CA-issued Transport Layer Security (TLS) or Secure Socket Layer (SSL) certificates use AES (128 bits) for symmetric keys and 2048 bit RSA for asymmetric keys.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters

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

Parameter Quality Checking
Public key parameters for signature algorithms defined in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186. Parameter checking (including primarily testing for prime numbers) shall be performed in accordance with FIPS 186-2.

6.1.7 Key Usage Purposes (as per x509v3 field)

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

Domain controller certificates are the only certificates enabled with both signing and encryption functionality.

Subscriber certificates that assert *id-stn-ssp-rudimentary* are single key and shall assert only the *digitalSignature* bit.

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

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

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

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

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

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

Public keys that are bound into device certificates shall be 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 shall assert the *keyEncipherment* bit. Device certificates shall not assert the *nonRepudiation* bit.

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.

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

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

PIV-I Cards are PKI tokens that have private keys associated with certificates asserting the *stn-ssp-pivi-hardware* or *stn-ssp-pivi-cardAuth* policy. PIV-I Cards shall only be issued using card stock that has been tested and approved by the FIPS 201 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 populated, representative sample PIV-I Card shall be submitted by the RA to the FIPS 201 Evaluation Program for testing.

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

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

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

All cryptographic modules dedicated to management of Symantec 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 Symantec or an Organization RA, is physically separated from the SSP CA.

6.2.1.1 Custodial Subscriber Key Stores

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

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

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

6.2.3 Private Key Escrow

6.2.3.1 Escrow of CA private signature key

CA private keys are not escrowed.

6.2.3.2 Escrow of CA encryption keys

CA private keys are not escrowed.

6.2.3.3 Escrow of Subscriber private signature keys

Subscriber private signature keys are not escrowed.

6.2.3.4 Escrow of Subscriber Private Encryption and Dual Use Keys

The Symantec SSP provides key escrow and key recovery services for Symantec SSP Subscriber private encryption keys.

6.2.4 Private Key Backup

6.2.4.1 Backup of Entity CA Private Signature Key

Backup copies of the SSP CA and CSA private keys are made to facilitate disaster recovery.

6.2.4.2 Backup of Subscriber Private Signature Key

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

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

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

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

6.2.4.3 Backup of Subscriber Key Management Private Key

Symantec SSP subscribers are obligated to prevent unauthorized disclosure of their private keys. This includes any means undertaken to establish a backup copy of their keys in support of disaster recovery ensuring security

controls consistent with the protection provided by the subscriber's cryptographic module. Backup private key management keys shall not be stored in plain text form outside the cryptographic module.

6.2.4.4 Backup of CSS Private Key

See 6.2.4.1.

6.2.4.5 Backup of PIV-I Content Signing Key

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

6.2.4.6 Backup of Device Private Keys

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

6.2.5 Private Key Archival

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

6.2.6 Private Key Transfer Into or From a Cryptographic Module

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

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

6.2.7 Private Key Storage on Cryptographic Module

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

6.2.8 Method of Activating Private Keys

The SSP CA and CSA hardware tokens utilize a PIN-based activation mechanism.

Symantec SSP subscribers are obligated to select a password or PIN during key generation. Entry of the password or PIN is required to activate the private key whose corresponding public key is contained in a certificate asserting the *id-stn-ssp-medium*, or *id-stn-ssp-mediumHardware* policy object identifier. The subscriber is the only entity that knows the password; at no time does the Symantec 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.

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

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

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

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

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

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

6.2.9 Method of Deactivating Private Keys

The SSP CA and CSA hardware tokens are operated in a 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 or by removing them from the smart card reader.

6.2.10 Method of Destroying Private Keys

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

6.2.11 Cryptographic Module Rating

See section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

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

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

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

PIV-I Cards shall have an expiration date not to exceed 5 years of issuance. PIV-I Subscriber certificate expiration shall not be later than the expiration date of the PIV-I hardware token on which the certificates reside. Expiration of the PIV-I Card shall not be later than expiration of PIV-I Content Signing certificate residing on the card.

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

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

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

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

6.4.2 Activation Data Protection

The SSP CA and CSA activation data PINs are split into 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.

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

6.4.3 Other Aspects of Activation Data

See Section 6.4.1.

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

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

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 Symantec systems development and change management procedures.

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

6.6.2 Security Management Controls

Equipment (hardware and software) procured to operate the Symantec CA, RA and CSA is purchased in a fashion to reduce the likelihood that any particular component was tampered with, such as random selection.

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 Symantec SSP is designed to mitigate risk to external threats.

7. CERTIFICATE, CRL AND OCSP PROFILES

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

7.1 Certificate Profile

7.1.1 Version Number(s)

SSP shall issue X.509 Version 3 certificates only.

7.1.2 Certificate Extensions

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

7.1.3 Algorithm Object Identifiers

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

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

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

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

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

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

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

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

7.1.4 Name Forms

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

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

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

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

7.1.5 Name Constraints

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

7.1.6 Certificate Policy Object Identifier

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

7.1.7 Usage of Policy Constraints Extension

The Symantec SSP does not enforce policy constraints.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued by the Symantec 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.

7.2 CRL Profile

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

7.2.1 Version Number(s)

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

7.2.2 CRL and CRL Entry Extensions

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

7.3 OCSP Profile

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

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

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

8.1 Frequency or Circumstances of Compliance Audit

The SSP CA, CSA and RA shall undergo an annual compliance audit as part of the Symantec annual PKI audit. The organization RA and CMS shall undergo an annual compliance audit. Compliance audits shall be conducted in accordance with the *Compliance Audit Requirements* document located at http://www.idmanagement.gov/fpki-documents

8.2 Identity/Qualifications of Reviewer

The Symantec SSP auditor is the same professional auditing firm responsible for conducting Symantec's commercial PKI audit. The Symantec SSP auditor is intimately familiar with Symantec's practices and policies, as it has been performing these services for Symantec for more than five years. The auditing team has extensive experience in all relevant matters of physical, personnel, technical, and logical security. Specifically, the compliance audit team has the following applicable experience:

- a minimum of 5 year experience performing security audits;
- a minimum of 3 year PKI engineering/design experience;
- a minimum of 6 years cryptography engineering experience; and
- a minimum of 6 years computer security experience.

