VeriSign Certification Practice Statement

Version 3.2

Effective Date: May 01, 2006

VeriSign, Inc.
487 E. Middlefield Road
Mountain View, CA 94043 USA
+1 650.961.7500
http//:www.verisign.com

History of changes: version 3.2 (Effective date May 01, 2006)

General	Corrected typographical errors
Section 1.4.1.2 (Table 2)	Added TLS as an appropriate use for organization certificates.
Section 3.2.3	Amended "Class 3 Administrator certificates shall also include authentication of the organization and a confirmation from the organization of the employment and authorization of the person to act as Administrator. " to say "The authentication of Class 3 Administrator certificates is based on authentication of the organization and a confirmation from the organization of the employment and authorization of the person to act as Administrator"
Section 3.3.1 and Section 4.6.3	Specified that it is the Corporate Contact and Technical Contact information that must remain unchanged for an automatically issued renewal.
Section 3.3.1 and section 4.6.3	Added: "In particular, for subsequent renewal requests for Class 3 Organizational certificates, VeriSign reauthenticates the Organization name and domain name included in the certificate. In circumstances where • The challenge phrase is correctly used for the subsequent renewal certificate and: • The certificate Distinguished Name has not been changed, and • The Corporate and Technical Contact information remains unchanged from that which was previously verified, VeriSign will not have to reconfirm by telephone, confirmatory postal mail, or comparable procedure to the Certificate Applicant certain information about the organization, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Certificate Applicant is authorized to do so."
Section 7.2	Removed reference to RFC 3280
Section 7.2.1	Added that "Version 2 CRLs comply with the requirements of RFC 3280."
Section 9.2.1	Updated from: "Enterprise Customers shall maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention. This insurance requirement does not apply to governmental entities. VeriSign maintains such errors and omissions insurance coverage." to: "Enterprise Customers are encouraged to maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention. VeriSign maintains such errors and omissions insurance coverage."
Section 9.2.3	Updated Section title from "Insurance or Warranty Coverage for End-Entities" to "Extended Warranty Coverage"
Section 9.2.3	Replaced the following content: "The NetSure Protection Plan is an extended warranty program that applies within VeriSign's Subdomain of the VTN. Where it applies, the NetSure Protection Plan provides Subscribers receiving with protection against accidental occurrences such as theft, corruption, loss, or unintentional disclosure of the Subscriber's private key (corresponding to the public key in the Certificate), as well as impersonation and certain loss of use of the Subscriber's Certificate. The NetSure Protection Plan also provides protection to Relying Parties when they rely on Certificates covered by the NetSure Protection Plan. NetSure is a program provided by VeriSign and backed by insurance obtained from commercial carriers. For general information concerning the NetSure Protection Plan, and a discussion of which Certificates are covered by it, see http://www.verisign.com/netsure. The protections of the NetSure Protection Plan are also offered, for a fee, to Enterprise Customers of VeriSign. They can obtain protections under the NetSure Protection Plan subject to the terms of an appropriate agreement for this service. This service not only extends the protections of the NetSure Protection Plan to the Subscribers whose Certificate Applications are approved by the Enterprise Customer, it also extends these protections to the Enterprise Customer itself. For example, if a Managed PKI Customer approves a Certificate Application of an employee of the Managed PKI Customer, who uses the Certificate for the business purposes of the Managed PKI Customer, and if the Subscriber's actions cause a loss, the real party bearing the loss may be the Managed PKI Customer in its role as the Subscriber's employer. If covered by the NetSure Protection Plan, the Managed PKI Customer may submit a claim for the loss sustained because of the Subscriber's actions." With: "The NetSure Protection Plan is an extended warranty program that provides VeriSign SSL and code signing certificate subscribers with protection against loss or damage that is due to a defect in VeriSign's issuance of the certificate or other malfeasance caused by VeriSign's negligence or breach of its contractual obligations, provided that the subscriber of the certificate has fulfilled its obligations under the applicable service agreement. For general information concerning the NetSure Protection Plan, and a discussion of which Certificates are covered by it, see http://www.verisign.com/netsure"

History of changes: version 3.1 (Included December 01, 2005)

Section 2.3	Changed reference to Section 8 to Section 9.12
Section 4.5.2	Updated to include the following language: “Relying Party is solely responsible to investigate whether reliance on a digital signature performed by an end-user Subscriber Certificate prior to revocation of a Certificate in the Certificate chain is reasonable. Any such reliance is made solely at the risk of the Relying party.”
Section 4.12.1	Made the list of requirements for key recovery a VeriSign recommendation
Section 6.2.1	Deleted “For other CAs, VeriSign uses hardware cryptographic modules that are certified at or meet the requirements of at least FIPS 140-1 Level 2”
Section 9.2.2	Updated URL to VeriSign SEC filings: http://www.verisign.com/verisign-inc/vrsn-investors/sec-filings/index.html

VeriSign Trust Network Certificate Policies

Published date: April 01, 2005

Trademark Notices

Table of Contents

1. INTRODUCTION

This document is the VeriSign Certification Practice Statement ("CPS"). It states the practices that VeriSign certification authorities ("CAs") employ in providing certification services that include, but are not limited to, issuing, managing, revoking, and renewing certificates in accordance with the specific requirements of the VeriSign Trust Network Certificate Policies ("CP").

