

# **VeriSign Shared Service Provider**

## **Certification Practice Statement**

(Portions of this Document Have Been Redacted)

**Version 1.1**

**5 Feb 2007**



**VeriSign, Inc.  
487 East Middlefield Road  
Mountain View, CA 94043  
+1 650.961.7500  
<http://www.verisign.com>**

## **VeriSign Shared Service Provider (SSP) Certification Practice Statement**

© 2006 VeriSign, Inc. All rights reserved.

Printed in the United States of America.

Revision Date: 5 Feb 2007

### **Trademark Notices**

VeriSign is a registered trade mark of VeriSign, Inc. The VeriSign logo is a trademark and service mark of VeriSign, Inc. Other trademarks and service marks in this document are the property of their respective owners.

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

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

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

VeriSign, Inc.  
487 East Middlefield Road  
Mountain View, CA 94043 USA  
Attn: Practices Development.  
Tel: +1 650.961.7500  
Fax: +1-650-335-1077  
SSP-practices@verisign.com

## TABLE OF CONTENTS

<b>1. INTRODUCTION.....</b>	<b>1</b>
1.1 OVERVIEW .....	1
1.2 POLICY IDENTIFICATION .....	2
1.3 COMMUNITY AND APPLICABILITY .....	3
1.3.1 PKI Authorities .....	3
1.3.1.1 PKI Policy Authority .....	3
1.3.1.2 Agency Policy Management Authority .....	3
1.3.1.3 Certification Authority (CA).....	3
1.3.1.4 Registration Authority (RA) .....	4
1.3.1.5 Related Authorities .....	4
1.3.1.6 Trusted Agent .....	4
1.3.2. End Entities .....	5
1.3.2.1 Subscribers.....	5
1.3.2.2 Relying Parties.....	5
1.3.3 Applicability .....	5
1.4 CONTACT DETAILS.....	6
1.4.1 Specification Administration Organization .....	6
1.4.2 Contact Persons.....	6
1.4.3 Person Determining CPS Suitability for the Policy.....	6
<b>2. GENERAL PROVISIONS .....</b>	<b>7</b>
2.1 OBLIGATIONS .....	7
2.1.1 PA Obligations .....	7
2.1.2 Agency PMA Obligations .....	8
2.1.3 CA Obligations .....	8
2.1.4 RA Obligations .....	8
2.1.5 Trusted Agent Obligations.....	8
2.1.6 Subscriber Obligations .....	9
2.1.7 Relying Party Obligations .....	9
2.1.8 Repository Obligations.....	10
2.2 LIABILITY .....	10
2.2.1 Warranties and Limitations on Warranties .....	10
2.2.1.1 Certificate Authority Warranties.....	10
2.2.1.2 Subscribers' Representations .....	11
2.2.2 Disclaimers of Warranty and Liability .....	11
2.2.2.1 Specific Disclaimers .....	11
2.2.2.2 General Disclaimer .....	12
2.2.3 Limitations of Liability .....	12
2.2.3.1 Limitations on Amount of Damages .....	12
2.2.3.2 Exclusion of Certain Elements of Damages.....	12
2.3 FINANCIAL RESPONSIBILITY.....	12
2.3.1 Subscriber's Liability and Indemnity.....	13
2.3.2 Fiduciary Relationships.....	13
2.3.3 Administrative Processes.....	13
2.4 INTERPRETATION AND ENFORCEMENT .....	13
2.4.1 Interpretation.....	13
2.4.1.1 Governing Law .....	13
2.4.1.2 Conflict of Provisions .....	14
2.4.1.3 Interpretation .....	14
2.4.1.4 Headings and Appendices of this CPS.....	14
2.4.2 Severability, Survival, Merger, and Notice.....	14
2.4.2.1 Severability .....	14
2.4.2.2 Survival.....	14
2.4.2.3 Merger .....	14
2.4.2.4 Notice .....	14

2.4.3	<i>Dispute Resolution Procedures and Choice of Forum</i> .....	15
2.4.3.1	<i>Notification Among Parties to a Dispute</i> .....	15
2.4.3.2	<i>Formal Dispute Resolution</i> .....	15
2.4.4	<i>Successors and Assigns</i> .....	16
2.4.5	<i>No Waiver</i> .....	16
2.4.6	<i>Compliance with Export Laws and Regulations</i> .....	16
2.4.7	<i>Choice of Cryptographic Methods</i> .....	16
2.4.8	<i>Force Majeure</i> .....	17
2.5	<b>FEES</b> .....	17
2.5.1	<i>Certificate Issuance or Renewal Fees</i> .....	17
2.5.2	<i>Certificate Access Fees</i> .....	17
2.5.3	<i>Revocation or Status Information Access Fees</i> .....	17
2.5.4	<i>Fees for Other Services</i> .....	17
2.5.5	<i>Refund Policy</i> .....	17
2.6	<b>PUBLICATION AND REPOSITORIES</b> .....	17
2.6.1	<i>Publication of CA Information</i> .....	17
2.6.2	<i>Frequency of Publication</i> .....	18
2.6.3	<i>Access Controls</i> .....	18
2.6.4	<i>Repositories</i> .....	18
2.7	<b>COMPLIANCE AUDIT</b> .....	19
2.7.1	<i>Frequency of Compliance Audit</i> .....	19
2.7.2	<i>Identity/Qualifications of Reviewer</i> .....	19
2.7.3	<i>Auditor's Relationship to Audited Party</i> .....	19
2.7.4	<i>Topics Covered by Compliance Audit</i> .....	19
2.7.5	<i>Actions Taken as a Result of Deficiency</i> .....	19
2.7.6	<i>Communication of Results</i> .....	20
2.8	<b>CONFIDENTIALITY</b> .....	20
2.8.1	<i>Types of Information to Be Kept Confidential</i> .....	20
2.8.2	<i>Information Release Circumstances</i> .....	20
2.9	<b>INTELLECTUAL PROPERTY RIGHTS</b> .....	20
<b>3.</b>	<b>IDENTIFICATION AND AUTHENTICATION</b> .....	<b>22</b>
3.1	<b>INITIAL REGISTRATION</b> .....	22
3.1.1	<i>Types of Names</i> .....	22
3.1.1.1	<i>Internet Domain Component Name</i> .....	23
3.1.1.2	<i>Need for Names to be Meaningful</i> .....	24
3.1.1.3	<i>Rules for Interpreting Various Name Forms</i> .....	25
3.1.1.4	<i>Uniqueness of Names</i> .....	25
3.1.1.5	<i>Name Claim Dispute Procedure</i> .....	25
3.1.1.6	<i>Recognition, authentication, and role of trademarks</i> .....	25
3.1.1.7	<i>Method to prove possession of private key</i> .....	25
3.1.1.8	<i>Authentication of CA Certificate Issuance</i> .....	26
3.1.1.9	<i>Authentication of Individual Identity</i> .....	26
3.1.1.10	<i>Authentication of Component Identities</i> .....	29
3.2	<b>CERTIFICATE RENEWAL, UPDATE, AND ROUTINE RE-KEY</b> .....	29
3.2.1	<i>Certificate Renewal</i> .....	29
3.2.2	<i>Certificate Re-key</i> .....	29
3.2.3	<i>Certificate update</i> .....	30
3.3	<b>RE-KEY AFTER REVOCATION</b> .....	30
3.4	<b>REVOCATION REQUEST</b> .....	30
<b>4.</b>	<b>OPERATIONAL REQUIREMENTS</b> .....	<b>32</b>
4.1	<b>CERTIFICATE APPLICATION</b> .....	32
4.1.1	<i>Delivery of Subscriber's Public Key to Certificate Issuer</i> .....	33
4.2	<b>CERTIFICATE ISSUANCE</b> .....	33
4.2.1	<i>Delivery of Subscriber's Private Key to Subscriber</i> .....	34