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

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

8.3 Assessor's Relationship to Audited Party

The Symantec SSP auditor is under a contractual relationship to Symantec for its security audit services and has no role or responsibility relating to the Symantec SSP operation. The Organization RA and/or CMS auditor shall be an independent organization[6] engaged under a contractual relationship for audit services and may not have any other role or responsibility relating to the organization's SSP operation..

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

8.4 Topics Covered by Compliance Audit

The Compliance Audit shall verify that Symantec 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 Symantec or the organization CA/RA/CMS operations shall be subject to compliance audit inspections.

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

8.5 Actions Taken as a Result of Deficiency

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

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

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

8.6 Communication of Results

The Symantec SSP compliance auditor shall report the results of a compliance audit to Symantec and supply a signed Auditor Letter of Compliance addressed to the Symantec SSP PKI PMA. The organization RA and/or CMS compliance auditor shall report the results of a compliance audit to the organization and supply a signed Auditor Letter of Compliance addressed to the Symantec SSP PKI PMA. The organization shall supply the signed Auditor Letter of Compliance to the Symantec PKI PMA. Additionally, on request from the FPKI PA, the organization shall supply the full audit results report.

On an annual basis, the Symantec PMA shall submit an audit compliance package to the FPKIPA. This package shall be prepared in accordance with the *Compliance Audit Requirements* document and shall include Multiple Auditor Letters of Compliance, signed by their respective auditors, covering the Principal CA and all PKI components and functions under the overall responsibility of the Entity PKI PMA, including those that are separately managed and operated. This package shall include an assertion from the Symantec PMA 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

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

9.1.2 Certificate Access Fees

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

9.1.3 Revocation or Status Information Access Fees

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

9.1.4 Fees for Other Services

The Symantec SSP may charge a fee for key recovery services. The Symantec SSP may charge a fee for OCSP access to certificate status information.

9.1.5 Refund Policy

The Symantec 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 Symantec 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 Symantec revoke the certificate and provide a refund if Symantec 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 Symantec's refund policy at *www.symantec.com/about/profile/policies/repository.jsp*. This refund policy is not an exclusive remedy and does not limit other remedies that may be available to Subscribers.

9.2 Financial Responsibility

Symantec 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. Symantec also maintains professional liability insurance.

9.2.1 Insurance Coverage

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

9.2.2 Other Assets

An annual report of Symantec can be obtained by submitting a written request to the address specified in section 1.4. Symantec's financial resources are set forth in disclosures appearing at: *http://investor.symantec.com/phoenix.zhtml?c=89422&p=irol-irhome*.

9.2.3 Insurance or Warranty Coverage for End-Entities

The Symantec non-federal SSP does not offer warranty protection.

9.3 Confidentiality of Business Information

Information deemed confidential is protected in accordance with section 9.4.

9.3.1 Scope of Confidential Information

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

- CA application records, whether approved or disapproved,
- Certificate Application records,
- Private keys held by Customers,
- Transactional records (both full records and the audit trail of transactions),
- Audit trail records created or retained by Symantec or a Customer,
- Audit reports created by Symantec 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 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

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

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

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

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

9.4.2 Information Treated as Private

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

9.4.3 Information Not Deemed Private

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

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

9.4.4 Responsibility to Protect Private Information

Symantec 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. Symantec shall not release or be required to release any confidential information without an authenticated, reasonably specific request prior to such release.

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

9.4.5 Notice and Consent to Use Private Information

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

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

All disclosure shall be pursuant to applicable laws.

9.4.7 Other Information Disclosure Circumstances

All disclosure shall be pursuant to applicable laws.

9.5 Intellectual Property Rights

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

- Certificates and CRLs: Certificates and CRLs are the personal property of the Symantec SSP. Symantec licenses relying parties to use certificates and CRLs.
- CPS: This CPS is personal property of Symantec Corporation.
- 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.
- Symantec Private Keys: Symantec SSP CA private keys are the personal property of Symantec Corporation.

- Symantec Public Keys: Symantec SSP CA public keys are the property of Symantec Corporation. Symantec 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

Symantec warrants to Subscribers that:

- There are no material misrepresentations of fact in such Certificate known to or originating from Symantec;
- There are no errors in the information in the Certificate that were introduced by Symantec 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.

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

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

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

- Providing to the FPKIPA a CPS, as well as any subsequent changes, for conformance assessment;
- Maintaining its operations in conformance to the stipulations of the approved CPS;
- Ensuring that registration information is accepted only from approved RAs operating under an approved CPS;
- Including only valid and appropriate information in certificates, and maintaining evidence that due diligence was exercised in validating the information contained in the certificates;
- Revoking the certificates of Subscribers found to have acted in a manner counter to their obligations in accordance with Section 9.6.3; and
- Operating or providing for the services of an online repository that satisfies the obligations under Section 2.1.1, and informing the repository service provider of their obligations if applicable.

Each SSP CA shall comply with the following requirements:

- For PIV-I credentials issued for Affiliated Organizations, the SSP CA shall maintain an agreement with the Affiliated Organization concerning the obligations pertaining to authorizing the affiliation with subscribers of PIV-I certificates.

- Upon termination of an affiliation relationship, the SSP CA shall revoke all certificates affiliated with that organization.

9.6.2 RA Representations and Warranties

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

- Performing in-person identify verification of certificate applicants in accordance with Section 3.2.3;
- Maintaining its operations in conformance to the stipulations of the approved CPS;
- Including only valid and appropriate information in certificate requests, and maintaining evidence that due diligence was exercised in validating the information contained in the certificate; and
- Ensuring that obligations are imposed on subscribers in accordance with Section 9.6.3, and that Subscribers are informed of the consequences of not complying with those obligations.

9.6.3 Subscriber Representations and Warranties

By accepting a SSP certificate issued by Symantec, the Subscriber certifies to and agrees with Symantec 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 Symantec 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 Symantec of any material inaccuracies in such information as set forth in CPS § 2.3.1;
- the certificate is being used exclusively for authorized and legal purposes, consistent with this CPS; and
- the Subscriber is an end-user and will not use the private key corresponding to any public key listed in the certificate for purposes of signing any certificate (or any other format of certified public key) or CRL.