The CP is the principal statement of policy governing the VTN. It establishes the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital Certificates within the VTN and providing associated trust services. These requirements, called the "VTN Standards," protect the security and integrity of the VTN, apply to all VTN Participants, and thereby provide assurances of uniform trust throughout the VTN. More information concerning the VTN and VTN Standards is available in the CP.

VeriSign has authority over a portion of the VTN called its "Subdomain" of the VTN. VeriSign's Subdomain includes entities subordinate to it such as its Customers, Subscribers, and Relying Parties.

While the CP sets forth requirements that VTN Participants must meet, this CPS describes how VeriSign meets these requirements within VeriSign's Subdomain of the VTN. More specifically, this CPS describes the practices that VeriSign employs for:

- securely managing the core infrastructure that supports the VTN, and
- issuing, managing, revoking, and renewing VTN Certificates

within VeriSign's Subdomain of the VTN, in accordance with the requirements of the CP and its VTN Standards.

1.1 Overview

This CPS is specifically applicable to:

- VeriSign's Public Primary Certification Authorities (PCAs),
- VeriSign Infrastructure CAs, and VeriSign Administrative CAs supporting the VeriSign Trust Network
- VeriSign's Public CAs and the CAs of enterprise Customers, who issue Certificates within VeriSign's subdomain of the VTN.

More generally, the CPS also governs the use of VTN services within VeriSign's Subdomain of the VTN by all individuals and entities within VeriSign's Subdomain (collectively, VeriSign Subdomain Participants"). Private CAs and hierarchies managed by VeriSign are outside the scope of this CPS. The CAs managed by Affiliates are also outside the scope of this CPS.

The VTN includes four classes of Certificates, Classes 1-4. The CP is a single document that defines these certificate policies, one for each of the Classes, and sets VTN Standards for each Class.

VeriSign currently offers three Classes of Certificates within its Subdomain of the VTN. This CPS describes how VeriSign meets the CP requirements for each Class within its Subdomain. Thus, the CPS, as a single document, covers practices and procedures concerning the issuance and management of all three Certificate Classes.

VeriSign may publish Certificate Practices Statements that are supplemental to this CPS in order comply with the specific policy requirements of Government, or other industry standards and requirements.

These supplemental certificate policies shall be made available to subscribers for the certificates issued under the supplemental policies and their relying parties.

The CPS is only one of a set of documents relevant to VeriSign's Subdomain of the VTN. These other documents include:

- Ancillary confidential security and operational documents[1] that supplement the CP and CPS by providing more detailed requirements, such as:
  - The VeriSign Physical Security Policy, which sets forth security principles governing the VTN infrastructure,
  - The VeriSign Security and Audit Requirements Guide, which describes detailed requirements for VeriSign and Affiliates concerning personnel, physical, telecommunications, logical, and cryptographic key management security, and
  - Key Ceremony Reference Guide, which presents detailed key management operational requirements.

- Ancillary agreements imposed by VeriSign. These agreements bind Customers, Subscribers, and Relying Parties of VeriSign. Among other things, the agreements flow down VTN Standards to these VTN Participants and, in some cases, state specific practices for how they must meet VTN Standards.

In many instances, the CPS refers to these ancillary documents for specific, detailed practices implementing VTN Standards where including the specifics in the CPS could compromise the security of VeriSign's Subdomain of the VTN.

1.2 Document name and Identification

This document is the VeriSign Certification Practice Statement. VTN Certificates contain object identifier values corresponding to the applicable VTN Class of Certificate. Therefore, VeriSign has not assigned this CPS an object identifier value. Certificate Policy Object Identifiers are used in accordance with Section 7.1.6.

1.3 PKI Participants

1.3.1 Certification Authorities

The term Certification Authority (CA) is an umbrella term that refers to all entities authorized to issue public key certificates within the VTN. The CA term encompasses a subcategory of issuers called Primary Certification Authorities (PCA). PCAs act as roots of four domains[2], one for each class of Certificate. Each PCA is a VeriSign entity. Subordinate to the PCAs are Certification Authorities that issue Certificates to end-user Subscribers or other CAs.

VeriSign enterprise customers may operate their own CAs as subordinate CAs to a VeriSign PCA. Such a customer enters into a contractual relationship with VeriSign to abide by all the requirements of the VTN CP and the VeriSign CPS. These subordinate CAs may, however implement a more restrictive practices based on their internal requirements.

One VTN CA technically outside the three hierarchies under each of the PCAs is the Secure Server Certification Authority. This CA does not have a superior CA, such as a root or a PCA. Rather, the Secure Server CA acts as its own root and has issued itself a self-signed root

[1] Although these documents are not publicly available their specifications are included in VeriSign's Annual WebTrust for Certification authorities audit and may be made available to customer under special Agreement

[2] Class 4 certificates are not currently issued by the VTN

Certificate. It also issues Certificates to end-user Subscribers. Thus, the Secure Server Hierarchy consists only of the Secure Server CA. The Secure Server CA issues Secure Server IDs, which are deemed to be Class 3 Organizational Certificates.