- 4.2.2 CA Public Key Delivery to Users ..... 34
- 4.3 CERTIFICATE ACCEPTANCE ..... 35
- 4.4 CERTIFICATE SUSPENSION AND REVOCATION ..... 35
  - 4.4.1 Revocation ..... 35
    - 4.4.1.1 Circumstances for Revocation ..... 35
    - 4.4.1.2 Who Can Request Revocation ..... 36
    - 4.4.1.3 Procedure for Revocation Request ..... 36
    - 4.4.1.4 Revocation Request Grace Period ..... 37
  - 4.4.2 Suspension ..... 37
  - 4.4.3 Certificate Revocation Lists ..... 37
    - 4.4.3.1 CRL Issuance Frequency ..... 37
  - 4.4.4 Online Status Checking ..... 37
  - 4.4.5 Other Forms of Revocation Advertisements Available ..... 38
  - 4.4.6 Checking Requirements for Other Forms of Revocation Advertisements ..... 38
  - 4.4.7 Special Requirements Regarding Key Compromise ..... 38
- 4.5 SECURITY AUDIT /AUDIT LOGGING PROCEDURES ..... 38
  - 4.5.1 Types of Events Recorded ..... 38
  - 4.5.2 Frequency of Processing Log ..... 39
  - 4.5.3 Retention Period of Audit Log ..... 39
  - 4.5.4 Protection of Audit Log ..... 39
  - 4.5.5 Audit Log backup Procedures ..... 40
  - 4.5.6 Audit Collection System ..... 40
  - 4.5.7 Notification to Event-Causing Subject ..... 40
  - 4.5.8 Vulnerability Assessments ..... 40
- 4.6 RECORDS ARCHIVAL ..... 41
  - 4.6.1 Types of Data/Records Archived ..... 41
  - 4.6.2 Retention Period for Archive ..... 42
  - 4.6.3 Protection of Archive ..... 42
  - 4.6.4 Archive Backup Procedures ..... 42
  - 4.6.5 Requirements for Time-Stamping of Records ..... 42
  - 4.6.6 Procedures to Obtain and Verify Archive Information ..... 42
- 4.7 KEY CHANGEOVER ..... 42
- 4.8 COMPROMISE AND DISASTER RECOVERY ..... 43
  - 4.8.1 Computing Resources, Software, and or Data are Corrupted ..... 43
  - 4.8.2 CA Cannot Generate CRLs ..... 43
  - 4.8.3 CA Signature Keys are Compromised ..... 43
  - 4.8.4 Secure Facility Impaired after a natural or Other Type of Disaster ..... 44
- 4.9 CA TERMINATION ..... 44
- 5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS ..... 45**
  - 5.1 PHYSICAL CONTROLS ..... 45
    - 5.1.1 Site Location and Construction ..... 45
    - 5.1.2 Physical Access ..... 45
    - 5.1.3 Electric Power and Air Conditioning ..... 45
    - 5.1.4 Water Exposure ..... 45
    - 5.1.5 Fire Prevention and Protection ..... 45
    - 5.1.6 Media Storage ..... 46
    - 5.1.7 Waste Disposal ..... 46
    - 5.1.8 Off-Site Backup ..... 46
  - 5.2 PROCEDURAL CONTROLS ..... 46
    - 5.2.1 Trusted Roles ..... 46
      - 5.2.1.1 Administrator ..... 46
      - 5.2.1.2 Officer ..... 46
      - 5.2.1.3 Auditor ..... 46
      - 5.2.1.4 Operator ..... 46
      - 5.2.1.5 Trusted Agent ..... 46
      - 5.2.1.6 PKI Sponsor ..... 46

5.2.2 Separation of Roles.....	46
5.2.3 Identification and Authentication for Each Role .....	46
5.3 PERSONNEL CONTROLS .....	46
5.3.1 Background, Qualifications, Experience and Clearance Requirements.....	46
5.3.2 Background Check Procedures .....	47
5.3.3 Training Requirements .....	47
5.3.4 Retraining Frequency and Requirements .....	47
5.3.5 Job Rotation Frequency and Sequence.....	47
5.3.6 Sanctions for Unauthorized Actions .....	48
5.3.7 Contracting Personnel Requirements.....	48
5.3.8 Documentation Supplied to Personnel .....	48
<b>6. TECHNICAL SECURITY CONTROLS.....</b>	<b>49</b>
6.1 KEY PAIR GENERATION AND INSTALLATION.....	49
6.1.1 Key Pair Generation.....	49
6.1.1.1 CA Key Pair Generation .....	49
6.1.1.2 Subscriber Key Pair Generation.....	49
6.1.2 Private Key Delivery to Subscriber .....	49
6.1.3 Public Key Delivery to Certificate Issuer.....	50
6.1.4 CA Public Key Delivery to Relying Parties .....	50
6.1.5 Key Sizes and Signature Algorithms.....	50
6.1.6 Public Key Parameters .....	51
6.1.7 Parameter Quality Checking.....	51
6.1.8 Hardware/Software Key Generation .....	51
6.1.9 Key Usage Purposes.....	51
6.2 PRIVATE KEY PROTECTION .....	52
6.2.1 Standards for cryptographic modules .....	52
6.2.2 Private Key Multi-person Control.....	53
6.2.3 Private Key Escrow .....	53
6.2.4 Private Key backup.....	53
6.2.4.1 Backup of CA Private Signature Key .....	53
6.2.4.2 Backup of Subscriber Private Keys .....	53
6.2.5 Private Key Archival .....	53
6.2.6 Private Key entry into cryptographic module.....	53
6.2.7 Method of Activating Private Key.....	54
6.2.8 Method of Deactivating Private Key .....	54
6.2.9 Method of Destroying Private Key .....	54
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT .....	54
6.3.1 Public Key Archival.....	54
6.3.2 Usage Periods for the Public and Private Keys .....	55
6.4 ACTIVATION DATA.....	55
6.4.1 Activation data generation and installation .....	55
6.4.2 Activation data protection .....	55
6.4.3 Other aspects of activation data .....	55
6.5 COMPUTER SECURITY CONTROLS .....	55
6.5.1 Specific computer security technical requirements .....	55
6.5.2 Computer security rating.....	55
6.6 LIFE CYCLE TECHNICAL CONTROLS.....	55
6.7 NETWORK SECURITY CONTROLS.....	56
6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS .....	56
<b>7. CERTIFICATE AND CRL PROFILES .....</b>	<b>57</b>
7.1 CERTIFICATE PROFILE .....	57
7.1.1 Version Numbers .....	57
7.1.2 Certificate Extensions.....	57
7.1.3 Algorithm Object Identifiers.....	57

7.1.4 Name Forms ..... 57

7.1.5 Name Constraints ..... 57

7.1.6 Certificate Policy Object Identifier ..... 58

7.1.7 Usage of Policy Constraints ..... 58

7.1.8 Policy Qualifiers Syntax and Semantics ..... 58

7.1.9 Processing Semantics for the Critical Certificate Policy Extension..... 58

7.1.10 Key Usage Constraints for id-fpki-common-authentication ..... 58

7.2 CRL PROFILE ..... 58

7.2.1 Version numbers ..... 58

7.2.2 CRL and CRL Entry Extensions ..... 58

**8. SPECIFICATION ADMINISTRATION..... 59**

8.1 SPECIFICATION CHANGE PROCEDURES..... 59

8.2 PUBLICATION AND NOTIFICATION PROCEDURES ..... 59

8.3 CPS APPROVAL PROCEDURES ..... 59

8.4 CPS WAIVERS ..... 59

**APPENDIX A: CERTIFICATE AND CRL FORMATS ..... 60**

**APPENDIX B: DEFINITIONS..... 61**

**APPENDIX C: REFERENCES ..... 66**

**APPENDIX D: ACRONYMS AND ABBREVIATIONS ..... 67**

# 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. VeriSign is an approved Shared Service Provider operating under a Memorandum of Agreement (MOA) signed by the Federal PKI Policy Authority (PA). The VeriSign SSP Certificate Practices Statement (CPS) and associated Compliance Audit have been approved by the PA. The VeriSign SSP PKI is also certified as an approved service by the GSA FIPS 201 Evaluation Program.

This VeriSign SSP Certification Practice Statement (CPS) in conjunction with the X.509 Certificate Policy for the Common Policy Framework (CP) defines the practices that VeriSign will employ in issuing and managing certificates and in maintaining a certificate-based public key infrastructure (PKI) for the SSP..

## 1.1 Overview

This CPS is the statement of practices that VeriSign will employ when issuing digital certificates as an approved SSP. This CPS is structured in accordance with RFC 2527 of the Internet Engineering Task Force (IETF). The VeriSign SSP PKI service offering provides complete certificate life-cycle support and certificate repository services for approved entities.

