Symantec
Shared Service Provider

Certification Practice Statement

Version 1.14
12 April 2013

(Portions of this document have been redacted.)

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

Symantec Shared Service Provider (SSP) Certification Practice Statement

Printed in the United States of America.
Revision Date: April 12, 2013

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 Practices Statement 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
practices@symantec.com

TABLE OF CONTENTS

1. INTRODUCTION

The US Government has identified the need for Shared Service Providers (SSP) to provide PKI services for Federal employees, contractors and other affiliated individuals requiring PKI credentials for access to Federal systems. Symantec is an approved Shared Service Provider operating under a Memorandum of Agreement (MOA) signed by the Federal PKI Policy Authority (PA). The Symantec SSP Certificate Practices Statement (CPS) and associated Compliance Audit have been approved by the PA. The Symantec SSP PKI is also certified as an approved service by the GSA FIPS 201 Evaluation Program.

This Symantec SSP Certification Practice Statement (CPS) in conjunction with the X.509 Certificate Policy for the Common Policy Framework (CP) defines the practices that Symantec will employ in issuing and managing certificates and in maintaining a certificate-based public key infrastructure (PKI) for the SSP. The Symantec SSP CPS is posted in the Symantec repository at *www.symantec.com/about/profile/policies/repository.jsp*.

1.1 Overview

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

The Symantec SSP PKI service offering provides complete certificate life-cycle support and certificate repository services for approved entities. The architecture and functional solution for the Symantec SSP offering is based on Symantec's managed PKI service offering which has been deployed at numerous government agencies, and also has been approved for cross-certification with the Federal Bridge Certification Authority (FBCA) at the Medium assurance level. The Symantec SSP PKI operates multiple assurance levels defined by the SSP Common Policy as listed in section 1.1.2.

The Symantec SSP CA primary location is at the Symantec data center located in a Symantec facility 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.

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

End-entities supported by the Symantec SSP PKI are Federal employees, contractors and affiliates needing access to Federal facilities and IT systems. The Symantec SSP CA will issue X.509 Version 3 certificates compliant with the certificate profiles listed in the CP and Appendix A of this CPS. The certificates can be used by the Subscribers and Relying Parties for both physical and logical access including use in a variety of secure commercial and government-developed applications such as electronic mail, signature of electronic forms and contract documents, secure document exchange, and secure web access and transmission.

1.1.1 Certificate Practices Statement (CPS)

This CPS is the statement of practices that Symantec will employ when issuing digital certificates as an approved SSP. This CPS is structured in accordance with RFC 3647 of the Internet Engineering Task Force (IETF).

This CPS describes a PKI for Federal employees, individuals and organizations transacting business electronically with Federal agencies. 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.

The SSP Certificate Policy defines the requirements 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 SSP PKI services delivered in accordance with the CP. The CP includes seven distinct certificate policies: a policy for user with software cryptographic modules, a policy for users with hardware cryptographic modules, a policy for devices with software cryptographic modules, a policy for devices with hardware cryptographic modules, a high assurance user policy, a user authentication policy, and a card authentication policy. Certificates issued by the Symantec SSP PKI service will assert at least one of the following Policy Object Identifiers defined in the CP:

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

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

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

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

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

id-fpki-common-authentication ::= {2 16 840 1 101 3 2 1 3 13}
For user authentication only, no digital signature capability (e.g., PIV authentication with *pivFASC-N* attribute specific to FIPS 201 Personal Identity Verification Card). Uses: client authentication for physical access after private key activation; requires OCSP services.

id-fpki-common-cardAuth ::= {2 16 840 1 101 3 2 1 3 17}
For user authentication only, no digital signature capability (e.g., PIV authentication with *pivFASC-N* attribute specific to FIPS 201 Personal Identity Verification Card). Uses: client authentication for physical access – private key can be used without Subscriber activation; requires OCSP services

Certificates issued to the SSP CA may contain any or all of these OIDs. Certificates issued to users to support digitally signed documents or key management may contain the *id-fpki-common-policy, id-fpki-common-hardware,* or *id-fpki-common-High*. Certificates issued to users supporting authentication but not digital signature may contain *id-fpki-common-authentication*. Certificates issued to users supporting token authentication where the private key can be used without user authentication may contain *id-fpki-common-cardAuth*. The devices policies apply to hardware devices and software applications (non-person entities) operated by or on behalf of federal agencies. Subscriber certificates issued to devices under this policy that use FIPS 140 Level 2 or higher cryptographic modules shall include either *id-fpki-common-devices, id-fpki-common-devicesHardware* or both. Subscriber certificates issued to devices under this policy using software cryptographic modules shall include *id-fpki-common-devices*. These Policy Object Identifiers are populated in accordance with CPS § 7.1.6.

NOTE: The OID breakdown for 2.16.840.1.101.3.2.1.3 is as follows: joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) csor(3) pki(2) cert-policy(1) fpki-common(3).

Only SSP CA Certificates with SHA-2 key pairs support the issuance of certificates containing SHA-2 key pairs. Only SSP CA Certificates with SHA-1 key pairs may, after December 31, 2010, continue to issue certificates containing SHA-1 key pairs that assert one of the following SHA-1 Federal Root CA related policy OIDs and signed using SHA-1.

SHA1 Federal Root Policy	OID	Corresponding id-fpki-common policy
id-fpki-SHA1-policy	::= {2 16 840 1 101 3 2 1 3 23}	*id-fpki-common-policy*
id-fpki-SHA1-hardware	::= {2 16 840 1 101 3 2 1 3 24}	*id-fpki-common-hardware*
id-fpki-SHA1-devices	::= {2 16 840 1 101 3 2 1 3 25}	*id-fpki-common-devices*
id-fpki-SHA1-authentication	::= {2 16 840 1 101 3 2 1 3 26}	*id-fpki-common-authentication*
id-fpki-SHA1-cardAuth	::= {2 16 840 1 101 3 2 1 3 27}	*id-fpki-common-cardAuth*

1.3 PKI Participants

1.3.1 PKI Authorities

1.3.1.1 Federal PKI Policy Authority (FPKIPA)

The Federal PKI Policy Authority (PA) is a group of U.S. Federal Government Agencies (including cabinet-level Departments) established by the Federal CIO Council. The PA is responsible for maintaining the CP, approving the CPS and Compliance Audit for each CA that issues certificates under the CP.

1.3.1.2 Policy Management Authority

The Symantec SSP Policy Management Authority (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 FPKI Common Policy regardless of by whom the PKI component is managed and operated.