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

- Notify the Symantec 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;
- Agree not to monitor, interfere with, or reverse engineer the technical implementation of the Symantec SSP except as explicitly permitted by this CPS or upon written approval by Symantec; and
- Agree not to submit to Symantec or the Symantec repository any materials that contains statements that are (i) libelous, defamatory, obscene, pornographic, abusive, bigoted, hateful, or racially offensive, (ii) advocate illegal activity or discuss illegal activities with the intent to commit them, or (iii) otherwise violate any law.

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

9.6.4 Relying Party Representations and Warranties

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

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

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

9.6.5 Representations and Warranties of Other Participants

9.6.5.1 Symantec PMA Obligations

The Symantec PMA shall –

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

9.6.5.2 Organization PMA Obligations

The Organization PMA shall—

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

9.6.5.3 Affiliated Organization Obligations

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

9.7 Disclaimers of Warranties

9.7.1 Specific Disclaimers

Except as otherwise set forth in this CPS, Symantec:

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 Symantec's liability in tort for negligent, reckless, or fraudulent conduct;

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

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

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

9.7.2 General Disclaimer

Except as set forth in this CPS and the applicable subscriber agreement, and to the extent permitted by applicable law, Symantec 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 Symantec that constitute or may be held to constitute strict liability, whether sole or jointly with any other person or entity.

9.7.3 Disclaimer of Fiduciary Relationships

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

9.8 Limitations of Liability

9.8.1 Limitations on Amount of Damages

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

The total liability of Symantec to any party for general contract, tort or any other damages for negligent, reckless, or fraudulent conduct by the Symantec CAs, its RAs or Trusted Agents in connection with a single transaction involving the use or reliance on a Non-Federal SSP certificate shall be limited to one hundred dollars ($100) for a Class 1 certificate, five thousand dollars ($5,000 USD) for a Class 2 certificate and ten thousand dollars ($10,000) for a Class 3 certificate. Furthermore, Symantec's total liability for any incident (aggregate of all transactions) involving the use or reliance on a certificate shall be limited to one hundred thousand ($100,000

USD). These liability caps shall be the same regardless of the number of digital signatures, acts of authentication, or encrypted messages related to, or claims arising out of such transaction.

Notwithstanding the foregoing, to the extent Symantec has issued and managed the Certificate(s) at issue in compliance with its Certification Practice Statement, Symantec 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, Symantec 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 Symantec has been advised of the possibility of such damages.

To the extent permitted by applicable law, Symantec 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 Symantec 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 Symantec 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 Symantec or any person receiving or relying on the certificate; or (iii) failure to protect the Subscriber's private key, to use a trustworthy system, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key.

9.10 Term and Termination

9.10.1 Term

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

9.10.2 Termination

See section 4.9.

9.10.3 Effect of Termination and Survival

Each SSP CA shall comply with the following requirements.

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

9.11 Individual Notices and Communications with Participants

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

To Symantec:

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043 USA
Attn: Certification Services
(+1 650-527-8000)

By Symantec to another person:

To the most recent address of record to another person on file with Symantec Corporation.

9.12 Amendments

9.12.1 Procedure for Amendment

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

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

9.12.2 Notification Mechanism and Period

Upon approval of a CPS modification by the FPKIPA, an updated version of this document will be provided to the FPKIPA.

9.12.3 Circumstances under Which OID must be Changed

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 Class of Certificate. Otherwise, amendments shall not require a change in Certificate policy object identifier.

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 policy. .
Symantec shall investigate and correct if necessary any name collisions brought to its attention. If appropriate,

Symantec shall coordinate with and defer to the EPMA naming authority.

Disputes among Symantec 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 Symantec require an initial negotiation period of sixty (60) days followed by litigation in the federal or state court encompassing Santa Clara County, California, 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 Symantec.

9.14 Governing Law

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

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

9.15 Compliance with Applicable Law

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

9.15.1 Compliance with Export Laws and Regulations

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Not applicable.

9.16.2 Assignment

This CPS inures to the benefit of, and shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties. The rights and obligations detailed in this CPS are assignable by the parties, by operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with CPS § 4.9, concerning termination or cessation of CA operations; and provided further, that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

9.16.3 Severability

If any provision of this CPS, or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this CPS (and the application of the invalid or unenforceable provision to other

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

9.16.4 Merger

No term or provision of this CPS directly affecting the respective rights and obligations of Symantec 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 Symantec) 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

Symantec 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 Symantec Trust Network CP and this CPS, the Symantec Trust Network 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.

10. REFERENCES

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

Number	Title	Revision	Date
ABADSG	*Digital Signature Guidelines* http://www.abanet.org/scitech/ec/isc/dsgfree.html		1 August 1996
FPKI-E	*Federal PKI Version 1 Technical Specifications: Part E-X.509 Certificate and CRL Extensions Profile*		*7 July 1997*
FPKI-PROF	*Federal PKI X.509 Certificate and CRL Extensions Profile* http://www.idmanagement.gov/fpki-documents		
E-Auth	*E-Authentication Guidance for Federal Agencies, M-04-04*		16 Dec 2003
FIPS140	*Security Requirements for Cryptographic Modules* http://csrc.nist.gov/publications/index.html		21 May 2001
FIPS112	*Password Usage* http://csrc.nist.gov/		5 May 1985
FIPS186-2	*Digital Signature Standard http://www.itl.nist.gov/fipspubs/fip186.htm*		27 January 2000
FIPS201-1	*Personal Identity Verification (PIV) of Federal Employees and Contractors* http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf		March 2006
FOIAACT	*5 U.S.C. 552, Freedom of Information Act* http://www4.law.cornell.edu/uscode/5/552.html		
NIST SP 800-73	Interfaces for Personal Identity Verification (4 Parts) http://csrc.nist.gov/publications/PubsSPs.html		
NIST SP 800-76	Biometric Data Specification for Personal Identity Verification http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf		
NIST SP 800-78	Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV) http://csrc.nist.gov/publications/nistpubs/800-78-2/sp800-78-2.pdf		
NS4009	*NSTISSI 4009, National Information Systems Security Glossary*		January 1999
PACS	*Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems* http://www.idmanagement.gov/fpki-documents	2.2	30 July 2004
PIV-I Profile	X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards, April 23, 2010, http://www.idmanagement.gov/fpki-documents		April 23, 2010
PKCS-1	*PKCS #1 v2.1: RSA Cryptography Standard* http://www.rsasecurity.com/rsalabs/node.asp?id=2125	2.1	14 June 2002
PKCS-12	*Personal Information Exchange Syntax Standard* http://www.rsasecurity.com/rsalabs/node.asp?id=2138	1.0	24 June 1999
SSPKRPS	*Key Recovery Practices Statement for Symantec SSP PKI Service*		
RFC3647	*Certificate Policy and Certification Practices Framework,* Chokhani and Ford http://www.ietf.org/rfc/rfc3647.txt		2003
RFC 5019	The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, *http://www.rfc-editor.org/pipermail/rfc-dist/2007-September/001760.html*		September 2007
RFC 5280	*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*		April 2002