VeriSign 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 VeriSign SSP CA. The architecture and functional solution for the VeriSign SSP offering is based on VeriSign’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 VeriSign SSP CA primary location is at the VeriSign data center located in Mountain View, California. A disaster recovery site with full backup and data mirroring is located in Virginia. All customer transactions are copied between the primary and disaster recovery systems in real-time over a secure VPN connection.

Authorized VeriSign 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 VeriSign SSP PKI are Federal employees, contractors and affiliates needing access to Federal facilities and IT systems. The VeriSign 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.

## 1.2 Policy Identification

This CPS describes VeriSign's practices for SSP PKI services delivered in accordance with the CP. The CP includes six distinct certificate policies: a policy for user with software cryptographic modules, a policy for users with hardware cryptographic modules, a policy for devices, a high assurance user policy, a user authentication policy, and a card authentication policy. Certificates issued by the VeriSign 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-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-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-devices ::= {2 16 840 1 101 3 2 1 3 8}

For devices 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). 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). 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 devices under this policy shall include the id-fpki-common-devices. Certificates issued to users supporting authentication but not digital signature may contain id-fpki-common-authentication. Certificates issued to users supporting authentication where the private key can be used without user authentication may contain id-fpki-common-cardAuth. 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).

## **1.3 Community and Applicability**

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.

### **1.3.1 PKI Authorities**

#### **1.3.1.1 PKI Policy Authority**

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 maintaining the CP, approving the CPS and Compliance Audit for each CA that issues certificates under the CP.

#### **1.3.1.2 Agency Policy Management Authority**

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 3.1.5). This body shall be referred to as an Agency Policy Management Authority, or Agency PMA.

#### **1.3.1.3 Certification Authority (CA)**

The VeriSign 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 VeriSign 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 VeriSign SSP CA. The VeriSign SSP CA issues all end-entity certificates within the VeriSign SSP domain.

The VeriSign 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 Registration Authority (RA)**

VeriSign personnel and designated Federal Agency personnel will perform the RA functions for the VeriSign SSP. VeriSign RA personnel are co-located with the SSP CA at the VeriSign secure data facility in Mountain View, CA. The RA may rely on an in-person identity validation process performed by a Trusted Agent. VeriSign 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.

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

VeriSign may appoint Agency RAs to perform RA functions on behalf of employees and affiliates of their Agency. An Agency RA is an employee of an Agency that has entered into a contract with VeriSign for SSP PKI services. The Agency RA will be bound by contract to comply with the requirements of the CP and this CPS. Agency RA personnel will be issued public key certificates to enable secure authenticated access to the SSP. The Agency RA certificate is stored on a FIPS 140 Level 2 hardware token.

#### **1.3.1.5 Related Authorities**

##### **1.3.1.5.1 Compliance Auditor**

VeriSign retains the services of an independent security auditing firm, (e.g. KPMG), which conducts a yearly examination of the controls associated with VeriSign's operations as set forth in VeriSign'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 Statement of Auditing Standards (SAS) 70 and the WebTrust for CA guidelines. The VeriSign SSP CPS is based on its existing commercial practices and controls. As such, the yearly independent SAS 70 and WebTrust for CA audits provide the assurance of VeriSign's compliance with the SSP CPS.

##### **1.3.1.5.2 Repository**

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

#### **1.3.1.6 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 VeriSign 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.

## **1.3.2. End Entities**

### **1.3.2.1 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.

### **1.3.2.2 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.

## **1.3.3 Applicability**

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.

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.

## **1.4 Contact Details**

### **1.4.1 Specification Administration Organization**

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

VeriSign, Inc.  
487 East Middlefield Road  
Mountain View, CA 94043 USA  
Attn: Practices Development – CPS  
+1 650-961-7500 (voice)  
+1-650-335-1077 (fax)  
[SSP-practices@verisign.com](mailto:SSP-practices@verisign.com)

### **1.4.2 Contact Persons**

Parties having questions as to the content, applicability, or interpretation of this CPS may address their comments to:

Nicholas Piazzola  
VeriSign, Inc.  
605 Shipley Road  
Linthicum, MD 21090  
410-691-2100  
[npiazzola@verisign.com](mailto:npiazzola@verisign.com)

### **1.4.3 Person Determining CPS Suitability for the Policy**

The Federal Policy Authority (PA) determines the suitability of the VeriSign SSP CPS and its compliance with the Federal Common Policy CP.

## 2. GENERAL PROVISIONS

This Section sets forth general provisions of obligations and defines and allocates specific responsibilities among the various parties participating in the PKI described in this CPS. These parties are:

- Policy Authority
- Policy Management Authority
- Certification Authority
- Registration Authority
- Trusted Agent
- Subscriber
- Relying Party
- Repository

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.

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

### 2.1 *Obligations*

#### 2.1.1 PA Obligations

The 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.

### **2.1.2 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 their approved CPSes; and
- Review name space control procedures to ensure that distinguished names are uniquely assigned within their agency.

### **2.1.3 CA Obligations**

The VeriSign 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 2.1.6; and
- Operating or providing for the services of an online repository that satisfies the obligations under Section 2.1.8, and informing the repository service provider of their obligations if applicable.

### **2.1.4 RA Obligations**

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

- 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 2.1.3, and that Subscribers are informed of the consequences of not complying with those obligations.

### **2.1.5 Trusted Agent Obligations**

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

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

- Performing in-person identify verification of certificate applicants in accordance with Section 3.1.9;
- 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 2.1.3, and that Subscribers are informed of the consequences of not complying with those obligations.

### **2.1.6 Subscriber Obligations**

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;
- Notify the VeriSign 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 VeriSign SSP except as explicitly permitted by this CPS or upon written approval by VeriSign; and
- Agree not to submit to VeriSign or the VeriSign 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.

### **2.1.7 Relying Party Obligations**

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

### **2.1.8 Repository Obligations**

The VeriSign 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 VeriSign SSP Repository. Therefore, the VeriSign SSP Repository provides unrestricted read-only access to subscribers, relying parties, and other interested parties. The VeriSign repository is accessible via methods described in Section 2.6.4. VeriSign may replicate certificates and CRLs in additional repositories for performance enhancement. Such repositories may be operated by VeriSign or other parties (e.g. Federal agencies).

## **2.2 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.

### **2.2.1 Warranties and Limitations on Warranties**

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.

#### **2.2.1.1 Certificate Authority Warranties**

VeriSign, warrants to Subscribers that:

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

VeriSign 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
- VeriSign has materially complied with the CPS when issuing the Certificate.

### **2.2.1.2 Subscribers' Representations**

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

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

## **2.2.2 Disclaimers of Warranty and Liability**

### **2.2.2.1 Specific Disclaimers**

Except as otherwise set forth in this CPS, VeriSign:

- 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 VeriSign's liability in tort for negligent, reckless, or fraudulent conduct;
- b) Does not warrant "nonrepudiation" for any VeriSign certificate or any message (because nonrepudiation is determined exclusively by law and the applicable final dispute resolution mechanism); and

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

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

### **2.2.2.2 General Disclaimer**

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

## **2.2.3 Limitations of Liability**

### **2.2.3.1 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, VeriSign's liability shall be limited as follows:

The total liability of VeriSign to any party for general contract, tort or any other damages for negligent, reckless, or fraudulent conduct by the VeriSign 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, VeriSign'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.

### **2.2.3.2 Exclusion of Certain Elements of Damages**

Except as expressly provided in this CPS, and to the extent permitted by applicable law, VeriSign 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 VeriSign has been advised of the possibility of such damages.

To the extent permitted by applicable law, VeriSign 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.

## **2.3 Financial Responsibility**

VeriSign 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. VeriSign also maintains professional liability insurance.

### **2.3.1 Subscriber's Liability and Indemnity**

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 VeriSign 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 VeriSign 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 VeriSign 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.

### **2.3.2 Fiduciary Relationships**

The VeriSign SSP CA or RA is not the agent, fiduciary, trustee, or other representative of subscribers or relying parties. The relationship between VeriSign and Subscribers and that between VeriSign and relying parties is not that of agent and principal. Neither Subscribers nor relying parties have any authority to bind VeriSign, by contract or otherwise, to any obligation. VeriSign shall make no representations to the contrary, either expressly, implicitly, by appearance, or otherwise.