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

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

1.3.1.3 Certification Authority (CA)

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

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

1.3.1.4 Certificate Status Authority/Certificate Status Server

The Symantec SSP provides online status information using OCSP as described in sections 4.9.9 and 4.9.10. A Certificate Status Authority (CSA) shall assert all the policy OIDs for which it is authoritative.

1.3.2 Registration Authorities

1.3.2.1 Registration Authority (RA)

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

The Symantec SSP RA is a Symantec trusted person operating a dedicated RA workstation within Symantec's secure facilities on Symantec's internal corporate network. The Agency RA is a trusted person operating a dedicated RA workstation on the Agency internal network. RA personnel will be issued public key certificates to enable secure authenticated access to the SSP CA. The RA certificate is stored on a FIPS 140 Level 2 hardware token.

1.3.2.2 Trusted Agent

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

1.3.3 Subscribers

An SSP Subscriber is an entity whose name appears as the subject in an SSP certificate, and who asserts that it uses its key and certificate in accordance with SSP policy. Subscribers are limited to Federal employees, contractors and affiliated personnel, workstations, firewalls, routers, trusted servers (e.g., database, FTP, and WWW), and other infrastructure components communicating securely with or for a US government agency at local, state or Federal level. These components must be under the control of humans, who accept the certificate and are responsible for the correct protection and use of the associated private key.

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

1.3.4 Relying Parties

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

1.3.5 Other Participants

1.3.5.1 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.

1.3.5.2 Repository

Symantec will operate the SSP Repository from its secure data facility located in Delaware. This repository contains SSP Subscriber certificates, Certificate Revocation Lists (CRLs) and the Symantec SSP CA certificate and associated CRL. 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 personnel and processes. Subscribers and Relying Parties may query, view, and download certificate and CRL entries in the repository via an http query.

1.4 Certificate Usage

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

1.4.1 Appropriate Certificate Uses

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

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

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

The use of SHA-1 to create digital signatures is deprecated beginning January 1, 2011. As such, use of SHA-1 certificates issued on or after January 2011 under this policy are limited to applications for which the risks associated with the use of a deprecated cryptographic algorithm have been deemed acceptable.

1.4.2 Prohibited Certificate Uses

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

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

1.5 Policy Administration

1.5.1 Organization Administering the Document

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

Symantec Corporation
350 Ellis Street
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 Federal Policy Authority (PA) determines the suitability of the Symantec SSP CPS and its compliance with the Federal Common Policy CP.

1.5.4 CPS Approval Procedures

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

The PA is the final approval authority of any proposed waiver to CP which with this CPS is compliant.

1.6 Definitions and Acronyms

See Appendix B and D for definitions and acronyms.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The Symantec SSP Repository is accessible through UniformResource Identifier (URI) references asserted in valid certificates. The Repository is implemented in compliance with the standards contained in the Shared Service Provider Repository Service Requirements (SSP-REP). End users may search for SSP certificates or CRLs using http URI queries. The Symantec repository is accessible via http query at http://onsitecrl.verisign.com/<jurisdiction>/LatestCRL.crl.

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 repository is accessible via methods described in Section2.1.

Symantec may replicate certificates and CRLs in additional repositories for performance enhancement. Such repositories may be operated by Symantec or other parties (e.g. Federal agencies).

2.2 Publication of Certification Information

2.2.1 Publication of Certificates and Certificate Status

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

1. All CA certificates issued by or to the Symantec SSP CA;
2. All valid and un-expired Symantec SSP Certificates, except for *Certificates that contain the FASC-N in the subject alternative name extension, such as PIV Authentication certificates and Card Authentication certificates, which shall not be distributed via public repositories (e.g., via HTTP)*;
3. Certificate status information, including revocation;
4. The most recently issued CRL;
5. The Symantec SSP 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.

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

2.2.2 Publication of CA Information

The Common Policy CP is made publicly available by the FPKIPA at *http://www.idmanagement.gov/fpkipa* The Symantec document repository at *www.symantec.com/about/profile/policies/repository.jsp* provides access to an abridged version of this CPS including at least the following topics covered under the CP:

- Section 1.4, SSP Contact Information;
- Section 3.1, Initial Registration;

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

The 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 Symantec SSP shall immediately change the status of the certificate in the Symantec SSP Repository from pending to valid.

Upon revoking a certificate, the Symantec SSP 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 HTTP 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

For certificates issued by the Symantec SSP for *id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-High, id-fpki-common-authentication, id-fpki-common-devices and id-fpki-common-devicesHardware*, the CA shall use the X.500 DN name format for subject and issuer name fields. These distinguished names may be in either of two forms: an X.501 distinguished name specifying a geo-political name; or an Internet domain component name.

3.1.1.1 Geo-Political Name DN

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

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

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

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

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

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

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

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

* subjectAltname=FASC-N

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

* subjectAltName=UUID (see Practice Note)

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

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

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

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

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

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

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

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

In the first name form, nickname may be the Subscriber's first name, a form of the first name, middle name, or pseudonym (e.g., Buck) by which the Subscriber is generally known. A generational qualifier, such as "Sr." or "III", may be appended to any of the common name forms specified above. In the last form, dnQualifier is an integer value that makes the name unique. When a qualifier attribute is included, it may appear as part of a multi-valued relative distinguished name (RDN) with the common name or as a distinct RDN that follows the RDN containing the common name attribute. The last form shall be used only if the other three name forms have already been assigned to Subscribers.

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

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

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

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

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

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

3.1.1.2 Internet Domain Component Name

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.1.2 Need for Names to be Meaningful

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

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

* cn=firstname initial. lastname

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

* cn=AgencyX CA-3.

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

3.1.3 Anonymity or Pseudonymity of Subscribers

The SSP CAs shall not issue anonymous or pseudonymous names in 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 the pivFASC-N name type are specified in [PACS].

3.1.5 Uniqueness of Names

The Symantec SSP will ensure the uniqueness of names for all certificates issued within the SSP 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 Symantec SSP shall not knowingly issue a certificate including a name that a court of competent jurisdiction has determined infringes the trademark of another.

Symantec shall investigate and correct, if necessary, any name collisions brought to its attention. If appropriate, Symantec shall coordinate with and defer to the PA naming authority. Agency 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 Symantec SSP CA shall require proof of possession of the private key that corresponds to the public key in the certificate request. The technical mechanism to establish this proof is verification that the Subscriber's certificate enrollment request containing their public key is digitally signed with the corresponding private key.

For Agency smart card issuance, certificate enrollment requests are sent from an Agency RA workstation to the SSP CA as signed and encrypted messages (PKCS #7-enveloped PKCS #10 requests) over an 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 Symantec SSP CA performs the digital signature validation checks to ensure it is a properly formed message and that its integrity has not been altered.