11. ACRONYMS AND ABBREVIATIONS

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

12. GLOSSARY

access	Ability to make use of any information system (IS) resource.
access control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems.
accreditation	Formal declaration by a Designated Approving Authority that an IS is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
Affiliated Organization	Organizations that authorize affiliation with Subscribers of PIV-I certificates
Agency	Any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Executive Branch of the Federal Government.
applicant	The Subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed.
archive	Long-term, physically separate storage.
Attribute Authority	An entity, recognized by a CMA, as having the authority to verify the association of attributes to an identity.
audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
audit data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event.
authenticate	To confirm the identity of an entity when that identity is presented.
authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
backup	Copy of files and programs made to facilitate recovery if necessary.
binding	Process of associating two related elements of information.
biometric	A physical or behavioral characteristic of a person.
card management system	The system for managing the issuance of a smart card that may provide the electronic and graphical personalization of the card
certificate	A digital representation of information which at least (1) identifies the CA issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the CA issuing it.
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
Certification Authority (CA)	An authority trusted by one or more users to create and assign certificates.
CA facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
certificate-related information	Information, such as a Subscriber's postal address, that is not included in a certificate, but that may be used by a CA in certificate management.
client (application)	A system entity, usually a computer process acting on behalf of a human user that makes use of a service provided by a server.

compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by NIST
confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.
cryptographic module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.
cryptoperiod	Time span during which each key setting remains in effect.
data integrity	Assurance that the data are unchanged from creation to reception
dual use certificate	A certificate that is intended for use with both digital signature and data encryption services.
e-commerce	The use of network technology (especially the Internet) to buy or sell goods and services
Encryption (or Confidentiality) certificate	A certificate containing a public key that is used to encrypt or decrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes. The process of storing protecting and escrowing the private component of the key pair associated with the encryption certificate is sometimes referred to as key management.
erroneous issuance	Issuance of a certificate not materially in accordance with the procedures required by the CPS, issuance of a certificate to a person other that the one named as the subject of the certificate, or issuance of a certificate without the authorization of the person named as the subject of such certificate.
firewall	Gateway that limits access between networks in accordance with local security policy.
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.
Local Registration Authority (LRA)	An RA with responsibility for a local community.
naming authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
National Security System	Any telecommunications or information system operated by the U.S. Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]

non-repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data.
Non-verified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization; the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI OIDs are used to uniquely identify each of the four policies and cryptographic algorithms supported.
Organization CMS	The SSP customer organization operating the CMS function for the SSP service.
Out-of-Band	Communication between parties using a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
PKI Sponsor	Fills the role of a Subscriber on behalf of an organizational role or organizations that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this document.
Policy Authority (PA)	Authority that oversees the creation and update of Certificate Policies, reviews Certification Practice Statements, reviews the results of CA audits for policy compliance, evaluates non-domain policies for acceptance within the domain, and generally oversees and manages the PKI certificate policies. The individual or group that is responsible for maintaining the SSP CPS and for ensuring that all SSP PKI components (e.g., CAs, CSSs, CMSs, RAs) are operated in compliance with this CPS and the CP,
privacy	State in which data and system access is restricted to the intended user community and target recipient(s).
Private key compromise	A loss, theft or modification, or unauthorized access of a private key corresponding to the public key listed in a certificate governed by this CPS, including without limitation by cryptographic analysis or key extraction.
Public Key Infrastructure (PKI)	Framework established to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	Entity responsible for identification and authentication of certificate subjects that has automated equipment for the communication of applicant data to Certification Authorities and does not sign or directly revoke certificates.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application.
Relying Party	A person who has received a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
repository	A trustworthy system for storing and retrieving certificates or other information relevant to certificates.
revocation	The act or process of prematurely ending the operational period of a certificate effective at a specific date and time.
risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

risk tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
server	A system entity that provides a service in response to requests from clients.
Signature certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions. Also referred to as an Identity Certificate.
subordinate CA	In a hierarchical PKI, a CA whose certificate signing key is certified by another CA, and whose activities are constrained by that other CA. (see superior CA)
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to such an entity, and (2) holds a private key that corresponds to a public key listed in that certificate. Current subscribers possess valid CDS-issued certificates.
superior CA	In a hierarchical PKI, a CA who has certified the certificate signing key of another CA, and who constrains the activities of that CA. (see subordinate CA)
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.
unauthorized revocation	Revocation of a certificate without the authorization of the subscriber.
zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data.

APPENDIX A: CERTIFICATE AND CRL FORMATS

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

The following profiles are included:

A.1: Non-Federal SSP Intermediate Certificate Profile

A.2: Non-Federal SSP CRL Profile

A.3: Non-Federal SSP Signature Certificate Profile

A.4: Non-Federal SSP Encryption Certificate Profile

A.5: Non-Federal SSP Device Certificate Profile

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

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

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

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

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

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

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

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

A.1: Non-Federal SSP Intermediate Certificate Profile

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

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

Field	Criticality Flag	Value	Comments
issuerDomainPolicy		OID	OID of policy from the issuing CA domain that maps to the equivalent policy in the subject CA's domain.
subjectDomainPolicy		OID	OID of policy in the subject CA's domain that may be accepted in lieu of the issuing domain policy.