### **2.3.3 Administrative Processes**

An annual report of VeriSign can be obtained by submitting a written request to the address specified in section 1.4. VeriSign's financial resources are set forth in disclosures appearing at: <http://corporate.verisign.com/investor/sec-filings.html>

## ***2.4 Interpretation and Enforcement***

### **2.4.1 Interpretation**

#### ***2.4.1.1 Governing Law***

The relationship between this CPS and the CP and the MOA between VeriSign 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.

#### **2.4.1.2 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.

#### **2.4.1.3 Interpretation**

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

#### **2.4.1.4 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.

### **2.4.2 Severability, Survival, Merger, and Notice**

#### **2.4.2.1 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.

#### **2.4.2.2 Survival**

The obligations and restrictions contained within CPS § 2.7 (Audit), 2.8 (Confidential Information), CPS §§ 2.2.2, 2.2.3 (Disclaimers of Warranty and Limitations of Liability), and CPS § 2.4 (Interpretation and Enforcement) shall survive the termination of this CPS.

#### **2.4.2.3 Merger**

No term or provision of this CPS directly affecting the respective rights and obligations of VeriSign 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.

#### **2.4.2.4 Notice**

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 VeriSign:

VeriSign, Inc.  
487 East Middlefield Road  
Mountain View, CA 94043 USA  
Attn: Certification Services  
(+1 650-961-8820)

By VeriSign to another person:

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

### **2.4.3 Dispute Resolution Procedures and Choice of Forum**

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.

#### **2.4.3.1 Notification Among Parties to a Dispute**

Before invoking any dispute resolution mechanism (including litigation or arbitration, as detailed below) with respect to a dispute involving any aspect of this CPS or a certificate issued by VeriSign under this CPS, aggrieved persons shall notify VeriSign and any other party to a dispute for the purpose of seeking dispute resolution among themselves.

#### **2.4.3.2 Formal Dispute Resolution**

If you are an individual or entity within the United States Government, this CPS, 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, and if negotiations do not resolve the dispute, an aggrieved person may invoke a dispute resolution mechanism as follows. Nothing in CPS § 2.4.3.2 shall preclude VeriSign from seeking equitable (including injunctive) relief upon alleged compromise or alleged material breach in a manner consistent with governing law and this CPS. Disputes involving federal government entities shall be resolved in accordance with applicable federal law. Otherwise, disputes shall be resolved in accordance with CPS § 2.4.3.2(i)-(ii).

(i) When each indispensable party to a dispute is a Canadian or U.S. resident or organization situated or doing business in Canada or the United States except where each indispensable party to a dispute agrees to an alternative dispute resolution mechanism (such as arbitration), all suits to enforce any provision of this CPS or arising in connection with the CPS or any related business relationship between the parties hereto shall be brought in the United States District Court for the

Northern District of California or the Superior or Municipal Court in and for the County of Santa Clara, California, U.S.A. Each person hereby agrees that such courts shall have exclusive in personam jurisdiction and venue with respect to such person and each person hereby submits to the exclusive in personam jurisdiction and venue of such courts. The parties hereby waive any right to a jury trial regarding any action brought in connection with this CPS. Where an alternative dispute resolution is chosen by the parties, California law shall govern arbitability and procedure.

(ii) Where one or more parties to a dispute is not a Canadian or U.S. resident or organization situated or doing business in Canada or the United States. All disputes arising in connection with the CPS shall be finally settled under the Rules of Conciliation and Arbitration of the International Chamber of Commerce (ICC) modified as necessary to reflect the provisions herein by one or more arbitrators. The place of arbitration shall be in New York or San Francisco, U.S.A., and the proceedings shall be conducted in English. In cases involving a single arbiter, that single arbiter shall be appointed by mutual agreement of the parties. If the parties fail to agree on an arbiter within fifteen (15) days, the ICC shall choose an arbiter knowledgeable in computer software law, information security, and cryptography or otherwise having special qualifications in the field, such as a lawyer, academician, or judge in a common law jurisdiction.

#### **2.4.4 Successors and Assigns**

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

#### **2.4.5 No Waiver**

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.

#### **2.4.6 Compliance with Export Laws and Regulations**

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

#### **2.4.7 Choice of Cryptographic Methods**

All persons acknowledge that they (not VeriSign) 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.

## **2.4.8 Force Majeure**

VeriSign 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.

## **2.5 Fees**

### **2.5.1 Certificate Issuance or Renewal Fees**

VeriSign will publish its fees for SSP certificates on its web site at <http://www.verisign.com/>. Such fees are subject to change seven (7) days following their posting.

### **2.5.2 Certificate Access Fees**

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

### **2.5.3 Revocation or Status Information Access Fees**

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

### **2.5.4 Fees for Other Services**

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

### **2.5.5 Refund Policy**

The VeriSign 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 VeriSign 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 VeriSign revoke the certificate and provide a refund if VeriSign 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 VeriSign's refund policy at <http://www.verisign.com/repository/refund>. This refund policy is not an exclusive remedy and does not limit other remedies that may be available to Subscribers.

## **2.6 Publication and Repositories**

### **2.6.1 Publication of CA Information**

The VeriSign SSP will operate an online Repository available to Subscribers and Relying Parties. This Repository will contain or provide access to the following minimum information:

1. All valid and un-expired VeriSign SSP Certificates;
2. Certificate status information, including revocation;
3. The most recently issued CRL;

4. The VeriSign SSP certificate(s) needed to validate the signature on VeriSign SSP subscriber certificates;
5. Any other relevant information the VeriSign SSP considers relevant regarding the use of VeriSign SSP certificates by its subscribers or relying parties; and
6. A copy of the X.509 Certificate Policy for the Common Policy Framework and an abridged version of this CPS including at least the following topics covered under the CP:
  - Section 1.4, SSP Contact Information;
  - Section 2, General Provisions;
  - Section 3.1, Initial Registration;
  - Section 4.4, Certificate Suspension and Revocation;
  - Section 8, 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 VeriSign SSP CPS is considered VeriSign Proprietary information.

### **2.6.2 Frequency of Publication**

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

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

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

CRLs will be created and published as described in Section 4.4.3.1.

### **2.6.3 Access Controls**

The VeriSign 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 and LDAP queries.

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

### **2.6.4 Repositories**

The VeriSign SSP Repository is implemented using LDAP technology. End users may search for SSP certificates or CRLs using http queries or the LDAP protocol. The VeriSign repository is accessible via http query and LDAP query.

## **2.7 Compliance Audit**

### **2.7.1 Frequency of Compliance Audit**

The VeriSign SSP 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.

### **2.7.2 Identity/Qualifications of Reviewer**

The VeriSign SSP auditor is the same professional auditing firm responsible for conducting VeriSign's commercial PKI audit. The VeriSign SSP auditor is intimately familiar with VeriSign's practices and policies, as it has been performing these services for VeriSign 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.

### **2.7.3 Auditor's Relationship to Audited Party**

The VeriSign SSP auditor is under a contractual relationship to VeriSign for its security audit services and has no role or responsibility relating to the VeriSign SSP operation. The Federal agency PMA is responsible for identifying and engaging a qualified auditor of Agency operations implementing aspects of this CPS.

### **2.7.4 Topics Covered by Compliance Audit**

The Compliance Audit shall verify that VeriSign 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 VeriSign CA/RA operations shall be subject to compliance audit inspections.

### **2.7.5 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 notify the parties identified in Section 2.7.6 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 or RA, to revoke a certificate issued.

## 2.7.6 Communication of Results

The compliance auditor shall report the results of a compliance audit to VeriSign. After 30 days, the Audit Compliance report and identification of corrective measures taken or being taken by the CA or RA shall be provided to both the PA and (where applicable) the Agency PMA. A special compliance audit may be required to confirm the implementation and effectiveness of the remedy.

## 2.8 Confidentiality

### 2.8.1 Types of Information to Be Kept Confidential

All non-certificate information received from Subscribers shall be treated as confidential by the VeriSign SSP and shall not be posted in the VeriSign repository. This information including: Dun and Bradstreet numbers, business or home addresses, telephone numbers and credit card data shall be handled as sensitive. This information will be stored locally on the SSP equipment and access will be limited to authorized personnel using certificate-based access control over SSL.