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

3.2.2 Authentication of Organization Identity

Requests for CA certificates shall include the name of the Agency, address, and documentation of the existence of the organization. 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 Agency.

3.2.3 Authentication of Individual Identity

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

3.2.3.1 Authentication of Human Subscribers

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

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

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

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

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

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

   a) Process #1:

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

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

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

   b) Process #2:

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

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

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

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

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

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

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

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

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

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

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

   a) Process #1:

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

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

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

   b) Process #2:

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

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

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

4) A biometric of the applicant (e.g., a photograph or fingerprint) shall be recorded and maintained by the RA or CA. This establishes an audit trail for dispute resolution.

Additionally, the RA shall record the process that was followed for issuance of each certificate. The process documentation and authentication requirements shall include the following:

- The identity of the person performing the identification;
- A signed declaration by that person that he or she verified the identity of the Applicant as required by the CPS using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury);
- Unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- The biometric of the applicant;
- The date and time of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury).

Applications enrolling for certificates under *id-fpki-common-High* must appear in person before the RA. Except for applicants enrolling under *id-fpki-common-High*, where it is not possible for applicants to appear in person before the RA, a Trusted Agent may serve as proxy for the RA. The Trusted Agent forwards the information collected from the applicant directly to the RA in a secure manner. The requirement for recording a biometric of the applicant may be satisfied by making a copy of the government issued photo ID (passport or driver's license) presented to the Trusted Agent. The Trusted Agent shall verify the photograph against the appearance of the applicant and notarize a copy of the photo ID. The notarized copy of the photo ID shall be included with

the notarized Subscriber Enrollment form and sent to the RA either by first class postal mail, Federal Express or other similar means.

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

3.2.3.2 Authentication of Component Identities

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

- Device name (equipment identification (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.

The Symantec SSP requires in person registration of the PKI Sponsor, with the identity of the PKI Sponsor confirmed in accordance with the requirements of Section 3.2.3. 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

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

3.2.5 Validation of Authority

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

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

3.2.6 Criteria for Interoperation

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

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. For policies other than *id-fpki-common-High*, if it has been less than 6 years since a Subscriber was identified as required in Section 3.2, re-key requests for Subscriber certificates may be authenticated on the basis of existing Subscriber certificates. A Subscriber, whose certificates have not expired and whose initial Subscriber enrollment data has not changed, may re-key his or her certificates based on electronic authentication of a currently valid Signature and Encryption certificates. The Symantec SSP provides separate SSL-protected web pages for re-keying of Signature and Encryption certificates.

The Symantec SSP may issue Subscriber certificates with one, two or three year lifetimes. If more than six (6) years have passed since a Subscriber's identity was authenticated as specified in Section 3.2, a Subscriber certificate re-key shall follow the same procedures as initial certificate issuance.

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

CA Certificate Re-key and re-key of certificates issued under *id-fpki-common-High* 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 Symantec 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. Alternatively, the Subscriber may request revocation of his or her certificate by sending a digitally signed e-mail message to the RA. The RA will authenticate the request by verifying the digital signature on the signed-mail.

A Trusted Agent may request revocation of an affiliated Subscriber's certificate by sending a digitally signed e-mail message to Symantec. The RA will authenticate the request by validating the digital signature on the signed e-mail and will check that the Trusted Agent is requesting revocation for a Subscriber certificate that is affiliated with his or her Agency or organization.

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

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

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

A certificate application may be submitted to the SSP CA by the Subscriber or by an Agency RA on behalf of the Subscriber. An application for a device certificate may be submitted by the human sponsor of the device. An application for a CA certificate shall be submitted by an authorized representative of the applicant CA in accordance with section 3.2.5.

4.1.2 Enrolment Process and Responsibilities

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

- Establish the applicant's authorization (by the employing or sponsoring agency) to obtain a certificate. (per Section 3.2)
- Establish and record identity of the applicant (per Section 3.2)
- Obtain the applicant's public key and verify the applicant's possession of the private key for each certificate required (per Section 3.2.1)
- Verify any role or authorization information requested for inclusion in the certificate.

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

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Hardware Credential

1) Applicants enrolling for a SSP certificate on a PIV smart card must appear before a designated Agency official, for authentication of identity as described in Section 3.2.3. After successfully completing the authentication requirements, applicants receive a completed enrollment authorization from the Agency official.
2) The Applicant must appear before an Agency RA and present the enrollment authorization form. The Agency RA initiates the process for personalization of the smart card, and after printing of the smart card, the Agency RA shall enroll on behalf of the Subscriber for the mandatory PIV Authentication certificate and optionally for other certificate types. Alternatively, after issuance of the smart card the Subscriber receives a Passcode from the Agency RA which may be later presented to an Agency-hosted, SSL-protected web page for enrollment for the optional certificates types.
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 Section 3.1. 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, posts the certificate to the SSP Repository and returns the certificate to the smart card issuance system where it is then downloaded onto the Subscriber's smart card.

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

Software Credential

1) Applicants must appear before a designated Agency official for in-person identity proofing in accordance with the requirements of Section 3.2.3. After successfully completing the identity authentication requirements, the Applicant receives an enrollment Passcode to be used for authentication during the certificate enrollment process.
2) Using a web browser, applicants connect to an Agency-hosted SSL-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. 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 Agency-hosted Key Manager. 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

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

4.2.3 Time to Process Certificate Applications

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

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

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

- Verify the identity of the requester as described in section 4.2.1.
- Verify the authority of the requester and the integrity of the information in the certificate request.
- Build and sign a certificate if all certificate requirements have been met (in the case of an RA, have the CA sign the certificate).
- Make the certificate available to the subscriber after confirming that the subscriber has formally acknowledged their obligations as described in section 9.6.3.

The SSP CA shall issue 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 9.6.4. The Subscriber is also notified that the private key associated with their Encryption certificate is escrowed. After the Agency RA downloads the Subscriber's certificates to the smart card, the Subscriber takes possession of the smart card and signs a receipt.

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 sign 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 SSP CA shall notify the Federal PKI Policy Authority when a CA certificate is issued.

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. The Symantec SSP does not implement certificate renewal for Subscriber or CA keys. 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 or modified.

When the Symantec 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.

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

Subscribers with a currently valid certificate may request certification of a new public key. RAs may request certification of a new public key on behalf of a subscriber. For device certificates, the human sponsor of the device may request certification of a new public key.

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

No stipulation.

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

No stipulation.

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.