A.2: Non-Federal SSP CRL Profile

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

A.3: Non-Federal SSP Signature Certificate Profile

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

Field	Criticality Flag	Value	Comments
authorityInfoAccess	FALSE		authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued under the Common Certificate Policy must include an authorityInfoAccess extension with at least one instance of the caIssuers access method that specifies an HTTP URI. The OCSP access method may also be included if status information for this certificate is available via OCSP.
accessMethod		id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible Web server where certificates issued to the issuer of this certificate may be found.
accessLocation			
GeneralName			
uniformResourceIdentifier		http://…	See preamble text on URIs.
subjectAltName	FALSE		Must include the rfc822Name. Other name types may be present to support local applications.
rfc822Name		IA5String	This field contains the electronic mail address of the subject.
optional extensions			
extKeyUsage	FALSE		If included to support specific applications, the extension MUST include the anyExtendedKeyUsage value. Additional key purposes may be specified.
keyPurposeID		2.5.29.37.0	anyExtendedKeyUsage OID indicates that the certificate may also be used for other purposes meeting the requirements specified in the key usage extension.

A.4: Non-Federal SSP Encryption Certificate Profile

Field	Criticality Flag	Value	Comments
Certificate			
tbsCertificate			Fields to be signed.
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		INTEGER	Unique positive integer.
signature			
AlgorithmIdentifier		Choice of following algorithms:	
		1.2.840.113549.1.1.11	Sha256WithRSAEncryption
		1.2.840.10045.4.3.2	ecdsa-with-SHA256
		NULL	For all RSA algorithms except id-RSASSA-PSS
issuerName			Must use one of the name forms specified in section 3.1.1 of the CPS.
validity			
notBefore			
notAfter			
subjectName			X.500 Distinguished name of the owner of the certificate.
RDNSequence			Must use one of the name forms specified in section 3.1.1 of the Common Certificate Policy.
subjectPublicKeyInfo			
AlgorithmIdentifier			Public key algorithm associated with the public key.
algorithm		1.2.840.113549.1.1.1	RSA Encryption
		1.2.840.10045.2.1	Elliptic curve key
RSAParameters		NULL	For RSA, parameters field is populated with NULL.
subjectPublicKey		BIT STRING	For RSA public keys: certificates shall have a modulus of at least 2048 bits.
required extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
keyUsage	TRUE		
digitalSignature		0	
nonRepudiation		0	
keyEncipherment		1	Asserted when public key is RSA.
dataEncipherment		0	
certificatePolicies	FALSE		
PolicyInformation			Key management certificates issued to human subscribers should assert one of the following policies. Other policy OIDs may be asserted as well.
policyIdentifier		2.16.840.1.113733 1.7.23.1.1.1	*id-stn-ssp-rudimentary*
		2.16.840.1.113733 1.7.23.2.1.1	*id-stn-ssp-basic*
		2.16.840.1.113733 1.7.23.3.1.6	*id-stn-ssp-medium*

Field	Criticality Flag	Value	Comments
		2.16.840.1.113733 1.7.23.3.1.7	*id-stn-ssp-mediumHardware*
		2.16.840.1.113733 1.7.23.3.1.14	id-stn-ssp-medium CBP
		2.16.840.1.113733 1.7.23.3.1.15	id-stn-ssp-mediumHardware CBP
cRLDistributionPoints	FALSE		This extension is required in all end entity certificates and must contain at least one HTTP URI. The reasons and cRLIssuer fields must be omitted.
uniformResourceIdentifier		http://…	See preamble text on URIs.
authorityInfoAccess	FALSE		authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued under the FBCA Certificate Policy must include an authorityInfoAccess extension with at least one instance of the caIssuers access method: one that specifies an HTTP URI. The OCSP access method may also be included if status information for this certificate is available via OCSP.
AccessDescription			
accessMethod		id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible Web server where certificates issued to the issuer of this certificate may be found.
accessLocation			
GeneralName			
uniformResourceIdentifier		http://…	See preamble text on URIs.
subjectAltName	FALSE		Must include the rfc822Name. Other name types may be present to support local applications.
rfc822Name		IA5String	This field contains the electronic mail address of the subject.

A.5: Non-Federal SSP Device Certificate Profile

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

Field	Criticali	Value	Comments
policyIdentifier		2.16.840.1.113733.1.7.23.3.1.8	*id-stn-ssp-mediumDevices*
		2.16.840.1.113733.1.7.23.3.1.36	*id-stn-ssp-mediumDevicesHardware*
cRLDistributionPoints	FALSE		This extension is required in all end entity certificates and must contain at least one HTTP URI. The reasons and cRLIssuer fields must be omitted.
uniformResourceIdentifier		http://…	See preamble text on URIs.
authorityInfoAccess	FALSE		authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued under the FBCA Certificate Policy must include an authorityInfoAccess extension with at least one instance of the calssuers access method that specifies an HTTP URI. The OCSP access method may be included if status information for this certificate is available via OCSP.
accessMethod		id-ad-calssuers (1.3.6.1.5.5.7.48.2)	The access location shall include the URI name form to specify the location of an HTTP accessible Web server where certificates issued to the issuer of this certificate may be found.
accessLocation			
GeneralName			
uniformResourceIdentifier		http://…	See preamble text on URIs.
optional extensions			
extKeyUsage		BOOLEAN	This extension may be included as either a critical or non-critical extension if its inclusion is required by the application(s) for which the certificate will be used. If the inclusion of this extension is not intended to limit acceptable uses of the subject public key, then the extension should be marked non-critical and the anyExtendedKeyUsage value should be included. Additional key purposes may be specified.
KeyPurposeID		2.5.29.37.0	anyExtendedKeyUsage OID indicates that the certificate may also be used for other purposes meeting the requirements specified in the key usage extension.
issuerAltName	FALSE		Any name types may be present; only the most common are specified here.
rfc822Name		IA5String	Electronic mail address of the PKI administration
subjectAltName	FALSE		Any name types may be present; only the most common are specified here. Other names may be included to support local applications.
GeneralNames			
GeneralName			
dNSName		IA5String	This field contains the DNS name of the subject
iPAddress		IA5String	This field contains the IP address of the subject