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

### 2.8.2 Information Release Circumstances

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

## 2.9 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 VeriSign SSP. VeriSign licenses relying parties to use certificates and CRLs.
- CPS: This CPS is personal property of VeriSign, Inc.
- Distinguished Names: Distinguished names are the personal property of the persons named (or their employer or principal).
- Subscriber Private Keys: Subscriber private keys are the personal property of the subscribers who rightfully use or are capable of using them (or their employer or principal), regardless of the physical medium within which they are stored or protected.
- Subscriber Public Keys: Subscriber public keys are the personal property of subscribers (or their employers or principal), regardless of the physical medium within which they are stored or protected.
- VeriSign Private Keys: VeriSign SSP private keys are the personal property of VeriSign, Inc.

- VeriSign Public Keys: VeriSign SSP public keys are the property of VeriSign Inc. VeriSign licenses relying parties to use such keys.

## 3. IDENTIFICATION AND AUTHENTICATION

### 3.1 Initial Registration

#### 3.1.1 Types of Names

For certificates issued by the VeriSign SSP for id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-High, and id-fpki-common-devices, 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.

For certificates issued under id-fpki-common-authentication, assignment of X.500 distinguished names is optional. If assigned, distinguished names 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. 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. If included, the subject distinguished name shall take the following form:

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

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. Device names may take the following forms:

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

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.

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

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

C=US, [o=department], [ou=agency]

New implementations shall assign names in the following directory 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. In the last form, dnQualifier is an integer value that makes the name unique. 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

Legacy implementations which predate this policy may use the directory tree:

C=US, [o=department], [ou=agency]

Common name fields shall be populated as specified above.

### **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]

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

VeriSign 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 CP 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 3280, even if the subject's name is not meaningful.

### **3.1.3 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].

### **3.1.4 Uniqueness of Names**

The VeriSign 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 VeriSign SSP database to prevent duplication and to ensure the uniqueness of SSP certificate distinguished names and serial numbers.

### **3.1.5 Name Claim Dispute Procedure**

VeriSign shall investigate and correct, if necessary, any name collisions brought to its attention. If appropriate, VeriSign shall coordinate with and defer to the PA naming authority. Agency PMAs shall resolve name collisions within their own space.

### **3.1.6 Recognition, authentication, and role of trademarks**

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

### **3.1.7 Method to prove possession of private key**

For all certificate requests in which either the subscriber generates the key pair (Signature certificate) or the VeriSign Key Manager generates the key pair on behalf of the subscriber (Encryption certificate), the VeriSign 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 VeriSign 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.

### **3.1.8 Authentication of CA Certificate Issuance**

Requests for CA certificates shall include the CA name, address, and documentation of the existence of the CA. The issuing CA 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 CA.

### **3.1.9 Authentication of Individual Identity**

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

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).

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

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

### **3.1.10 Authentication of Component Identities**

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

- Device name;
- Device public keys (using a Certificate Signing Request);
- Device authorizations and attributes (if any are to be included in the certificate); and
- Contact information to enable VeriSign to communicate with the PKI sponsor when required.

The VeriSign SSP requires in person registration of the PKI Sponsor, with the identity of the PKI Sponsor confirmed in accordance with the requirements of Section 3.1.9. 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.

## **3.2 Certificate Renewal, Update, and Routine Re-Key**

### **3.2.1 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 VeriSign 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.

### **3.2.2 Certificate Re-key**

The VeriSign 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.

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 3.1, re-key requests for Subscriber certificates may be authenticated on the basis of existing subscriber certificates. A Subscriber, whose certificates have not expired and whose initial subscriber enrollment data has not changed, may re-key his or her certificates based on electronic authentication of a currently valid Signature and Encryption certificates. The VeriSign SSP provides separate SSL-protected web pages for re-keying of Signature and Encryption certificates.

For certificates issued under id-fpki-common-High shall follow the same procedures as initial certificate issuance.

The VeriSign 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 3.1, a Subscriber certificate re-key shall follow the same procedures as initial certificate issuance.

CA Certificate Re-key and re-key of certificates issued under id-fpki-common-High shall follow the same procedures as initial certificate issuance.

### **3.2.3 Certificate update**

The VeriSign 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 3.1.9, and the old certificate shall be revoked.

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

### **3.3 Re-Key After Revocation**

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

### **3.4 Revocation Request**

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

## 4. OPERATIONAL REQUIREMENTS

### 4.1 Certificate Application

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 3.1)
- Establish and record identity of the applicant (per Section 3.1)
- Obtain the applicant's public key and verify the applicant's possession of the private key for each certificate required (per Section 3.1.7)
- 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:

#### 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 3.1.9. 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 3.1.9.2. 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.

**4.1.1 Delivery of Subscriber's Public Key to Certificate Issuer**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.

**4.2 Certificate Issuance**

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 SP CA is automatic. The certificate is immediately delivered back to the browser, which stores the certificate in the browser cache.

### **4.2.1 Delivery of Subscriber's Private Key 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 until the Subscriber accepts possession of it. The Subscriber acknowledges receipt of the smart card.

Private Encryption keys for smart cards are generated in the 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. The private encryption keys are delivered in a PKCS#12 format to the Subscriber in an 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.

### **4.2.2 CA Public Key Delivery to Users**

The US Government Common Policy Root Certificate and the VeriSign SSP CA certificate shall be delivered to users and relying parties by downloading the certificates from a web site secured with a VeriSign 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, VeriSign 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.

## **4.3 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 2.1.5. 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 2.1.5. 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 Certificate Suspension and Revocation**

### **4.4.1 Revocation**

#### **4.4.1.1 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 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.

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.

#### **4.4.1.2 Who Can Request Revocation**

The Subscriber is authorized to request the revocation of his or her own certificate. The VeriSign 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.

#### **4.4.1.3 Procedure for Revocation Request**

The revocation request must identify the certificate to be revoked and must include the reason for revocation. The revocation requests may be manually or digitally signed and must be authenticated by a 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 VeriSign SSP RA. The message must include a reason for the revocation. The VeriSign SSP 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 VeriSign. The Web page is protected using SSL. Upon successful validation of the revocation request by the SSP RA, the VeriSign 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 Trusted Agent:* A Trusted Agent may request revocation of a Subscriber's certificate by sending a digitally signed message to the VeriSign SSP RA. The VeriSign SSP RA will validate the request by verifying the signature on the signed message 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 VeriSign SSP RA, the VeriSign 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 VeriSign SSP to request revocation is protected using SSL and requires presentation of a valid RA certificate. The VeriSign SSP validates the RA certificate and checks that the RA affiliation is the same as the organizational affiliation in the certificate to be revoked. If these checks are successful, the VeriSign 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.

The VeriSign 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 4.4.3.1.

#### **4.4.1.4 Revocation Request Grace Period**

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

#### **4.4.2 Suspension**

The VeriSign SSP does not support certificate suspension for any certificates issued under this CPS.

#### **4.4.3 Certificate Revocation Lists**

The VeriSign SSP CA shall issue CRLs covering all unexpired certificates issued under this CPS.

##### **4.4.3.1 CRL Issuance Frequency**

The VeriSign SSP will generate and issue CRLs at least every eighteen (18) hours. All CRLs shall have an eighteen (18) hour validity interval. Superseded CRLs are removed from the repository upon posting of the latest CRL. When a CA certificate is revoked because of compromise or suspected compromise of a private key, a CRL will be issued within six (6) hours of notification. When a certificate issued under the id-fpki-common-High is revoked because of compromise or suspected compromise of a private key, a CRL must be issued within 6 hours of notification.

The VeriSign 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.

#### **4.4.4 Online Status Checking**

The VeriSign SSP will provide an online CSA to enable certificate status checking using the Online Certificate Status Protocol (OCSP compliant with RFC 2560). The OCSP responder certificate will be issued on a FIPS 140 Level 2 hardware token. 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.

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

#### **4.4.5 Other Forms of Revocation Advertisements Available**

The VeriSign SSP will also provide a Web page at which relying parties may query the revocation status of a subscriber certificate. Each SSP CA will have a dedicated Web page, which is protected with a VeriSign class 3 server certificate,

#### **4.4.6 Checking Requirements for Other Forms of Revocation Advertisements**

No stipulation.

#### **4.4.7 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 VeriSign 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 4.2.2.