The Secure Server CA employs lifecycle practices that are substantially similar with those of other Class 3 CAs within the VTN. Thus, VeriSign has approved and designated the Secure Server Certification Authority as a Class 3 CA within the VTN. The Certificates it issues are considered to provide assurances of trustworthiness comparable to other Class 3 organizational Certificates.

1.3.2 Registration Authorities

A Registration Authority is an entity that performs identification and authentication of certificate applicants for end-user certificates, initiates or passes along revocation requests for certificates for end-user certificates, and approves applications for renewal or re-keying certificates on behalf of a VTN CA. VeriSign may act as an RA for certificates it issues.

Third parties, who enter into a contractual relationship with VeriSign, may operate their own RA and authorize the issuance of certificates by a VeriSign CA. Third party RAs must abide by all the requirements of the VTN CP, the VeriSign CPS and the terms of their enterprise services agreement with VeriSign. RAs may, however implement more restrictive practices based on their internal requirements. [3]

1.3.3 Subscribers

Subscribers under the VTN include all end users (including entities) of certificates issued by a VTN CA. A subscriber is the entity named as the end-user Subscriber of a certificate. End-user Subscribers may be individuals, organizations or, infrastructure components such as firewalls, routers, trusted servers or other devices used to secure communications within an Organization.

In some cases certificates are issued directly to individuals or entities for their own use. However, there commonly exist other situations where the party requiring a certificate is different from the subject to whom the credential applies. For example, an organization may require certificates for its employees to allow them to represent the organization in electronic transactions/business. In such situations the entity subscribing for the issuance of certificates (i.e. paying for them, either through subscription to a specific service, or as the issuer itself) is different from the entity which is the subject of the certificate (generally, the holder of the credential). Two different terms are used in this CPS to distinguish between these two roles: "Subscriber", is the entity which contracts with Verisign for the issuance of credentials and; “Subject", is the person to whom the credential is bound. The Subscriber bears ultimate responsibility for the use of the credential but the Subject is the individual that is authenticated when the credential is presented.

When ‘Subject’ is used, it is to indicate a distinction from the Subscriber. When “Subscriber” is used it may mean just the Subscriber as a distinct entity but may also use the term to embrace the two. The context of its use in this CPS will invoke the correct understanding.

CAs are technically also subscribers of certificates within the VTN, either as a PCA issuing a self signed Certificate to itself, or as a CA issued a Certificate by a superior CA. References to “end entities” and “subscribers” in this CP, however, apply only to end-user Subscribers.

[3] An example of a third party RA is a customer of Managed PKI services customer.

1.3.4 Relying Parties

A Relying Party is an individual or entity that acts in reliance of a certificate and/or a digital signature issued under the VTN. A Relying party may, or may not also be a Subscriber within the VTN.

1.3.5 Other Participants

Not applicable

1.4 Certificate Usage

1.4.1 Appropriate Certificate Usages

1.4.1.1 Certificates Issued to Individuals

Individual Certificates are normally used by individuals to sign and encrypt e-mail and to authenticate to applications (client authentication). While the most common usages for individual certificates are included in Table 1 below, an individual certificate may be used for other purposes, provided that a Relying Party is able to reasonably rely on that certificate and the usage is not otherwise prohibited by law, the VTN CP, the CPS under which the certificate has been issued and any agreements with Subscribers.

Certificate Class	**Assurance Level**			**Usage**		
	Low assurance level	**Medium assurance level**	**High assurance Level**	**Signing**	**Encryption**	**Client Authentication**
Class 1 Certificates	✓			✓	✓	✓
Class 2 Certificates		✓		✓	✓	✓
Class 3 Certificates			✓	✓	✓	✓

Table 1. Individual Certificate Usage

1.4.1.2 Certificates issued to Organizations

Organizational Certificates are issued to organizations after authentication that the Organization legally exists and that other Organization attributes included in the certificate (excluding non-verified subscriber information) are authenticated e.g. ownership of an Internet or e-mail domain. It is not the intent of this CPS to limit the types of usages for Organizational Certificates. While the most common usages are included in Table 2 below, an organizational certificate may be used for other purposes, provided that a Relying Party is able to reasonably rely on that certificate and the usage is not otherwise prohibited by law, by the VTN CP, by any CPS under which the certificate has been issued and any agreements with Subscribers.

Certificate Class	Assurance Level		Usage			
	High assurance level	Medium assurance level	Code/Content Signing	Secure SSL/TLS-sessions	Authentication	Signing and encryption
Class 3 Certificates	✓		✓	✓	✓	✓

Table 2. Organizational Certificate Usage[4]

1.4.1.3 Assurance levels

Low assurance certificates are certificates that should not be used for authentication purposes or to support Non-repudiation. The digital signature provides modest assurances that the e-mail originated from a sender with a certain e-mail address. The Certificate, however, provides no proof of the identity of the Subscriber. The encryption application enables a Relying Party to use the Subscriber's Certificate to encrypt messages to the Subscriber, although the sending Relying Party cannot be sure that the recipient is in fact the person named in the Certificate.

Medium assurance certificates are certificates that are suitable for securing some inter- and intra-organizational, commercial, and personal e-mail requiring a medium level of assurances of the Subscriber identity, in relation to Class 1 and 3.

High assurance Certificates are individual and organizational certificates Class 3 Certificates that provide a high level of assurance of the identity of the Subscriber in comparison with Class 1 and 2.