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

Field	Criticality Flag	Value	Comments
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		INTEGER	Unique positive integer.
signature			
AlgorithmIdentifier			Must match Algorithm Identifier in signatureAlgorithm field. The parameters field is only populated when the algorithm is RSA.
algorithm		Choice of following algorithms:	
		1.2.840.113549.1.1.11	Sha256WithRSAEncryption
		1.2.840.10045.4.3.2	ecdsa-with-SHA256
parameters		NULL	
issuer			
Name			
RDNSequence			Must use one of the name forms specified in section 3.1.1 of the CPS.
validity			
notBefore		YYMMDDHHMMSSZ	
notAfter		YYMMDDHHMMSSZ	The notAfter time MUST not be after the PIV-I card expiration date.
subject			
Name			
RDNSequence			Must use one of the name form specified in section 3.1.1 of the CPS.
subjectPublicKeyInfo			
AlgorithmIdentifier			Public key algorithm associated with the public key. May be either RSA or elliptic curve.
algorithm		1.2.840.113549.1.1.1	RSA Encryption
		1.2.840.10045.2.1	Elliptic curve key
RSAParameters		NULL	For RSA, parameters field is populated with NULL.
subjectPublicKey		BIT STRING	For RSA public keys: certificates shall have a modulus of at least 2048 bits
required extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
keyUsage	TRUE		Only digitalSignature shall be set.
digitalSignature		1	
nonRepudiation		0	
keyEncipherment		0	
dataEncipherment		0	
extKeyUsage	TRUE		This extension shall assert only the *id-stn-ssp-pivi-cardAuth* keyPurposeID.
keyPurposeID		2.16.840.1.101.3.6.8	The *id-stn-ssp-pivi-cardAuth* keyPurposeID specifies that the public key is used to authenticate the PIV-I card rather than the PIV-I card holder.

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

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

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

Field	Criticality Flag	Value	Comments
uniformResourceIdentifier		http://…	See preamble text on URIs.
authorityInfoAccess	FALSE		authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued for PIV-I must include an authorityInfoAccess extension with at least one instance of the calssuers access method: that specifies an HTTP URI. The OCSP access method must be included since FBCA mandates OCSP distribution of status information for this certificate.
accessMethod		id-ad-calssuers (1.3.6.1.5.5.7.48.2)	When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible Web server where certificates issued to the issuer of this certificate may be found.
uniformResourceIdentifier		http://…	See preamble text on URIs.
accessMethod		id-ad-ocsp (1.3.6.1.5.5.7.48.1)	When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible OCSP server distributing status information for this certificate.
uniformResourceIdentifier		http://…	See preamble text on URIs.
subjectAltName	FALSE		
GeneralNames			This extension MUST include the UUID as specified below. Any additional name types may be present; only the most common are specified here. Other names may be included to support local applications.
GeneralName			
uniformResourceIdentifier		UUID	This field contains the UUID from the CHUID of the PIV-I card encoded as a URI as specified in Section 3 of RFC 4122.
otherName			Where supporting Microsoft *Smart Card Logon*, this name must be present
type-id		1.3.6.1.4.1.311.20.2.3	UPN OtherName OID
value		UTF8String	This field specifies Microsoft user principal name for use with Microsoft Windows logon.
optional extensions			
extKeyUsage	FALSE		This extension need not appear. If included to support specific applications, the extension MUST include the anyExtendedKeyUsage value. Additional key purposes may be specified.
keyPurposeID		1.3.6.1.4.1.311.20.2.2	Microsoft Smart Card Logon
		1.3.6.1.5.5.7.3.2	TLS client authentication
		2.5.29.37.0	anyExtendedKeyUsage OID indicates that the certificate may also be used for other purposes meeting the requirements specified in the key usage extension.

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

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

Field	Criticality Flag	Value	Comments
uniformResourceIdentifier		http://…	See preamble text on URIs.
authorityInfoAccess	FALSE		authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued for PIV-I must include an authorityInfoAccess extension with at least one instance of the calssuers access method that specifies an HTTP URI. The OCSP access method must be included since FBCA mandates OCSP distribution of status information for this certificate.
accessMethod		id-ad-calssuers (1.3.6.1.5.5.7.48.2)	When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible Web server where certificates issued to the issuer of this certificate may be found.
uniformResourceIdentifier		http://…	See preamble text on URIs.
accessMethod		id-ad-ocsp (1.3.6.1.5.5.7.48.1)	When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible OCSP server distributing status information for this certificate.
uniformResourceIdentifier		http://…	See preamble text on URIs.
optional extensions			
subjectAltName	FALSE		
GeneralNames			This extension MUST include the UUID as specified below. Any additional name types may be present; only the most common are specified here. Other names may be included to support local applications.
GeneralName			
rfc822Name		IA5String	This field contains the electronic mail address of the subject.
AttributeType		OID	
AttributeValue			This field contains the electronic mail address of the subject.
extKeyUsage	FALSE		If included in a certificate that is specifically designated for use in a single application, the extension may be marked either critical or non-critical. If included in any other certificate (to support specific applications), the extension must include the anyExtendedKeyUsage value and must be marked non-critical. Additional key purposes may be specified.
keyPurposeID		2.5.29.37.0	anyExtendedKeyUsage OID indicates that the certificate may also be used for other purposes meeting the requirements specified in the key usage extension.

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

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

Field	Criticality Flag	Value	Comments
uniformResourceIdentifier		http://…	See preamble text on URIs.
authorityInfoAccess	FALSE		authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued for PIV-I must include an authorityInfoAccess extension with at least one instance of the calssuers access method that specifies an HTTP URI. The OCSP access method must be included since FBCA mandates OCSP distribution of status information for this certificate.
accessMethod		id-ad-calssuers (1.3.6.1.5.5.7.48.2)	When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible Web server where certificates issued to the issuer of this certificate may be found.
uniformResourceIdentifier		http://…	See preamble text on URIs.
accessMethod		id-ad-ocsp (1.3.6.1.5.5.7.48.1)	When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible OCSP server distributing status information for this certificate.
uniformResourceIdentifier		http://…	See preamble text on URIs.
optional extensions			
subjectAltName	FALSE		
GeneralNames			
GeneralName			
rfc822Name		IA5String	This field contains the email address of the subject.
AttributeType		OID	
AttributeValue			

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

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

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

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

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

APPENDIX B: PIV-I CMS REQUIREMENTS

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

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

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

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

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

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

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

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

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

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

APPENDIX C: PIV-I SMART CARD DEFINITION

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

The following requirements shall apply to PIV-I Cards:

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

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

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

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

Revision History

History of changes: version 2.0 (effective September 15, 2017)