4.9 Certificate Revocation and Suspension

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

4.9.1 Circumstances for Revocation

An SSP certificate shall be revoked when the binding between the subject and the subject's public key defined within the certificate is no longer considered valid. Under the following circumstances a certificate will be revoked:

- Identifying information including the organizational affiliation in the Subscriber's certificate changes, the affiliation is terminated, or the organization no longer authorizes the affiliation before the certificate expires;
- Privilege attributes asserted in the Subscriber's certificate are reduced;
- The certificate subject can be shown to have violated the requirements of this CPS or the Subscriber agreement;
- The private key is suspected of compromise; or
- The Subscriber or other authorized party asks for his/her certificate to be revoked.

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

4.9.2 Who Can Request Revocation

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

4.9.3 Procedure for Revocation Request

The revocation request must identify the certificate to be revoked and must include the reason for revocation. The certificate to be revoked must be uniquely identified with information including: the agency name, the subject name and the email address on the certificate. This information alone or combined is used to uniquely

identify the correct Subject DN of the certificate to be revoked. Optionally, the certificate serial number may be used to correctly discriminate one certificate among a history of certificates issued to the Subject. The certificate serial number value is unique across all generations of the Symantec SSP.

The revocation requests may be manually or digitally signed and must be authenticated by an RA. If the revocation is being requested for reason of key compromise or suspected fraudulent use, then the Subscriber's and the RA's revocation request must so indicate. The processes for revocation are as follows:

Certificate Revocation Request by Subscriber: An SSP Subscriber may request revocation of a certificate by sending a digitally signed message to the Agency RA. The message must include a reason for the revocation. The Agency RA will validate the request by verifying the signature on the signed message.

If the Subscriber is not in possession of their private Signature key, he or she may also request revocation of his or her certificate by presenting the unique challenge phrase selected during certificate enrollment to a revocation Web page hosted by Symantec. The Web page is protected using SSL. Upon successful validation of the revocation request by the SSP RA, the Symantec SSP will change the certificate status in the repository from "valid" to "revoked" and place the revoked certificate's serial number on the next published CRL.

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

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

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

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

Certificate Revocation Request by PKI Sponsor: A PKI Sponsor may request revocation of the non-human entity for which the Sponsor is identified as the representative. The Sponsor shall initiate the request for revocation to either a Trusted Agent or Agency RA, uniquely identifying themself as described above, and uniquely identifying the component by subject name (eg, DNS of the host). The RA and TA shall verify that requestor is the authorized Sponsor for the named Subscriber entity. The request is processed by the RA or TA using the relevant process variation described above, authenticating the identity of the Sponsor as representing

the Subscriber.

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

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

4.9.4 Revocation Request Grace Period

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

4.9.5 Time within Which CA Must Process the Revocation Request

The Subscriber or RA is obligated to request that the SSP CA revoke his or her certificate as soon as possible after the need for revocation has been determined. The SSP CA will revoke certificates as quickly as practical upon receipt of a proper revocation request.

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

4.9.6 Revocation Checking Requirement for Relying Parties

The 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

The Symantec SSP will generate and issue CRLs at least every eighteen (18) hours. All CRLs shall have a twenty-four (24) hour validity interval (*nextUpdate*). Superceded CRLs are removed from the repository upon posting of the latest CRL.

When a CA certificate is revoked because of compromise or suspected compromise of a private key, a CRL will be issued within six (6) hours of notification.

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

4.9.8 Maximum Latency for CRLs

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

4.9.9 On-Line Revocation/Status Checking Availability

The 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 2 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

Agencies issuing end entity certificates under *id-fpki-common-authentication* and *id-fpki-common-cardAuth* are required to utilize OCSP services as the primary status checking mechanism for such certificates.

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 server certificate at which Relying Parties may query the revocation status of a Subscriber certificate. This Web page is located at *https://pki-search.symauth.com/*

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 PA shall be immediately informed, as well as the US Government Root CA and any cross certified CAs. The SSP shall initiate procedures to notify Subscribers of the compromise; and the US Government Common Policy 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.

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

4.9.13 Circumstances for Suspension

For CA certificates, suspension is not permitted.

4.10 Certificate Status Services

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

4.11 End of Subscription

Subscription for a 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. CA private keys are never escrowed. The Subscriber private signature key is never escrowed. Under no circumstances shall a Subscriber's Signature key be held in trust by a third party.

Escrowed keys shall be protected at no less than the level of security in which they are generated, delivered, and protected by the Subscriber. Recovery of the private encryption key is under two man 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 *Agency RA* is a representative of a Federal Agency that has entered into a contract with Symantec for SSP PKI services. The Agency RA performs the equivalent functions of the Symantec SSP RA. The Agency RA has a secure, remote interface to the Symantec SSP. All communications between the Agency RA and the Symantec SSP are via an SSL session with certificate-based access control. The Agency RA certificate is stored on a FIPS 140 Level 2 hardware token. All persons filling the *Agency RA* role shall be US citizens.

5.2.1.5 Trusted Agent

A *Trusted Agent* is a person authorized to act as a representative of the Agency RA in providing Subscriber identity verification during the registration process. Trusted Agents do not have automated interfaces with the Symantec SSP CA. All persons filling the role of *Trusted Agent* shall be US citizens.

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 Agency RA and, when appropriate, Trusted Agents, to register components (web servers, routers, firewalls, etc.) in accordance with Section 3.2.3.4, and is responsible for meeting the obligations of Subscribers as defined throughout this document. All persons filling the roles of *PKI Sponsor* shall be US citizens.

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.
  (a)

5.3.3 Training Requirements

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

5.4 Audit Logging Procedures

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

5.4.1 Types of Events Recorded

All security auditing capabilities shall be enabled during installation of the Symantec SSP equipment to record events for the CA, RA, Agency 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
- Record of Re-key
- Revocation requests
- Subscriber identity Authentication data as per Section 3.1.9
- Subscriber agreements
- Documentation of receipt of tokens
- All CARLs and CRLs issued and/or published
- Other data or applications to verify archive contents
- Compliance Auditor Reports
- Changes made to the Audit parameters, e.g. audit frequency, type of event audited
- Attempts to delete or modify the Audit logs
- CA key generation (not mandatory for single session or one-time use symmetric keys)
- Access to escrowed Subscriber private encryption keys escrowed for key recovery purposes
- Changes to the trusted public keys including additions and deletions
- Export of private and secret keys (with the exception of keys used for a single session or messages)
- Approval or rejection of a certificate status change request
- Appointment of an individual to a Trusted Role
- Destruction of cryptographic modules
- All certificate compromise notifications
- Remedial action taken as a result of violations of physical security
- Violations of Certificate Policy
- Violations of Certification Practice Statement

5.5.2 Retention Period for Archive

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.

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

5.6 Key Changeover

The SSP will use its private signature keys for signing certificates and CRLs only. CA key pairs established under this CPS will be prevented by technical means from signing Subscriber certificates whose validity periods would extend beyond the expiration dates of the CA certificate's validity interval.