1.4.2 Prohibited Certificate Uses

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

VeriSign Certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage. Also, Class 1 Certificates shall not be used as proof of identity or as support of non repudiation of identity or authority. Client Certificates are intended for client applications and shall not be used as server or organizational Certificates.

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

VeriSign periodically rekeys Intermediate CAs. Third party applications or platforms that have an Intermediate CA embedded as a root certificate may not operate as designed after the

[4] "In limited circumstances Class 2 certificates may be issued by a Managed MPKI customer to an affiliated organization (and not an individual within the organization). Such certificate may be used for organization authentication and application signing only. Except as expressly authorized by VeriSign through an Enterprise Service Agreement imposing authentication and practice requirements consistent with the security standards of this CPS, Subscribers are prohibited from using this certificate for code and content signing, SSL encryption and S/mime signing and such key usage will be disabled for these certificates."

Intermediate CA has been rekeyed. VeriSign therefore does not warrant the use of Intermediate CAs as root certificates and recommends that Intermediate CAs not be embedded into applications and/or platforms as root certificates. VeriSign recommends the use of PCA Roots as root certificates.

1.5 Policy Administration

1.5.1 Organization Administering the Document

VeriSign Inc
487 E. Middlefield Road
Mountain View CA 94043
USA

1.5.2 Contact Person

The Certificate Policy Manager
VeriSign Trust Network Policy Management Authority
c/o VeriSign, Inc.
487 E. Middlefield Road
Mountain View, CA 94043 USA
+1 (650) 961-7500 (voice)
+1 (650) 426-7300 (fax)
practices@verisign.com

1.5.3 Person Determining CP Suitability for the Policy

The VTN Policy Management Authority PMA determines the suitability and applicability of this CPS.

1.5.4 CPS Approval Procedure

Approval of this CPS and subsequent amendments shall be made by the PMA. Amendments shall either be in the form of a document containing an amended form of the CPS or an update notice. Amended versions or updates shall be linked to the Practices Updates and Notices section of the VeriSign Repository located at: https://www.verisign.com/repository/updates. Updates supersede any designated or conflicting provisions of the referenced version of the CPS. The PMA shall determine whether changes to the CPS require a change in the Certificate policy object identifiers of the Certificate policies corresponding to each Class of Certificate.

1.6 Definitions and Acronyms

See Appendix A for a table of acronyms and definitions

2. Publication and Repository Responsibilities

2.1 Repositories

VeriSign is responsible for the repository functions for its own CAs and the CAs of its Enterprise Customers (either Managed PKI or ASB customers). VeriSign publishes Certificates it issues to end-user Subscribers in the repository in accordance with CPS § 2.6.

Upon revocation of an end-user Subscriber's Certificate, VeriSign publishes notice of such revocation in the repository. VeriSign issues CRLs for its own CAs and the CAs of Service Centers and Enterprise Customers within its Subdomain, pursuant to the provisions of this CPS. In addition, Enterprise Customers who have contracted for Online Certificate Status Protocol ("OCSP") services, VeriSign provides OCSP services pursuant to the provisions of this CPS.

2.2 Publication of Certificate Information

VeriSign maintains a web-based repository that permits Relying Parties to make online inquiries regarding revocation and other Certificate status information. VeriSign provides Relying Parties with information on how to find the appropriate repository to check Certificate status and, if OCSP (Online Certificate Status Protocol) is available, how to find the right OCSP responder.

VeriSign publishes the Certificates it issues on behalf of its own CAs, and the CAs of Client Service Centers in their Subdomain. Upon revocation of an end-user Subscriber's Certificate, VeriSign shall publish notice of such revocation in the repository. In addition, VeriSign issues Certificate Revocation Lists (CRLs) and, if available, provide OCSP services (Online Certificate Status Protocol) for its own CAs and the CAs of Service Centers within its Subdomain.

VeriSign will at all times publish a current version of:

- This VTN CP
- Its CPS,
- Subscriber Agreements,
- Relying Party Agreements

VeriSign is responsible for the repository function for:

- VeriSign's Public Primary Certification Authorities (PCAs) and VeriSign Infrastructure/Administrative CAs supporting the VTN, and
- VeriSign's CAs and Enterprise Customers' CAs that issue Certificates within VeriSign's Subdomain of the VTN.

VeriSign publishes certain CA information in the repository section of VeriSign's web site at http://www.verisign/com/repository/ as described below.

VeriSign publishes the VTN CP, this CPS, Subscriber Agreements, and Relying Party Agreements in the repository section of VeriSign's web site.

VeriSign publishes Certificates in accordance with Table 3 below.

Certificate Type	***Publication Requirements***
VeriSign PCA and VeriSign Issuing Root CA Certificates	Available to Relying Parties through inclusion in current browser software and as part of a Certificate Chain that can be obtained with the end-user Subscriber Certificate through the query functions described below.
VeriSign Issuing CA Certificates	Available to Relying Parties as part of a Certificate Chain that can be obtained with the end-user Subscriber Certificate through the query functions described below.