Section	Changes made
Various	Specified PA throughout the document as either FPKIPA or Symantec PMA; Corrected some typos; Replaced http queries with ldap queries
1. INTRODUCTION	Removed: The US Government has identified the need for Shared Service Providers (SSPs) to provide Public Key Infrastructure (PKI) services for Federal employees, contractors and other affiliated individuals requiring PKI credentials for access to Federal government physical and logical systems. Symantec is an approved (Federal) PKI Shared Service Provider operating under a Memorandum of Agreement (MOA) with the Federal PKI Policy Authority (FPKIPA). The Symantec SSP PKI service for Federal agencies has been certified for compliance with the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework.
1.2 Document Name and Identification	Specified CP as Symantec Trust Network CP Removed Sha-1 references Removed: however, this does not restrict certificates issued to non-person entities from asserting one or more other policies if all requirements for those policies are met. Added: End-Entity certificates issued to devices after January 15, 2017 shall assert the id-stn-ssp-mediumDevices, id-stn-ssp-mediumDevicesHardware, or id-stn-ssp-pivi-contentSigning policy. All other policies defined in this document should be reserved for human subscribers when used in End-Entity certificates.
1.3.1.3 Organization Policy Management Authority	Removed the Federal PKI PA in this context
1.4.1 Appropriate Certificate Uses	Removed Sha-1 references
1.4.2 Prohibited Certificate Uses	Replaces “No Stipulation” with: Certificates shall be used only to the extent the use is consistent with applicable law, and in particular shall be used only to the extent permitted by applicable export or import laws. Symantec Certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage. CA Certificates may not be used for any functions except CA functions. In addition, end-user Subscriber Certificates shall not be used as CA Certificates. The SSP and its Participants do not issue any certificate that can be used for man-in-the-middle (MITM) or traffic management of domain names or IP addresses that the certificate holder does not legitimately own or control. Such certificate usage is expressly prohibited. Symantec periodically rekeys Intermediate CAs. Third party applications or platforms that have an Intermediate CA embedded as a root certificate may not operate as designed after the Intermediate CA has been rekeyed. Symantec therefore does not warrant the use of Intermediate CAs as root certificates and recommends that Intermediate CAs not be embedded into applications and/or platforms as root certificates. Symantec recommends the use of PCA Roots as root certificates.
1.5.4 CPS Approval Procedures	Replaced “waivers” with “changes”. Added: This CPS and corresponding compliance audit are submitted to the FPKIPA for approval.
3.1.2 Need for Names to be Meaningful	Removed: “even if the subject’s name is not meaningful.:
4.2.3 Time to Process Certificate Application	Replaced “No Stipulation” with: Symantec begins processing certificate applications within a reasonable time of receipt. There is no time stipulation to complete the processing of an application unless otherwise indicated in

Section	Changes made
	the relevant Subscriber Agreement, CPS or other Agreement between STN participants. A certificate application remains active until rejected.
4.4.3 Notification of Certificate Issuance by the CA to Other Entities	Replaced “any cross-certificate” with “any CA certificate”
4.6 Certificate Renewal	Added: SSP CAs may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the Subscriber name and attributes are unchanged.
4.7.4 Notification of New Certificate Issuance to Subscriber	Replaced “No Stipulation” with: Notification of issuance of a re-keyed certificate to the Subscriber is in accordance with Section 4.3.2
4.7.7 Notification of Certificate Issuance by the CA to Other Entities	Replaced “No Stipulation” with: RAs may receive notification of the issuance of certificates they approve.
4.9.1 Circumstances for Revocation	Added an example for suspected key compromise
4.9.7 CRL Issuance Frequency (If Applicable)	Changed SSP CA CRL issuance from “at least every 18 hours” to “at least every 12 hours”
4.9.13 Circumstances for Suspension	Replaced “No Stipulation” for end-entity certificates with “not supported”
5.2.1.2 Officer	Removed: All persons filling the Organization RA role shall be US citizens. Added: Organization RA personnel for Federal Agency PKIs must be US citizens. Organization RA personnel for other organization PKIs may be citizens of the country where the RA is located.
5.2.1.5 Trusted Agent	Removed: All persons filling the role of Trusted Agent shall be US citizens Added: Trusted Agents for Federal Agency PKIs must be US citizens. Trusted Agents for other organization PKIs may be citizens of the country where the RA they are representing is located.
5.2.1.6 PKI Sponsor	Removed: All persons filling the roles of PKI Sponsor shall be US citizens.
5.5.1 Types of Events Archived	Added: • Receipt and Acceptance of certificates
5.8 CA or RA Termination	Added: 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.
6.1.1.1 CA Key Pair Generation	Replaced “video taped” with “recorded”
6.1.5 Key Sizes	Removed all Sha-1 references
6.1.7 Key Usage Purposes (as per x509v3 field)	Added: Domain controller certificates are the only certificates enabled with both signing and encryption functionality.
6.2.1 Cryptographic Module Standards and Controls	Added “hardware” to “FIPS 140 Level 2 hardware” Added: PIV-I Cards are PKI tokens that have private keys associated with certificates asserting the stn-ssp-pivi-hardware or stn-ssp-pivi-cardAuth policy. PIV-I Cards shall only be issued using card stock that has been tested and approved by the FIPS 201 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 populated, representative sample PIV-I Card shall be submitted to the FIPS 201 Evaluation Program for testing. Removed references to specific crypto (LunaCA3) Added “minimum” to crypto requirement
6.2.1.1 Custodial Subscriber Key Stores	Added this entire new section: Custodial Subscriber Key Stores hold keys for a number of Subscriber certificates in one location. When a collection of private keys for Subscriber certificates are held in a single location, there is a higher risk associated with compromise of that cryptographic module than that of a single Subscriber.