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

When an SSP CA key is changed, the old SSP CA keys will be retained to issue CRLs for Subscribers that have been issued certificates signed with the old SSP CA signing key.

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 Symantec 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 unexpired certificates signed by the SSP CA will be revoked. Dissemination of revocation notice will be achieved as discussed in CPS section 5.7.2.

The SSP CA shall transfer its archival records to an Agency PMA approved archival facility.

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

Symantec SSP CA and CSA key pairs are generated within Symantec's secure Key Ceremony room on hardware tokens. The ceremony is video taped and a full audit trail 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 SSP uses validated FIPS 140 software or hardware cryptographic modules to generate all Subscriber key pairs, as well as pseudo-random numbers and parameters used in key pair generation. Any pseudo-random numbers used for key generation material shall be generated by a FIPS-approved method. Symmetric keys may be generated by means of either software or hardware mechanisms.

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

For *id-fpki-common-hardware, id-fpki-common-devicesHardware, id-fpki-common-High, id-fpki-common-authentication,* or *id-fpki-common-cardAuth*, Subscriber signature key pairs are generated in a FIPS 140 Level 2 cryptographic module and may not be exported from the module that generated the key pairs (e.g., smart card).

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

6.1.2 Private Key Delivery to Subscriber

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

Hardware Credential

Key generation for authentication certificates 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 Agency RA who is responsible for accountability of the module until the Subscriber accepts possession of it. The Subscriber acknowledges receipt of the smart card and the SSP CA retains a record of the subscriber acknowledgment.

Private Encryption keys for smart cards are generated in the Agency 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.

Software Credential

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

Private encryption keys associated with software certificates are generated in hardware cryptographic modules and escrowed by the Agency hosted Key Manager. Immediately after escrowing of the private Encryption keys, all keying material is deleted from the Key Manager cryptographic module. Subscribers download the private encryption keys in a server-side SSL-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.

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

6.1.2.1 Acknowledgement of Private Key Delivery

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

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

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

6.1.3 Public Key Delivery to Certificate Issuer

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

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 US Government Common Policy Root Certificate and the Symantec SSP CA certificate 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 SSP Root Certificate hash against the hash value received from a Trusted Agent, Symantec RA or Agency RA.

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

6.1.5 Key Sizes and Signature Algorithms

After December 31, 2010, the Symantec SSP PKI shall operate two parallel PKI infrastructures, one of which will support the continued use of the SHA-1 which shall expire no later than December 31, 2013, and a second to support the use of SHA-256. Signature algorithms shall conform to RSA PKCS#1. Key sizes and hash algorithms are detailed below:

- The key pairs for Symantec SSP CAs are 2048-bit RSA key pairs and those that expire after 12/31/2030 shall be at least 3072 bits for RSA or 256 bits for elliptic curve algorithms.
- The key pairs for all end entity certificates are at least 2048-bit RSA key pairs.
- All Symantec SSP CAs, including the Symantec SSP Intermediate CA and the Agency SSP CAs shall use SHA-256 for digital signature except as noted below. The Symantec CSAs use the same signature algorithm, key size and hash algorithm used by the CA to sign CRLs. Signatures on certificates and CRLs shall be generated using SHA-256 except as noted below.
    - After December 31, 2010, only SSP CA certificates with SHA-1 key pairs may continue to issue certificates with SHA-1 key pairs asserting one of the specific set of SHA-1 related policy OIDs listed in section 1.2 with a validity period that expires on or before December 31, 2013.
    - CRLs issued after December 31, 2010 but before January 1, 2014 that include status information for certificates that were generated using SHA-1 may continue to be generated using SHA-1.
    - Certificates issued to OCSP responders that include SHA-1 certificates may be signed using SHA-1 until December 31, 2013.
- Symantec SSP CA-issued Transport Layer Security (TLS) or Secure Socket Layer (SSL) certificates currently use AES (128 bits) for symmetric keys and 2048 bit RSA for asymmetric keys.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters
Prime numbers for use with the RSA algorithm defined in [PKCS-1] shall be generated and checked in accordance with [PKCS-1]. Public key parameters for signature algorithms defined in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186.

Parameter Quality Checking

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)

All certificates shall include a critical key usage extension. The Symantec 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.

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

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 that contain elliptic curve public keys that are used for key agreement shall assert the *keyAgreement* 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-fpki-common-policy, id-fpki-common-devices*) 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-fpki-common-hardware, id-fpki-common-devicesHardware, id-fpki-common-authentication, id-fpki-common-cardAuth, id-fpki-common-High*) are obligated to use cryptographic modules that meet at least the criteria for FIPS 140 Level 2 for all cryptographic operations.

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

The Symantec SSP CA and CSA shall use a FIPS 140 Level 3 hardware cryptographic token.

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 Agency RA, is physically separated from the SSP.

6.2.3 Private Key Escrow

6.2.3.1 Escrow of CA Private Signature Key

CA private keys are not escrowed.

6.2.3.2 Escrow of CA Encryption Key

CA private keys are not escrowed.

6.2.3.3 Escrow of Subscriber Private Signature Key

Subscriber private signature keys are not escrowed.

6.2.3.4 Escrow of Subscriber Encryption Key

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 CA Private Signature Key

Backup copies of the Symantec 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 ensuring security controls consistent with the protection provided by the Subscriber's cryptographic module.

Subscriber private Signature keys are never escrowed.

For Subscriber private signature keys whose corresponding public key is contained in a certificate asserting the *id-fpki-common-authentication, id-fpki-common-cardAuth,* or *id-fpki-common-High* policy may not be backed up or copied.

Subscriber private signature keys whose corresponding public key is contained in a certificate that does not assert *the id-fpki-common-authentication, id-fpki-common-cardAuth, id-fpki-common-hardware* or *id-fpki-common-High* policy 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 CSA Private Key

See 6.2.4.1.

6.2.4.5 Backup of Device Private Key

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

6.2.5 Private Key Archival

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

6.2.6 Private Key Transfer Into or From a Cryptographic Module

When the Symantec SSP CA makes a backup copy of its 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 in a FIPS 140 Level 2 cryptographic module. RA private keys never exist in plaintext form outside of the boundary of the cryptographic module.

Subscribers whose certificates do not assert the *id-fpki-common-authentication, id-fpki-common-cardAuth, id-fpki-common-hardware, id-fpki-common devicesHardware* or *id-fpki-common-High* policy may use the secure export/import capability in the latest versions of the browsers to transfer keys and certificates via the PKCS#12 protocol.