Certificate Type	*Publication Requirements*
Certificate of the VeriSign CA supporting Managed PKI Lite Certificates and CA Certificates of Managed PKI Customers	Available through query of the VeriSign LDAP directory server at directory.verisign.com.
VeriSign OCSP Responder Certificates	Available through query of the VeriSign LDAP directory server at directory.verisign.com.
End-User Subscriber Certificates	Available to relying parties through query functions in the VeriSign repository at: https://digitalid.verisign.com/services/client/index.html and https://digitalid.verisign.com/services/server/search.htm. Also available through query of the VeriSign LDAP directory server at directory.verisign.com.
End-User Subscriber Certificates issued through Managed PKI Customers	Made available through the query functions listed above, although at the discretion of the Managed PKI Customer, the Certificate may be accessible only via a search using the Certificate's serial number.

Table 3 – Certificate Publication Requirements

2.3 Time or Frequency of Publication

Updates to this CPS are published in accordance with Section 9.12. Updates to Subscriber Agreements and Relying Party Agreements are published as necessary. Certificates are published upon issuance. Certificate status information is published in accordance with the provisions of this CPS.

2.4 Access Controls on Repositories

Information published in the repository portion of the VeriSign web site is publicly-accessible information. Read only access to such information is unrestricted. VeriSign requires persons to agree to a Relying Party Agreement or CRL Usage Agreement as a condition to accessing Certificates, Certificate status information, or CRLs. VeriSign has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying repository entries.

3. Identification and Authentication

3.1 Naming

Unless where indicated otherwise in this VTN CP, this CPS or the content of the digital certificate, names appearing in Certificates issued under VTN are authenticated.

3.1.1 Type of Names

VeriSign CA Certificates contain X.501 Distinguished Names in the Issuer and Subject fields. VeriSign CA Distinguished Names consist of the components specified in Table 4 below.

Attribute	*Value*
Country (C) =	"US" or not used.
Organization (O) =	"VeriSign, Inc." [5]
Organizational Unit (OU) =	VeriSign CA Certificates may contain multiple OU attributes. Such attributes may contain one or more of the following: • CA Name • VeriSign Trust Network • A statement referencing the applicable Relying Party Agreement governing terms of use of the Certificate and • A copyright notice. • Text to describe the type of Certificate.
State or Province (S) =	Not used.
Locality (L) =	Not used except for the VeriSign Commercial Software Publishers CA, which uses "Internet."
Common Name (CN) =	This attribute includes the CA Name (if the CA Name is not specified in an OU attribute) or is not used.

Table 4 – Distinguished Name Attributes in CA Certificates

End-user Subscriber Certificates contain an X.501 distinguished name in the Subject name field and consist of the components specified in Table 5 below.

Attribute	*Value*
Country (C) =	2 letter ISO country code or not used.
Organization (O) =	The Organization attribute is used as follows: • "VeriSign, Inc." for VeriSign OCSP Responder and optionally for individual Certificates that do not have an organization affiliation. • Subscriber organizational name for web server Certificates and individual Certificates that have an organization affiliation.
Organizational Unit (OU) =	VeriSign end-user Subscriber Certificates may contain multiple OU attributes. Such attributes may contain one or more of the following: • Subscriber organizational unit (for organizational Certificates and individual Certificates that have an organization affiliation) • VeriSign Trust Network • A statement referencing the applicable Relying Party Agreement governing terms of use of the Certificate • A copyright notice • "Authenticated by VeriSign" and "Member, VeriSign Trust Network" in Certificates whose applications were authenticated by VeriSign • "Persona Not Validated" for Class 1 Individual Certificates • Text to describe the type of Certificate.
State or Province (S) =	Indicates the Subscriber's State or Province (State is not a required field in certificates issued to individuals).
Locality (L) =	Indicates the Subscriber's Locality (Locality is not a required field in certificates issued to individuals).
Common Name (CN) =	This attribute includes:

[5] An exception to this is the Secure Server CA, which indicates "RSA Data Security, Inc.," but is now a VeriSign CA.

Attribute	*Value*
	• The OCSP Responder Name (for OCSP Responder Certificates) • Domain name (for web server Certificates) • Organization name (for code/object signing Certificates) • Name (for individual Certificates).
E-Mail Address (E) =	E-mail address for Class 1 individual Certificates and generally for MPKI Subscriber Certificates

Table 5 – Distinguished Name Attributes in End User Subscriber Certificates

The Common Name (CN=) component of the Subject distinguished name of end-user Subscriber Certificates is authenticated in the case of Class 2-3 Certificates.
The authenticated common name value included in the Subject distinguished names of organizational Certificates is a domain name (in the case of Secure Server IDs and Global Server IDs) or the legal name of the organization or unit within the organization.

The authenticated common name value included in the Subject distinguished name of a Class 3 Organizational ASB Certificate, however, is the generally accepted personal name of the organizational representative authorized to use the organization's private key, and the organization (O=) component is the legal name of the organization. The common name value included in the Subject distinguished name of individual Certificates represents the individual's generally accepted personal name.

3.1.2 Need for Names to be Meaningful

Class 2 and 3 end-user Subscriber Certificates contain names with commonly understood semantics permitting the determination of the identity of the individual or organization that is the Subject of the Certificate.

VeriSign CA certificates contain names with commonly understood semantics permitting the determination of the identity of the CA that is the Subject of the Certificate.