### **4.5 Security Audit /Audit Logging Procedures**

#### **4.5.1 Types of Events Recorded**

VeriSign SSP equipment will record events for the CA, RA, Agency RAs and the CSA. The events include server installation, modification, accesses and application requests, responses, actions, publications, and error conditions. The information recorded includes the type of event, the time the event occurred, and the identity of the operator that caused the event. Depending on the type of event, additional information such as the success or failure, the source and destination of a message or the disposition of a created object (e.g., a filename) will also be recorded. Electronic-based audit data is automatically collected. Physical data is recorded in a logbook, paper form, or other physical mechanism as appropriate to the process being audited.

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

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

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

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

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

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

VeriSign records all required audit events and record data in either manual or electronic logs.

#### **4.5.2 Frequency of Processing Log**

Audit logs are removed by trusted personnel. The system continuously monitors the available storage space and automatically sends an alert when storage capacity reaches 70%. The magnetic media is then removed from the system and labeled with an identification number that is provided by the system. The archived media is driven by trusted personnel to the offsite storage facility.

Comprehensive reviews of audit logs are conducted at least once every two months by designated system security personnel. A statistically significant portion (typically 20%) of the security audit data generated by the SSP CA since the last review is examined. All significant events are explained in an audit log summary and any action taken as a result of the reviews is documented.

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

#### **4.5.3 Retention Period of Audit Log**

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

Audit logs are retained as archive records in accordance with section 4.6.2 of this CPS.

#### **4.5.4 Protection of Audit Log**

As a general design practice, the system audit log is not open for reading or modification by any human, or by any automated process other than those that perform audit processing. Entities that do not have modification access to the audit log may archive it. Weekly/monthly audit data is moved to a safe, secure storage location separate from the CA equipment. The VeriSign SSP currently relies on procedural (personnel and facility) controls to protect audit records from accidental or malicious overwrite. The audit data is under supervision of trusted VeriSign personnel

#### **4.5.5 Audit Log backup Procedures**

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

#### **4.5.6 Audit Collection System**

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

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

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

#### **4.5.7 Notification to Event-Causing Subject**

No notification is provided to an event-causing subject.

#### **4.5.8 Vulnerability Assessments**

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

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

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

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

VeriSign conducts quarterly vulnerability assessments to determine its ability to protect against external network threats. VeriSign personnel, in addition to external consultants, perform this

routine assessment. Finally, VeriSign undergoes a yearly extensive SAS 70 Type 2-security audit and a WebTrust audit to validate its operation in accordance with this practice documentation.

## **4.6 Records Archival**

### **4.6.1 Types of Data/Records Archived**

The VeriSign 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
- Security audit data (in accordance with Section 4.5)
- 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
- Documentation required by compliance auditors
- Access to escrowed Subscriber private encryption keys

## **4.6.2 Retention Period for Archive**

VeriSign 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 records are stored at an offsite third party.

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.

## **4.6.3 Protection of Archive**

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

Archive media are only handled by trusted employees and stored in a separate, safe, secure storage facility on magnetic media.

## **4.6.4 Archive Backup Procedures**

A full image tape backup of the VeriSign SSP system and database is prepared once a week and sent to a secure off-site storage under the control of trusted personnel. Once a month, these full image backups are sent to a secure off-site location where they are retained for the archive period specified in section 4.6.2.

## **4.6.5 Requirements for Time-Stamping of Records**

Certificates, CRLs, and other revocation database entries contain time and date information. Such time information is not cryptographic-based. A VeriSign time server, synchronized via Global Positioning Service to the Coordinated Universal Time is accurate to within one (1) second

## **4.6.6 Procedures to Obtain and Verify Archive Information**

Procedures for creating, verifying, packaging, transmitting and storing archive information are detailed in Sections 4.5.2, 4.5.3 and 4.5.4. In the event it becomes necessary for an external party to obtain archive information, VeriSign Production Services personnel, upon receipt of a duly authorized request, will produce such information.

## **4.7 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 validity periods will be set to 6 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 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.

## **4.8 Compromise and Disaster Recovery**

VeriSign maintains a Disaster Recovery Facility (DRF) located at a VeriSign-owned facility in Virginia. The VeriSign DRF is operated under the same security policies and procedures as the primary facility.

VeriSign has developed a Disaster Recovery Plan for all of its managed PKI services including the SSP PKI service. The Disaster Recovery Plan defines the procedures for the VeriSign Disaster Recovery Team to reconstitute VeriSign SSP operations using backup data and backup copies of the SSP keys.

### **4.8.1 Computing Resources, Software, and or Data are Corrupted**

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

In the case of a disaster whereby the VeriSign SSP installation is physically damaged and the primary operational copy of the VeriSign SSP signature key is destroyed as a result, the VeriSign SSP will initiate certificate management operations from its Disaster Recovery site.

### **4.8.2 CA Cannot Generate CRLs**

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

### **4.8.3 CA Signature Keys are Compromised**

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 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 VeriSign SSP will reconstitute its operation under a new PKI hierarchy using the same procedures that were performed during initial system initialization. Subscribers will be required to re-key and must repeat the initial application process. The new SSP CA certificate will be distributed as defined in section 4.2.2.

In the event of the compromise of the VeriSign SSP OCSP responder, the VeriSign SSP shall revoke the OCSP responder certificate, add the certificate serial number to a CRL and subsequently re-key the OCSP responder.

#### **4.8.4 Secure Facility Impaired after a natural or Other Type of Disaster**

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

#### **4.9 CA Termination**

In the event of termination of the VeriSign SSP CA, certificates signed by the SSP CA will be revoked. Dissemination of revocation notice will be achieved as discussed in CPS section 4.8.1. The SSP CA shall transfer its archival records to an Agency PMA approved archival facility.

## **5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS**

### **5.1 Physical Controls**

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

Unauthorized use of CA equipment is forbidden. Physical security controls are implemented to protect the CA hardware and software from unauthorized use. CMA cryptographic modules are protected against theft, loss and unauthorized use.

#### **5.1.1 Site Location and Construction**

The system components and operation of the VeriSign SSP will be contained within a physically protected environment to deter, detect, and prevent unauthorized use of, access to, or disclosure of sensitive information. The primary site location is at VeriSign headquarters in Mountain View, CA, and the DRF is at a VeriSign-owned facility in Virginia. The facilities housing the primary and back-up CA and Repository provide extensive physical security and access control systems to limit access only to authorized personnel and authorized visitors.

#### **5.1.2 Physical Access**

The system components and operation of the VeriSign SSP will be contained within a physically protected environment to deter, detect, and prevent unauthorized use of, access to, or disclosure of sensitive information.

#### **5.1.3 Electric Power and Air Conditioning**

The VeriSign SSP primary and backup facilities are supplied with power and air conditioning sufficient to create a reliable operating environment.

Power for the primary site is backed up in case of emergency failure. If a major power failure occurs, a battery based UPS system can supply sufficient power until the diesel generators are activated. The diesel generators are supplied from external to the building for unlimited refueling capacity. The diesel generators can operate for a minimum of 30 hours without refueling.

#### **5.1.4 Water Exposure**

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

#### **5.1.5 Fire Prevention and Protection**

An automated fire detection and suppression system has been installed in both the primary and backup facilities in accordance with local fire policy and code.

### **5.1.6 Media Storage**

Critical system data is incrementally backed-up on a daily basis. Full back-ups are performed on a weekly basis and the magnetic media is sent off site. The VeriSign SSP has a disaster recovery (hot) site on the East Coast. Access to media is limited to authorized personnel and stored in fire-rated media safes.

### **5.1.7 Waste Disposal**

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

### **5.1.8 Off-Site Backup**

See section 5.1.6.

## ***5.2 Procedural Controls***

### **5.2.1 Trusted Roles**

All employees, contractors, and consultants of the VeriSign 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. Such personnel include, but are not limited to, customer service personnel, system administration personnel, security auditors, designated engineering personnel, and executives who are designated to oversee the trustworthy infrastructures. All employees serving in a trusted position must acquire and periodically re-qualify (every five years) for “trusted employee” status as a condition of employment

## ***5.3 Personnel Controls***

### **5.3.1 Background, Qualifications, Experience and Clearance Requirements**

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

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

Personnel appointed to operate CMA equipment shall:

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

### **5.3.2 Background Check Procedures**

Except as specifically noted in Section 5.2.1, all persons filling trusted roles for the VeriSign SSP shall be US citizens. All VeriSign persons filling trusted roles shall undergo a background investigation.