Section	Changes made
	Cryptographic modules for Custodial Subscriber Key stores at the Rudimentary Assurance Level shall be no less than FIPS 140 Level 1 (Hardware or Software). For all other levels, the cryptographic module shall be no less than FIPS 140 Level 2 Hardware. In addition, authentication to the Cryptographic Device in order to activate the private key associated with a given certificate shall require authentication commensurate with the assurance level of the certificate.
6.2.4.2 Backup of Subscriber Private Signature Key	Specified in a bulleted list the exact policies that may not be backup up. Updated the list in the process.
6.2.10 Method of Destroying Private Keys	Added “by individual in 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 Removed: Guidance regarding the selection of their password/PIN is provided during the enrollment process Added: RAs are also required to choose their own PINs with an appropriate level of strength to protect their private key. Removed: RAs are also required to choose their own PINs. Guidance regarding the selection of PINs is provided during the enrollment process.
7.1.2 Certificate Extensions	Updated the titles of the two referenced documents
7.1.3 Algorithm Object Identifiers	Removed Sha-1 reference
7.2 CRL Profile 7.2.2 CRL and CRL Entry Extensions	Updated the document reference(s)
8.1 Frequency or Circumstances of Compliance Audit	Updated the URL
8.4 Topics Covered by Compliance Audit	Added “as well as any MOAs between the Entity PKI and any other PKI” to the list of requirements to comply with
9.2.3 Insurance or Warranty Coverage for End-Entities	Replaced “No Stipulation” with: The Symantec non-federal SSP does not offer warranty protection.
9.3.1 Scope of Confidential Information	Replaced “No Stipulation” with: 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 Symantec or a Customer, • Audit reports created by Symantec 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 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: 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: Symantec secures private information it receives from compromise and disclosure to third parties.
9.12.3 Circumstances under Which OID must be Changed	Replaced “No Stipulation” with: 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 Class of Certificate. Otherwise, amendments shall not require a change in Certificate policy object identifier.
9.16.1 Entire Agreement	Replaced “No Stipulation” with “Not applicable”
10. References	Updated URLs linking to referenced documents
11. Acronyms and Abbreviations	Added CSS and KMD to the list

Section	Changes made
Appendix A: Certificate and CRL Formats	Updated the titles of the two referenced documents
A.1 – A.11 Certificate Profiles	Removed Sha-1 references for signature algorithms and policy OIDs
A.6: Non-Federal SSP PIV-I Card Authentication Certificate Profile	Removed the option to set subjectAltName extension as 'Critical'
A.7: Non-Federal SSP PIV-I Authentication Certificate Profile	Removed exception in right-hand column for RDNSequence Removed the option to set subjectAltName extension as 'Critical'
Appendix C: PIV-I Smart Card Definition	Changed PIV-I Card expiration requirement from 5 to 6 years.

Version	Date / Status	Revision Details
1.24	October 2012	2012-01 – updates for RA & CMS audits (sections 1.3.1.2, 1.3.1.3, 8.0-8.6, glossary)
	March 2012	Modifications to comply with Change Proposals: 2010-05 –Section 3.2.3.1 - REAL ID credential accepted for identity proofing 2010-06 – Section 3.2.3.1 & 4.9.1 – Declaration of identity signature may be digitally signed. 2011-01 – section 3.2.3.1 – controls for databases supporting validation of subscriber attributes. 2011-02 – section 5.3.2 – Trusted Roles background check shall be refreshed every 10 years. 2011-03 – section 6.1.1.2 – clarification that for PIV-I certs used for digital sig or authentication, keys shall be generated in a h/w token (not generated by the CA). 2011-04 – Appx B - CMS system personnel are governed by the Trusted Roles eligibility & separation of duties in section 5. 2011-05 – n/a. 2011-06 – throughout doc – removed all references to LDAP services. 2011-07 – sections 1.1, 1.2, 1.3.4, 3.1.1, 3.2.3.4, 6.1.1.2, 6.2.1, 6.2.3.4, 6.2.4.6, 6.2.6, 6.2.8, A.1, A.5 – added policy for *id-fpki-mediumDevicesHardware*
		Section 4.9.9 & 10: Changed from RFC2560 OCSP to RFC5019 OCSP Section 6.1.5: Removed all Dec 31, 2011 deadlines for 2048 RSA asymmetric keys & 128 AES symmetric keys. Section 9.8.1: Addition to Limitation of Liability Throughout doc – changed ownership and branding from VeriSign to Symantec.
1.23	13 December 2010	Addition of deprecated SHA-1 OIDs which are in effect from 1/1/2011 until 1/1/2014. Sections: 1.2, 1.4.1, 6.1.5, 6.5.1, 6.6.2, 6.7, A, A.1, A.3, A.4, A.5, A.6, A.7, A.10.
1.23	27 September 2010	This CPS (RFC3647 format) replaces Version 1.10 dated November 6, 2008 and incorporates changes to comply with the U.S. Federal Bridge PKI Certificate Policy version 2.16, dated May 14, 2010.
1.22	28 May 2010	Updated for compliance with PIV-I assurance levels as specified by CP changes (# 2010-03, May 11, 2010), sections: 1.0, 1.2, 1.3.1.5, 1.3.3, 1.3.5, 1.4.1, 3.1.1, 3.1.2, 3.1.4, 3.2.2, 3.2.3, 3.2.3.1, 4.2.1, 4.9.1, 4.9.2, 4.9.10, 4.10, 5.1.2.1, 5.2.2, 5.2.4, 6.1.1.2, 6.1.2, 6.1.5, 6.1.7, 6.2.1, 6.2.4.2, 6.2.4.5, 6.2.8, 6.3.2, 6.4.3, 7.1.3, 7.1.4, 7.1.10, 8.1, 8.4, 8.5, 9.6.1, 9.6.5.3, 10, 11,12, Appx A, Appx B, Appx C. Added Medium-CBP & MediumHardware-CBP policies, sections 1.2, 5.3.2.

1.21	10 May 2010	Updated location of Primary & DR Facility: Primary changed from CA to Delaware, DRF changed from Virginia to CA (sections 1.1, 1.3.6.2. 5.7.1, 5.1.1). Section 5.1.1 – removed reference to Army Regs 380-5. Section 6.7 – clarified tools by systems & network; changed network scanning tools from "SATAN & Nessus" to "Qualys". Section 6.5.2 – updated to Solaris 8 & Oracle 10.
1.21	30 April 2010	Converted from rfc2527 to rfc3647 format.
1.20	12 Nov, 2009	This CPS replaces Version 1.10 dated Nov 6, 2008 to incorporate all changes resulting from the policy mapping against the SAFE CP. This revision further incorporates changes to the VeriSign PKI infrastructure resulting from planned evolution and internal compliance monitoring.
1.10	06 November, 2008	Incorporates all changes resulting from the policy mapping against the Federal Bridge CP.

* * * End of Document * * *