3.1.3 Anonymity or pseudonymity of Subscribers

The identity of Class 1 individual Subscribers is not authenticated. Class 1 subscribers may use pseudonyms. Unless when required by law or requested by a State or Government authority to protect the identity of certain end user subscribers (e.g., minors, or sensitive government employee information), Class 2 and 3 Subscribers are not permitted to use pseudonyms (names other than a Subscriber's true personal or organizational name). Each request for anonymity in a certificate will be evaluated on its merits by the PMA and, if allowed the certificate will indicate that identity has been authenticated but is protected.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation

3.1.5 Uniqueness of Names

VeriSign ensures that Subject Distinguished Names of Subscriber are unique within the domain of a specific CA through automated components of the Subscriber enrollment process. It is possible for a Subscriber to have two or more certificates with the same Subject Distinguished Name.

3.1.6 Recognition, Authentication, and Role of Trademarks

Certificate Applicants are prohibited from using names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. VeriSign, however, does not verify whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. VeriSign is entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The certificate applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate. The method to prove possession of a private key shall be PKCS #10, another cryptographically equivalent demonstration, or another VeriSign-approved method. This requirement does not apply where a key pair is generated by a CA on behalf of a Subscriber, for example where pregenerated keys are placed on smart cards.

3.2.2 Authentication of Organization identity

Whenever a certificate contains an organization name, the identity of the organization and other enrollment information provided by Certificate Applicants (except for Nonverified Subscriber Information) is confirmed in accordance with the procedures set forth in VeriSign's documented Validation Procedures.

At a minimum VeriSign shall:

- Determine that the organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government agency or competent authority that confirms the existence of the organization,
- Confirm by telephone, confirmatory postal mail, or comparable procedure to the Certificate Applicant certain information about the organization, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Certificate Applicant is authorized to do so. When a certificate includes the name of an individual as an authorized representative of the Organization, the employment of that individual and his/her authority to act on behalf of the Organization shall also be confirmed.

Where a domain name or e-mail address is included in the certificate VeriSign authenticates the Organization's right to use that domain name either as a fully qualified Domain name or an e-mail domain.

Additional checks necessary to satisfy United States export regulations and licenses issued by the United States Department of Commerce Bureau of Industry and Science ("BIS") are performed by VeriSign and Affiliates when required.

Additional procedures are performed for specific types of Certificates as described in Table 6 below.

Certificate Type	***Additional Procedures***
OFX Server IDs	VeriSign verifies that the Organization is a bank or financial institution, or classified under one of the following SIC codes:

Certificate Type	*Additional Procedures*
	• 60xx Depository institutions • 61xx Nondepository credit institutions • 62xx Security, commodity brokers, and services • 63xx Insurance carriers • 64xx Insurance agents, brokers, and services • 67xx Holding and other investment offices • 7372 Prepackaged software • 7373 Computer integrated systems design • 7374 Data processing and preparation • 3661 Telephone and telegraph apparatus • 8721 Accounting, auditing, and bookkeeping.
Hardware Protected SSL Certificate	VeriSign verifies that the key pair was generated on FIPS 140 certified hardware
Managed PKI for Intranet SSL Certificate	VeriSign verifies that the host name or IP address assigned to a Device is not accessible from the Internet (publicly facing), and is owned by the Certificate Subscriber.
Authenticated Content Signing Certificate	Before VeriSign Digitally Signs any content using ACS it authenticates that the content is the original content signed by the Organization using its Code Signing Certificate.

Table 6 – Specific Authentication Procedures

3.2.3 Authentication of Individual Identity

Authentication of individual identity differs according to the Class of Certificate. The minimum authentication standard for each class of VTN certificate is explained in Table 7 below.

Certificate Class	Authentication of Identity
Class 1	No identity authentication. There is a limited confirmation of the Subscriber's e-mail address by requiring the Subscriber to be able to answer an e-mail to that address.
Class 2	Authenticate identity by matching the identity provided by the Subscriber to: • information residing in the database of a VeriSign-approved identity proofing service, such as a major credit bureau or other reliable source of information providing, or • information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals
Class 3	The authentication of Class 3 individual Certificates is based on the personal (physical) presence of the Certificate Applicant before an agent of the CA or RA, or before a notary public or other official with comparable authority within the Certificate Applicant's jurisdiction. The agent, notary or other official

	shall check the identity of the Certificate Applicant against a well-recognized form of government-issued photographic identification, such as a passport or driver's license and one other identification credential. The authentication of Class 3 Administrator certificates is based on authentication of the organization and a confirmation from the organization of the employment and authorization of the person to act as Administrator. VeriSign may also have occasion to approve Certificate Applications for their own Administrators. Administrators are "Trusted Persons" within an organization. In this case, authentication of their Certificate Applications shall be based on confirmation of their identity in connection with their employment or retention as an independent contractor and background checking procedures.[6]

Table 7. Authentication of individual identity

3.2.4 Non-Verified Subscriber information

Non-verified subscriber information includes:

- Organization Unit (OU)
- Subscriber's name in Class 1 certificates
- Any other information designated as non-verified in the certificate.