### **5.3.3 Training Requirements**

Operations personnel are sufficiently trained prior to performing independent, unattended duties. The employee training program is typically 4-8 weeks in duration, consisting of: mentoring by a functional area expert and/or supervisor; video, Computer Based Training (CBT), and hands-on training; and formal testing and certification. Training topics include the operation of the SSP software and hardware, operational and security procedures, disaster recovery and business continuity operations, and requirements of this CPS.

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

### **5.3.4 Retraining Frequency and Requirements**

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

### **5.3.5 Job Rotation Frequency and Sequence**

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

### **5.3.6 Sanctions for Unauthorized Actions**

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

### **5.3.7 Contracting Personnel Requirements**

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

### **5.3.8 Documentation Supplied to Personnel**

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

## **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***

VeriSign SSP CA and CSA key pairs are generated within VeriSign's secure Key Ceremony room on hardware tokens. The ceremony is video taped and witnessed and a full audit record is created to ensure that all security requirements, including separation of roles were followed. The audit record identifies any failures or anomalies in the key generation process, and any corrective action taken. At no time does the VeriSign SSP CA or CSA private key appear in plain-text form outside the hardware protection boundary of the hardware token. CA and CSA certificate signing keys are generated in FIPS 140 Level 3 validated cryptographic hardware modules.

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

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-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).

#### **6.1.2 Private Key Delivery to Subscriber**

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

- Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key after delivery of the private key to the Subscriber;
- The private key must be protected from activation, compromise, or modification during the delivery process;
- The Subscriber shall acknowledge receipt of the private key(s); and

- Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers:
  - For hardware modules, accountability for the location and state of the module must be maintained until the Subscriber accepts possession of it.
  - For electronic delivery of private keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data shall be delivered using a separate secure channel.

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

### 6.1.3 Public Key Delivery to Certificate Issuer

The Subscriber's identity information and public key are delivered to the certificate issuer simultaneously in 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 Root Certificate and the VeriSign SSP CA certificate shall be delivered to users and relying parties by downloading the certificates from a web site secured with a VeriSign Class 3 web server certificate. Subscribers will be required to compare the certificate hash against the hash value received from a Trusted Agent, VeriSign RA or Agency RA.

### 6.1.5 Key Sizes and Signature Algorithms

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

- For all CA certificates that expire **before** January 1, 2011: All CA signing key pairs will be at least 1024-bit RSA key pairs. Certificates and CRLs generated by the VeriSign SSP CA will use SHA-1 or better for digital signatures.
- For all CA certificates that expire **after** December 31, 2010: All CA signing key pairs will be generated with at least 2048 bit RSA keys. Certificates and CRLs generated by the VeriSign SSP CA will use SHA-256 for digital signatures.
- For all Subscriber certificates asserting id-fpki-common-authentication, id-fpki-common-cardAuth, or id-fpki-common-device object identifiers that expire **before** January 1, 2011: All Subscriber key pairs will be at least 1024-bit RSA key pairs. Certificates and CRLs generated by the VeriSign SSP CA will use SHA-1 or better for digital signatures.
- For all Subscriber certificates asserting id-fpki-common-authentication, id-fpki-common-cardAuth, or id-fpki-common-device object identifiers that expire **after** December 31, 2010: All Subscriber key pairs will be 2048-bit RSA key pairs. Certificates and CRLs generated by the VeriSign SSP CA will use SHA-256 for digital signatures.
- For all Subscriber certificates asserting id-fpki-common-policy, id-fpki-common-hardware, or id-fpki-common-High object identifiers that expire **before** January 1, 2009: All CA signing key

pairs and Subscriber key pairs will be at least 1024-bit RSA key pairs. Certificates and CRLs generated by the VeriSign SSP CA will use SHA-1 or better for digital signatures.

- For all Subscriber certificates asserting id-fpki-common-policy, id-fpki-common-hardware, or id-fpki-common-High object identifiers that expire after December 31, 2008: All CA signing key pairs and Subscriber key pairs will be 2048-bit RSA key pairs. Certificates and CRLs generated by the VeriSign SSP CA will use SHA-256 for digital signatures.
- Any use of Transport Layer Security (TLS) or Secure Socket Layer (SSL) protocol to accomplish the requirements of this CPS before January 1, 2009 will use three key Data Encryption Standard (triple-DES) for the symmetric key algorithm and 1024 bit RSA for asymmetric keys.
- Any use of Transport Layer Security (TLS) or Secure Socket Layer (SSL) protocol to accomplish the requirements of this CPS after December 31, 2008 will use a minimum of AES (128 bits) or equivalent for symmetric keys and 2048 bit RSA for asymmetric keys.

The trust anchor for the SSP CA, which is the US Government Common Policy Root CA, shall contain a public key of at least 2048 bits.

### 6.1.6 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].

### 6.1.7 Parameter Quality Checking

Parameter checking (including primarily testing for prime numbers) shall be performed in accordance with FIPS 186-2.

### 6.1.8 Hardware/Software Key Generation

Validated FIPS 140 software or hardware cryptographic modules shall be used 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.

### 6.1.9 Key Usage Purposes

The VeriSign 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.

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

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

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

## **6.2 Private Key Protection**

### **6.2.1 Standards for cryptographic modules**

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

VeriSign 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.

VeriSign SSP Subscribers utilizing hardware-based cryptographic modules (*id-fpki-common-hardware*, *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 VeriSign smart card issuance system supports FIPS 140 Level 2 certified cryptographic modules including NIST-certified PIV-2 smart cards.

The VeriSign 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 VeriSign SSP CA and CSA shall use a FIPS 140 Level 3 hardware cryptographic token. All cryptographic modules dedicated to management of VeriSign 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 VeriSign or an Agency RA, is physically separated from the SSP CA.

## 6.2.2 Private Key Multi-person Control

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

## 6.2.3 Private Key Escrow

The VeriSign SSP provides key escrow and key recovery services for VeriSign SSP Subscriber private encryption keys. Recovery of the private encryption key is under two man control. CA private keys are not escrowed. Subscriber private Signature keys are not escrowed. Under no circumstances shall a Subscriber's Signature key be held in trust by a third party.

## 6.2.4 Private Key backup

### 6.2.4.1 Backup of CA Private Signature Key

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

### 6.2.4.2 Backup of Subscriber Private Keys

VeriSign SSP subscribers are obligated to prevent unauthorized disclosure of their private keys. This includes any means undertaken to establish a backup copy of their keys in support of disaster recovery. The VeriSign SSP provides escrow of subscriber private Encryption keys, but 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.

For 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, 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).

## 6.2.5 Private Key Archival

CA private Signature keys and Subscriber private Signature keys are not archived. See Section 6.2.3 and Section 6.2.4 for additional details.

## 6.2.6 Private Key entry into cryptographic module

When the VeriSign 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, 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 Method of Activating Private Key**

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

VeriSign SSP subscribers are obligated to select a password or PIN during key generation. Entry of the password or PIN is required to activate the private key whose corresponding public key is contained in a certificate asserting the id-fpki-common-authentication, id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-devices or id-fpki-common-High policy object identifier. The subscriber is the only entity that knows the password; at no time does the VeriSign 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-cardAuth, subscriber authentication is not required to use the associated private key.

### **6.2.8 Method of Deactivating Private Key**

The VeriSign 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.

### **6.2.9 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 VeriSign 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

## ***6.3 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 Usage Periods for the Public and Private Keys**

The key usage periods for keying material are described in Section 3.2 and Section 4.7. The usage period for the SSP CA key pair is a maximum of six years. The SSP CA private key may be used to generate certificates for the first half of the usage period (3 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.

Subscriber public keys have a maximum usage period of one half the CA key pair usage period. 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**

VeriSign SSP subscribers are requested to select their own password/PIN to protect their private key. Guidance regarding the selection of is provided during the enrollment process.

The PINs used to protect the VeriSign SSP and CSA tokens are randomly and automatically generated.

RAs are also required to choose their own PINs. Guidance regarding the selection of is provided during the enrollment process.

### **6.4.2 Activation data protection**

The VeriSign 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. The RA or Subscriber activation PIN is only known by the holder of the token.

### **6.4.3 Other aspects of activation data**

See Section 6.4.1.

## **6.5 Computer Security Controls**

### **6.5.1 Specific computer security technical requirements**

The VeriSign SSP and CSA employ an operating system that has been evaluated for security functionality, including audit requirements, identification and authentication, and discretionary access controls. This current operating system is Sun Microsystems's Solaris.