6.2.7 Private Key Storage on Cryptographic Module

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

6.2.8 Method of Activating Private Key

The Symantec SSP 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-fpki-common-authentication, id-fpki-common-policy, id-fpki-common-hardware-* or *id-fpki-common-High* 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.

For certificates issued under *id-fpki-common-devices* and *id-fpki-common devicesHardware*, the device may be configured to activate its private key without requiring its human sponsor or authorized administrator to authenticate to the cryptographic token, provided that appropriate physical and logical access controls are implemented for the device and its cryptographic token. The strength of the security controls shall be

commensurate with the level of threat in the device's environment and shall protect the device's hardware, software and the cryptographic token and its activation data from compromise.

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

6.2.9 Method of Deactivating Private Key

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

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

6.2.10 Method of Destroying Private Key

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

6.2.11 Cryptographic Module Rating

See section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The key usage periods for keying material are described in Section 3.3.1 and Section 5.6. The usage period for all Symantec SSP CA key pairs is a maximum of ten (10) years. The SSP CA private key may be used to generate certificates for at most four (4) years, and the public key may be used to validate certificates for the entire usage period. If the CA private key is used to sign CRLs, it may be used to sign CRLs for the entire usage period. All certificates signed by a specific CA key pair must expire before the end of that key pair's usage period.

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

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

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Symantec SSP Subscribers are requested to select their own password/PIN to protect their private key. Guidance regarding the selection of their password/PIN for strength commensurate with authentication mechanisms for Level 2 in FIPS 140-2 is provided during the enrollment process.

RAs are also required to choose their own PINs. Guidance regarding the selection of PINs for strength commensurate with authentication mechanisms for Level 2 in FIPS 140-2 is provided during the enrollment process.

6.4.2 Activation Data Protection

The Symantec SSP CA and CSA activation data 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.

6.4.3 Other Aspects of Activation Data

See Section 6.4.1.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Software applications for the Symantec 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 CA, 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

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

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

7.1.3 Algorithm Object Identifiers

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

sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
ecdsa-with-SHA256	{iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2 (3) 2 }

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

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

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

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

The 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 responses.

7.1.4 Name Forms

The subject field in certificates issued under *id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-High, id-fpki-common-authentication, id-fpki-common-devices* and *id-fpki-common-devicesHardware* shall be populated with an X.500 Distinguished Name, with the attribute type as further constrained by RFC 5280. Each RDN contains a single attribute type, value pair. DirectoryString values are encoded as printable string.

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

The subject alternative name extension shall be present and include the pivFASC-N name type in certificates issued under *id-fpki-common-authentication* and *id-fpki-common-cardAuth*.

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 Symantec 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.

7.1.10 Key Usage Constraints for *id-fpki-common-authentication*

Certificates asserting *id-fpki-common-authentication* or *id-fpki-common-cardAuth* must include a critical key usage extension, asserting only *digitalSignature* value.

7.2 CRL Profile

CRLs issued by the SSP CA shall conform to the CRL profile specified in [CCP-PROF].

CRLs issued by a CA under the *id-fpki-SHA1-authentication*, *id-fpki-SHA1-cardAuth*, or *id-fpki-SHA1-hardware* policy shall conform to the CRL profile specified in [CCP-PROF] except that *SHA-1WithRSAEncryption* may be used as the signature algorithm in CRLs that are issued before January 1, 2014.

7.2.1 Version Number(s)

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

7.2.2 CRL and CRL Entry Extensions

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

7.3 OCSP Profile

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

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

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

8.1 Frequency or Circumstances of Assessment

The Symantec SSP CA, CSA and RA shall undergo an annual compliance audit as part of its annual PKI audit, and will make itself available for additional compliance audits that may be required by the PA. The Agency RA and CMS shall undergo an annual compliance audit. Compliance audits shall be conducted in accordance with the *Compliance Audit Requirements* document located at *www.idmanagement.gov/fpkipa/*

8.2 Identity/Qualifications of Assessor

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, COMSEC, COMPUSEC, and logical security. Specifically, the compliance audit team has the following applicable experience:

- a minimum of 5 years 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 Agency PMA is responsible for identifying and engaging a qualified auditor of Agency operations implementing aspects of this CPS with the following qualifications:

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

8.3 Assessor's Relationship to Assessed Entity

The 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 Symantec SSP auditor has not served in developing or maintaining Symantec's CA facility or Certification Practices Statement.

The Agency's RA and/or CMS auditor shall be an independent organization[2] engaged through a contractual relationship for audit services and may not have any other role or responsibility relating to the agency's SSP operation.

[2] 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 Assessment

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. All aspects of the Symantec CA/RA operations and the Agency RA/CMS operations shall be subject to compliance audit inspections in accordance with this CPS and any corresponding RPS.

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

8.5 Actions Taken as a Result of Deficiency

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

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

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

8.6 Communication of Results

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

On an annual basis, the Symantec PMA shall submit an audit compliance package to the Federal PKI Policy Authority. 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 1.5. 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

No stipulation.

9.3 Confidentiality of Business Information

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

9.3.1 Scope of Confidential Information

No stipulation.

9.3.2 Information Not Within the Scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

No stipulation.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

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

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

9.4.4 Responsibility to Protect Private Information

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.

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

9.4.5 Notice and Consent to Use Private Information

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

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

All disclosure shall be pursuant to applicable laws.

9.4.7 Other Information Disclosure Circumstances

All disclosure shall be pursuant to applicable laws.

9.5 Intellectual Property Rights

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

- Certificates and CRLs: Certificates and CRLs are the personal property of the 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 private keys are the personal property of Symantec Corporation.
- Symantec Public Keys: Symantec SSP 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;
- 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 PA a CPS, as well as any subsequent changes, for conformance assessment;
- Maintaining its operations in conformance to the stipulations of the approved CPS;
- Ensuring that registration information is accepted only from approved RAs operating under an approved CPS;
- Including only valid and appropriate information in certificates, and maintaining evidence that due diligence was exercised in validating the information contained in the certificates;
- Revoking the certificates of Subscribers found to have acted in a manner counter to their obligations in accordance with Section 9.6.4; and
- Operating or providing for the services of an online repository that satisfies the obligations under Section 2, and informing the repository service provider of their obligations if applicable.

9.6.2 RA Representations and Warranties

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

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

- Performing in-person identity verification of certificate applicants in accordance with Section 3.2.3;
- Maintaining its operations in conformance to the stipulations of the approved CPS;
- Including only valid and appropriate information in certificate requests, and maintaining evidence that due diligence was exercised in validating the information contained in the certificate; and
- Ensuring that obligations are imposed on Subscribers in accordance with Section 9.6.4, and that Subscribers are informed of the consequences of not complying with those obligations.