3.2.5 Validation of Authority

Whenever an individual's name is associated with an Organization name in a certificate in such a way to indicate the individual's affiliation or authorization to act on behalf of the Organization the VeriSign or a RA:

- determines that the organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization, and
- Uses information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to the organization, the employment with the Organization of the individual submitting the Certificate Application and, when appropriate, his/her authority to act on behalf of the Organization.

6 VeriSign may approve Administrator Certificates to be associated with a nonhuman recipient such as a device, or a server. Authentication of a Class 3 Administrator Certificate Applications for a non-human recipient shall include:
• Authentication of the existence and identity of the service named as the Administrator in the Certificate Application
• Authentication that the service has been securely implemented in a manner consistent with it performing an Administrative function
• Confirmation of the employment and authorization of the person enrolling for the Administrator certificate for the service named as Administrator in the Certificate Application.

3.2.6 Criteria for Interoperation

VeriSign may provide interoperation services that allow a non-VTN CA to be able to interoperate with the VTN by unilaterally certifying that CA. CAs enabled to interoperate in this way will comply with the VTN CP as supplemented by additional policies when required.

VeriSign shall only allow interoperation with the VTN of a non-VeriSign CA in circumstances where the CA, at a minimum:

- Enters into a contractual agreement with VeriSign
- Operates under a CPS that meets VTN requirements for the classes of certificates it will issue
- Passes a compliance assessment before being allowed to interoperate
- Passes an annual compliance assessment for ongoing eligibility to interoperate.

3.3 Identification and Authentication for Re-key Requests

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to obtain a new certificate to maintain continuity of Certificate usage. VeriSign generally requires that the Subscriber generate a new key pair to replace the expiring key pair (technically defined as "rekey") However, in certain cases (i.e., for web server certificates) Subscribers may request a new certificate for an existing key pair (technically defined as "renewal").

Generally speaking, both "Rekey" and "Renewal" are commonly described as "Certificate Renewal", focusing on the fact that the old Certificate is being replaced with a new Certificate and not emphasizing whether or not a new key pair is generated. For all Classes and Types of VeriSign Certificates, except for Class 3 Server Certificates, this distinction is not important as a new key pair is always generated as part of VeriSign's end-user Subscriber Certificate replacement process. However, for Class 3 Server Certificates, because the Subscriber key pair is generated on the web server and most web server key generation tools permit the creation of a new Certificate Request for an existing key pair, there is a distinction between "rekey" and "renewal."

3.3.1 Identification and Authentication for Routine Re-key

Re-key procedures ensure that the person or organization seeking to rekey an end-user Subscriber Certificate is in fact the Subscriber of the Certificate.

One acceptable procedure is through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. Subscribers choose and submit with their enrollment information a Challenge Phrase. Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's reenrollment information, and the enrollment information (including Corporate and Technical contact information) has not changed, a renewal Certificate is automatically issued.

After rekeying or renewal in this fashion, and on at least alternative instances of subsequent rekeying or renewal thereafter, VeriSign or the RA reconfirms the identity of the Subscriber in accordance with the identification and authentication requirements of an original Certificate Application. [7]

In particular, for subsequent renewal requests for Class 3 Organizational certificates, VeriSign reauthenticates the Organization name and domain name included in the certificate. In circumstances where:

[7] The authentication of a request to rekey/renew a Class 3 Organizational ASB Certificate, however, requires the use of a Challenge Phrase as well as the same identification and authentication as for the original Certificate Application.

- The challenge phrase is correctly used for the subsequent renewal certificate and:
- The certificate Distinguished Name has not been changed, and
- The Corporate and Technical Contact information remains unchanged from that which was previously verified,

VeriSign will not have to reconfirm by telephone, confirmatory postal mail, or comparable procedure to the Certificate Applicant certain information about the organization, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Certificate Applicant is authorized to do so."

Rekey after 30-days from expiration of the Certificate are reauthenticated as an original Certificate Application and are not automatically issued.

3.3.2 Identification and Authentication for Re-key After Revocation

Re-key/renewal after revocation is not permitted if the revocation occurred because:

- the Certificate (other than a Class 1 Certificate) was issued to a person other than the one named as the Subject of the Certificate, or
- the Certificate (other than a Class 1 Certificate) was issued without the authorization of the person or entity named as the Subject of such Certificate, or
- the entity approving the Subscriber's Certificate Application discovers or has reason to believe that a material fact in the Certificate Application is false. or
- For any other reason deemed necessary by VeriSign to protect the VTN

Subject to the foregoing paragraph, renewal of an organizational or CA Certificate following revocation of the Certificate is permissible as long as renewal procedures ensure that the organization or CA seeking renewal is in fact the Subscriber of the Certificate. Renewed organizational Certificates shall contain the same Subject distinguished name as the Subject distinguished name of the organizational Certificate being renewed.

Renewal of an individual Certificate following revocation must ensure that the person seeking renewal is, in fact, the Subscriber. One acceptable procedure is the use of a Challenge Phrase (or the equivalent thereof). Other than this procedure or another VeriSign-approved procedure, the requirements for the identification and authentication of an original Certificate Application shall be used for renewing a Certificate following revocation.

3.4 Identification and Authentication for Revocation Request

Prior to the revocation of a Certificate, VeriSign verifies that the revocation has been requested by the Certificate's Subscriber, the entity that approved the Certificate Application.