### **6.5.2 Computer security rating**

VeriSign uses Sun Microsystems Solaris operating system for production services.

## **6.6 Life Cycle Technical Controls**

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

such as random selection. Intended use of procured hardware and software is never indicated on order forms/paperwork.

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.

### ***6.7 Network Security Controls***

- The VeriSign SSP is designed to mitigate risk to external threats.

### ***6.8 Cryptographic Module Engineering Controls***

See Section 6.2.

## 7. CERTIFICATE AND CRL PROFILES

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

### 7.1 Certificate Profile

#### 7.1.1 Version Numbers

SSP shall issue X.509 Version 3 certificates only.

#### 7.1.2 Certificate Extensions

The VeriSign 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}

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}
---------------	--

The VeriSign 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 revocation 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, and id-fpki-common-device of the base certificate shall be populated with an X.500 Distinguished Name, with the attribute type as further constrained by RFC 3280.

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 3280.

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 VeriSign SSP does not enforce name constraints.

### **7.1.6 Certificate Policy Object Identifier**

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

### **7.1.7 Usage of Policy Constraints**

The VeriSign SSP does not enforce policy constraints.

### **7.1.8 Policy Qualifiers Syntax and Semantics**

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

### **7.1.9 Processing Semantics for the Critical Certificate Policy 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 keyusage 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].

### **7.2.1 Version numbers**

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

### **7.2.2 CRL and CRL Entry Extensions**

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

## **8. SPECIFICATION ADMINISTRATION**

### ***8.1 Specification Change Procedures***

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

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

### ***8.2 Publication And Notification Procedures***

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

This VeriSign SSP CPS is posted in the VeriSign document repository at <http://www.verisign.com/repository>. Applicable updates to this CPS that affect Subscribers and relying parties will be posted on the VeriSign corporate web site.

### ***8.3 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 VeriSign SSP CPS before commencing operations.

### ***8.4 CPS Waivers***

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

## **APPENDIX A: CERTIFICATE AND CRL FORMATS**

All certificates and CRLs associated with the VeriSign 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. [NS4009]
access control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]
accreditation	Formal declaration by a Designated Approving Authority that an IS is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
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. [ABADSG footnote 32]
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. [NS4009]
audit data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
authenticate	To confirm the identity of an entity when that identity is presented.
authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
binding	Process of associating two related elements of information. [NS4009]
biometric	A physical or behavioral characteristic of a person.
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. As used in this CP, the term "Certificate" refers to certificates that expressly reference the OID of this CP in the "Certificate Policies" field of an X.509 v.3 certificate.
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. [ISO9594-8]
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. [NS4009]
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by NIST
confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
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. [FIPS140]
cryptoperiod	Time span during which each key setting remains in effect. [NS4009]
data integrity	Assurance that the data are unchanged from creation to reception
discretionary access control	
dual use certificate	A certificate that is intended for use with both digital signature and data encryption services.
e-commerce	The use of network technology (especially the Internet) to buy or sell goods and services
Encryption (or Confidentiality) certificate	A certificate containing a public key that is used to encrypt or decrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes. The process of storing protecting and escrowing the private component of the key pair associated with the encryption certificate is sometimes referred to as key management.
erroneous issuance	Issuance of a certificate not materially in accordance with the procedures required by the CPS, issuance of a certificate to a person other than 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. [NS4009]
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. [NS4009]
intellectual property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
key escrow	The retention of the private component of the key pair associated with a subscriber's encryption certificate to support key recovery.
key exchange	The process of exchanging public keys (and other information) in order to establish secure communication.
key generation material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Local Registration Authority (LRA)	An RA with responsibility for a local community.

naming authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
National Security System	Any telecommunications or information system operated by the U.S. Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]
non-repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009]
Non-verified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization; the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI OIDs are used to uniquely identify each of the four policies and cryptographic algorithms supported.
Out-of-Band	Communication between parties using a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
PKI Sponsor	Fills the role of a Subscriber for non-human system components 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.
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. [ABADSG]
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. [ABADSG]
revocation	The act or process of prematurely ending the operational period of a certificate effective at a specific date and time.
risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
risk tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
server	A system entity that provides a service in response to requests from clients.
Signature certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions. Also referred to as an Identity Certificate.
subordinate CA	In a hierarchical PKI, a CA whose certificate signing key is certified by another CA, and whose activities are constrained by that other CA. (see superior CA)
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to such an entity, and (2) holds a private key that corresponds to a public key listed in that certificate. [ABADSG]. Current subscribers possess valid SSP-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. [NS4009]
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. [NS4009]
update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
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. [FIPS140]

## APPENDIX C: REFERENCES

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

Number	Title	Revision	Date
ABADSG	<i>Digital Signature Guidelines</i> <a href="http://www.abanet.org/scitech/ec/isc/dsgfree.html">http://www.abanet.org/scitech/ec/isc/dsgfree.html</a>		1 August 1996
CCP-PROF	<i>X.509 Certificate and CRL Extensions Profile for the Common Policy</i> <a href="http://www.cio.gov/ficc/documents/CertCRLprofileForCP.pdf">http://www.cio.gov/ficc/documents/CertCRLprofileForCP.pdf</a>		
E-Auth	<i>E-Authentication Guidance for Federal Agencies, M-04-04</i>		16 December 2003
FIPS140	<i>Security Requirements for Cryptographic Modules</i> <a href="http://csrc.nist.gov/publications/index.html">http://csrc.nist.gov/publications/index.html</a>		21 May 2001
FIPS112	<i>Password Usage</i> <a href="http://csrc.nist.gov/">http://csrc.nist.gov/</a>		5 May 1985
FIPS186-2	<i>Digital Signature Standard</i> <a href="http://csrc.nist.gov/fips/fips186-2.pdf">http://csrc.nist.gov/fips/fips186-2.pdf</a>		27 January 2000
FIPS201-1	<i>Personal Identity Verification (PIV) of Federal Employees and Contractors</i> <a href="http://csrc.nist.gov/publications/fips/fips201/FIPS-201-1-v5.pdf">http://csrc.nist.gov/publications/fips/fips201/FIPS-201-1-v5.pdf</a>		March 2006
FOIAACT	<i>5 U.S.C. 552, Freedom of Information Act</i> <a href="http://www4.law.cornell.edu/uscode/5/552.html">http://www4.law.cornell.edu/uscode/5/552.html</a>		
NS4009	<i>NSTISSI 4009, National Information Systems Security Glossary</i>		January 1999
PACS	<i>Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems</i> <a href="http://smart.gov/information/TIG_SCEPACS_v2.2.pdf">http://smart.gov/information/TIG_SCEPACS_v2.2.pdf</a>	2.2	27 July 2004
PKCS-1	<i>PKCS #1 v2.1: RSA Cryptography Standard</i> <a href="http://www.rsasecurity.com/rsalabs/node.asp?id=2125">http://www.rsasecurity.com/rsalabs/node.asp?id=2125</a>	2.1	14 June 2002
PKCS-12	<i>Personal Information Exchange Syntax Standard</i> <a href="http://www.rsasecurity.com/rsalabs/node.asp?id=2138">http://www.rsasecurity.com/rsalabs/node.asp?id=2138</a>	1.0	24 June 1999
SSPKRPS	<i>Key Recovery Practices Statement for VeriSign SSP PKI Service</i>		
RFC2527	<i>Certificate Policy and Certification Practices Framework, Chokhani and Ford</i> <a href="http://www.ietf.org/rfc/rfc2527.txt">http://www.ietf.org/rfc/rfc2527.txt</a>		March 1999
RFC 2560	<i>X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol-OCSP, Michael Myers, Rich Ankney, Amarish Malpani, Slava Galperin, and Carlisle Adams</i>		June 1999

**APPENDIX D: ACRONYMS AND ABBREVIATIONS**

CA	Certification Authority
CMA	Certificate Management Authority
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
SSP	External Certification Authority
FASC-N	Federal Agency Smart Credential Number
FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standard
FPKI	(US) Federal Public Key Infrastructure
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 Practices Statement
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Federal PKI Policy Authority
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PMA	Policy Management Authority
RA	Registration Authority
RFC	Request For Comment
RSA	Rivest, Shamir, Adleman (encryption and digital signature algorithm)
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Socket Layer
USC	United States Code
USD	United States Dollar

\* \* \* End of Document \* \* \*