9.6.3 Trusted Agent Representations and Warranties

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

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

- Performing in-person identity verification of certificate applicants in accordance with Section 3.2.3;
- Including only valid and appropriate information in certificate requests, and maintaining evidence that due diligence was exercised in validating the information contained in the certificate; and
- Ensuring that obligations are imposed on Subscribers in accordance with Section 9.6.4, and that Subscribers are informed of the consequences of not complying with those obligations.

9.6.4 Subscriber Representations and Warranties

By accepting a SSP certificate issued by 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 Section 9.9;
- the certificate is being used exclusively for authorized and legal purposes, consistent with this CPS; and
- the Subscriber is an end-user and will not use the private key corresponding to any public key listed in the certificate for purposes of signing any certificate (or any other format of certified public key) or CRL.

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

Subscribers shall:

- Accurately represent themselves and ensure the accuracy of information provided in all communications with the SSP CA, RA, and/or TA;
- Protect their private keys at all times, in accordance with this CPS, and as set forth in the applicable Subscriber agreements;
- Prevent unauthorized disclosure of their private keys and activation data in accordance with Sections 6.2.4.2 and 6.2.8;
- Notify the 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;
- Abide by all the terms, conditions, and restrictions levied upon the use of their private keys and certificates;
- Agree not to monitor, interfere with, or reverse engineer the technical implementation of the 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.

9.6.5 Relying Party Representations and Warranties

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

- Perform a risk analysis to decide whether the level of assurance provided by the certificate is adequate to protect the Relying Party based upon the intended use;
- Use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension);
- Check each certificate for validity, using procedures described in the X.509 standard [ISO 9594-8], prior to reliance;
- Establish trust in the CA who issued a certificate by verifying the certification path in accordance with the guidelines set by the X.509 Version 3 Amendment; and

- Preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data. Note: data format changes associated with application upgrades may invalidate digital signatures and shall be avoided.

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

9.6.6 Representations and Warranties of Other Participants

9.6.6.1 PA Obligations

The Federal PA shall—

- Approve the CPS for each CA that issues certificates under this policy;
- Review periodic compliance audits to ensure that CAs are operating in compliance with their approved CPSes;
- Review name space control procedures to ensure that distinguished names are uniquely assigned for all certificates issued under the Federal Common Policy CP;
- Revise the CP to maintain the level of assurance and operational practicality;
- Publicly distribute the CP; and
- Coordinate modifications to the CP to ensure continued compliance by CAs operating under approved CPSes.

The Symantec PMA shall –

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

9.6.6.2 Agency PMA Obligations

The Agency PMA shall—

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

9.7 Disclaimers of Warranties

9.7.1 Specific Disclaimers

Except as otherwise set forth in this CPS, 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 "non-repudiation" for any Symantec certificate or any message (because non-repudiation is determined exclusively by law and the applicable final dispute resolution mechanism); and
c) Does not warrant the standards or performance of any hardware or software not under exclusive ownership of, exclusive control of, or licensed to Symantec.

See also Section 9.7.3 (Disclaimer of Fiduciary Relationship).

9.7.2 General Disclaimer

Except as set forth in this CPS and the applicable Subscriber Agreement, and to the extent permitted by applicable law, 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 Relationship

The Symantec SSP CA or RA 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

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

9.8.1 Limitations on Amount of Damages

In the event a Subscriber or Relying Party initiates any claim, action, suit, arbitration, or other proceeding separate from a request for payment under this CPS and to the extent permitted by applicable law, 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 SSP, its RAs or Trusted Agents in connection with a single transaction involving the use or reliance on a certificate shall be limited to one thousand dollars ($1,000 USD).

Furthermore, Symantec's total liability for any incident (aggregate of all transactions) involving the use or reliance on a certificate shall be limited to fifty thousand ($50,000 USD). These liability caps shall be the same regardless of the number of digital signatures, acts of authentication, or encrypted messages related to, or claims arising out of such transaction.

Notwithstanding the foregoing, to the extent 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 5.8.

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

Whenever any person hereto desires or is required to give any notice, demand, or request with respect to this CPS, such communication shall be made either using digitally signed messages consistent with the requirements

of this CPS, or in writing. Electronic communications shall be effective upon the sender's receiving a valid, digitally signed acknowledgment of receipt from the recipient. Such acknowledgment must be received within five (5) days, or else written notice must then be communicated. Communications in writing must be delivered by a courier service that confirms delivery in writing or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows:

To Symantec at:

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 of the 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 1.5 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 PA, an updated version of this document will be provided to the PA.

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

9.12.3 Circumstances under Which OID must be Changed

No stipulation.

9.13 Dispute Resolution Provisions

The PA shall facilitate the resolution between entities when conflicts arise as a result of the use of certificates issued under this policy. When the dispute is between Federal agencies, and the PA is unable to facilitate resolution, dispute resolution may be escalated to OMB or U.S. Department of Justice, Office of Legal Counsel as necessary.

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 ECA 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 and the MOA between Symantec and the PA shall be governed by the laws of the United States of America.

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

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

No stipulation.

9.16.2 Assignment

This CPS inures to the benefit of, and shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties. The rights and obligations detailed in this CPS are assignable by the parties, by operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with Section 5.8, concerning termination or cessation of CA operations; and provided further, that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

9.16.3 Severability

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

9.16.4 Merger

No term or provision of this CPS directly affecting the respective rights and obligations of 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 Federal Common Policy CP and this CPS, the Federal Common Policy CP shall take precedence over this CPS.

9.17.2 Interpretation

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

9.17.3 Headings and Appendices of this CPS

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

APPENDIX A: CERTIFICATE AND CRL FORMATS

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

APPENDIX B: DEFINITIONS

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

compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by NIST
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.
cryptographic module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.
crypto period	Time span during which each key setting remains in effect.
data integrity	Assurance that the data are unchanged from creation to reception
e-commerce	The use of network technology (especially the Internet) to buy or sell goods and services
Encryption (or confidentiality) certificate	A certificate containing a public key that is used to encrypt or decrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes. The process of storing protecting and escrowing the private component of the key pair associated with the encryption certificate is sometimes referred to as key management.
erroneous issuance	Issuance of a certificate not materially in accordance with the procedures required by the CPS, issuance of a certificate to a person other that the one named as the subject of the certificate, or issuance of a certificate without the authorization of the person named as the subject of such certificate.
firewall	Gateway that limits access between networks in accordance with local security policy.
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.
Legacy Federal PKI	A PKI implementation owned and managed by a Federal Agency and cross-certified with the Federal Bridge prior to 12/31/2005.
Local Registration Authority (LRA)	An RA with responsibility for a local community.
naming authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
National Security System	Any telecommunications or information system operated by the U.S. Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]

non-repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data.
Non-verified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization; the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI OIDs are used to uniquely identify each of the four policies and cryptographic algorithms supported.
Out-of-Band	Communication between parties using a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
PKI Sponsor	Fills the role of a Subscriber 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, (2) holds a private key that corresponds to a public key listed in that certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual, an application or network device. Current Subscribers possess valid CDS-issued certificates.
superior CA	In a hierarchical PKI, a CA who has certified the certificate signing key of another CA, and who constrains the activities of that CA. (see subordinate CA)
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 C: REFERENCES

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

Number	Title	Date
ABADSG	*Digital Signature Guidelines* http://www.abanet.org/scitech/ec/isc/dsgfree.html	1 August 1996
CCP-PROF	*X.509 Certificate and CRL Extensions Profile for the Shared Service Providers (SSP) Program* http://www.cio.gov/fpkipac/documents/CertCRLprofileForCP.pdf	
E-Auth	*E-Authentication Guidance for Federal Agencies, M-04-04*	16 December 2003
FIPS140	*Security Requirements for Cryptographic Modules* http://csrc.nist.gov/publications/index.html	21 May 2001
FIPS112	*Password Usage* http://csrc.nist.gov/	5 May 1985
FIPS186-3	*Digital Signature Standard* http://csrc.nist.gov/publications/drafts/fips_186-3/Draft_FIPS-186-3%20_November2008.pdf	March 2006
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	
NS4009	*NSTISSI 4009, National Information Systems Security Glossary*	January 1999
PACS	*Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems* http://smart.gov/information/TIG_SCEPACS_v2.2.pdf	27 July 2004
PKCS-1	*PKCS #1 v2.1: RSA Cryptography Standard* http://www.rsasecurity.com/rsalabs/node.asp?id=2125	14 June 2002
PKCS-12	*Personal Information Exchange Syntax Standard* http://www.rsasecurity.com/rsalabs/node.asp?id=2138	24 June 1999
SSPKRPS	*Key Recovery Practices Statement for Symantec SSP PKI Service*	
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
RFC3647	*Certificate Policy and Certification Practices Framework, Chokhani and Ford.* http://www.ietf.org/rfc/rfc3647.txt	November 2003
RFC 4122	*A Universally Unique IDentifier (UUID) URN Namespace, Paul J. Leach, Michael Mealling, and Rich Salz.* http://www.ietf.org/rfc/rfc4122.txt	July 2005
RFC 5280	*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*	May 2008
SP 800-73-3(1)	*Interfaces for Personal Identity Verification – Part 1: End-Point PIV Card Application Namespace, Data Model and Representation, NIST Special Publication 800-73-3.*	February 2010

APPENDIX D: ACRONYMS AND ABBREVIATIONS

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

REVISION HISTORY

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

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

		5.8	Clarified that notice shall be given prior to CA termination & continued support of issued certificates shall be performed in accordance with agreements.
		6.1.1.1 & 6.2.4.1	-Clarified dual controls & witnessing of CA key generation ceremonies. -Backup copies are created via secure cloning process during the key ceremony.
		6.1.6	Public key parameters are generated in accordance with FIPS186.
		6.2.1	Removed VeriSign smart card issuance system (not provided by VeriSign).
		6.2.2	Changed from 12 to 16 shares.
		6.2.4.2 & 6.2.4.3	Backup of Key Management (ie, Encryption) Private key is moved to new section (6.2.4.3). Signature keys are not escrowed but Encryption keys are. Storage of backup copies ensure security is consistent with the protection provided by the Subscriber's crypto module.
		6.3.2	-Corrected: CA key pair usage period from 6 yrs to max of 10 yrs & generation period from 3 yrs to 4 yrs. Subscriber cert max usage is 3 yrs. -Added: usage periods for certs asserting the PIV-contentSigning extension to max usage of 8 yrs for public keys & max of 3 yrs for private keys.
		6.6.2	-Changed name of CBO to PKI Ops -corrected delivery packaging from tamper-resistant to tamper-evident. -corrected delivery services (removed 'registered mail & constant surveillance courier')
		6.7	Added secure comms between the KMS & KMD & SSP
		7.1.3	Added ECC algorithms
		7.1.5	RAs are limited to the jurisdictional name space assigned
		8.1	Added annual audit requirement for the Agency.
		9.1.1	Correction: VeriSign is entitled to charge fees (but removed the statement that we publish our fees on our website).
		9.4.1, 9.4.3	Added description of our privacy practices for compliance with policy
		9.6.2	Added missing responsibility – the RA performs in-person identity verification
		9.6.4	Added missing responsibility – the Subscriber shall prevent disclosure of their private keys & activation data.
		9.6.6.1	Added missing responsibility – the PA shall provide notifications in the event of disaster, compromise or termination.
		9.10.1 & 9.10.3	-the term of the CPS extends through the end of the archive period -corrected section reference #'s of obligations that survive termination of the CA.
		9.13.2, 9.14 & 9.15	Governing law & dispute resolution changed from Santa Clara CA to Virginia (in effect under the legacy owner, VeriSign – the next revision will correct this for the new owner, Symantec)
		Appx B, C & D	Corrected definitions, acronyms & references as required
1.13.1	12 Nov 2010	Convert to RFC3647 sequence	
1.13.1	30 March 2010	Maintenance updates: **Sections:**	**Description**:
		1.1, 1.3.2.1, 1.3.5.2, 5.1.1, 5.7.1	Updated location of Primary Facility from MV to Delaware & DRF from Virginia to CA.
		1.3.2.1	RAs are no longer co-located with Primary site.
		5.1.1	-Removed reference to Army regs 389-5 -Removed 'metal-clad construction' of perimeter doors.
		6.7	-Changed security monitoring tools to: Bladelogic, security audit scripts, Qualys, Sourcefire, Win-based virus scanners. -Changed firewall to: Checkpoint NGX-R55 and NGX-R62 -Changed primary IDS to: NS2000 and 3D2100 IDS appliances running OS version 4.8.02, with RNA enabled
		6.5.1 & 6.5.2	-Changed to Sun Solaris 8 (eval'd to EAL-4) & Oracle 10 (eval'd to EAL-4). -Removed EAL-4 certification of the VeriSign CA
1.13	Ready for submission to EPMA Review after upcoming release of Common Policy		
	12 Nov, 2009 – PWG Approval	This CPS replaces Version 1.12 dated March 10, 2008 to reflect the changes to the VeriSign PKI infrastructure resulting from planned evolution and internal compliance monitoring.	

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