Acceptable procedures for authenticating the revocation requests of a Subscriber include:

- Having the Subscriber for certain certificate types submit the Subscriber's Challenge
- Phrase (or the equivalent thereof), and revoking the Certificate automatically if it matches
- the Challenge Phrase (or the equivalent thereof) on record
- Receiving a message from the Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked,
- Communication with the Subscriber providing reasonable assurances in light of the Class of Certificate that the person or organization requesting revocation is, in fact the Subscriber. Such communication, depending on the circumstances, may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

VeriSign Administrators are entitled to request the revocation of end-user Subscriber Certificates within VeriSign's sub domain. VeriSign authenticates the identity of Administrators via access control using SSL and client authentication before permitting them to perform revocation functions, or another VTN-approved procedure.

RAs using an Automated Administration Software Module may submit bulk revocation requests to VeriSign. Such requests shall be authenticated via a digitally signed request signed with the private key in the RA's Automated Administration hardware token.

The requests to revoke a CA Certificate shall be authenticated by the VeriSign to ensure that the revocation has in fact been requested by the CA.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application?

Below is a list of people who may submit certificate applications:

- Any individual who is the subject of the certificate,
- Any authorized representative of an Organization or entity,
- Any authorized representative of a CA,
- Any authorized representative of an RA.

4.1.2 Enrollment Process and Responsibilities

4.1.2.1 End-user Certificate Subscribers

All end-user Certificate Subscribers shall manifest assent to the relevant Subscriber Agreement that contains representations and warranties described in Section 9.6.3 and undergo an enrollment process consisting of:

- completing a Certificate Application and providing true and correct information,
- generating, or arranging to have generated, a key pair,
- delivering his, her, or its public key, directly or through an RA, to VeriSign
- demonstrating possession of the private key corresponding to the public key delivered to VeriSign.

4.1.2.2 CA and RA Certificates

Subscribers of CA and RA Certificates enter into a contract with VeriSign. CA and RA Applicants shall provide their credentials to demonstrate their identity and provide contact information during the contracting process. During this contracting process or, at the latest, prior to the Key Generation Ceremony to create a CA or RA key pair, the applicant shall cooperate with VeriSign to determine the appropriate distinguished name and the content of the Certificates to be issued by the applicant.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

VeriSign or an RA shall perform identification and authentication of all required Subscriber information in terms of Section 3.2

4.2.2 Approval or Rejection of Certificate Applications

VeriSign or an RA will approve an application for a certificate if the following criteria are met:

- Successful identification and authentication of all required Subscriber information in terms of Section 3.2
- Payment has been received

VeriSign or an RA will reject a certificate application if:

- identification and authentication of all required Subscriber information in terms of Section 3.2 cannot be completed, or
- The Subscriber fails to furnish supporting documentation upon request
- The Subscriber fails to respond to notices within a specified time, or
- Payment has not been received, or
- The RA believes that issuing a certificate to the Subscriber may bring the VTN into disrepute

4.2.3 Time to Process Certificate Applications

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

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

A Certificate is created and issued following the approval of a Certificate Application by VeriSign or following receipt of an RA's request to issue the Certificate. VeriSign creates and issues to a Certificate Applicant a Certificate based on the information in a Certificate Application following approval of such Certificate Application.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

VeriSign shall, either directly or through an RA, notify Subscribers that they have created such Certificates, and provide Subscribers with access to the Certificates by notifying them that their Certificates are available. Certificates shall be made available to end-user Subscribers, either by allowing them to download them from a web site or via a message sent to the Subscriber containing the Certificate.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The following conduct constitutes certificate acceptance:

- Downloading a Certificate or installing a Certificate from a message attaching it constitutes the Subscriber's acceptance of the Certificate.
- Failure of the Subscriber to object to the certificate or its content constitutes certificate acceptance.

4.4.2 Publication of the Certificate by the CA

VeriSign publishes the Certificates it issues in a publicly accessible repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

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

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Use of the Private key corresponding to the public key in the certificate shall only be permitted once the Subscriber has agreed to the Subscriber agreement and accepted the certificate. The certificate shall be used lawfully in accordance with VeriSign's Subscriber Agreement the terms of the VTN CP and this CPS. Certificate use must be consistent with the KeyUsage field extensions included in the certificate (e.g., if Digital Signature is not enabled then the certificate must not be used for signing).

Subscribers shall protect their private keys from unauthorized use and shall discontinue use of the private key following expiration or revocation of the certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties shall assent to the terms of the applicable relying party agreement as a condition of relying on the certificate.

Reliance on a certificate must be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Party must obtain such assurances for such reliance to be deemed reasonable.

Before any act of reliance, Relying Parties shall independently assess:

- the appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by this CPS. VeriSign is not responsible for assessing the appropriateness of the use of a Certificate.
- That the certificate is being used in accordance with the KeyUsage field extensions included in the certificate (e.g., if Digital Signature is not enabled then the certificate may not be relied upon for validating a Subscriber's signature).
- The status of the certificate and all the CAs in the chain that issued the certificate. If any of the Certificates in the Certificate Chain have been revoked, the Relying Party is solely responsible to investigate whether reliance on a digital signature performed by an end-user Subscriber Certificate prior to revocation of a Certificate in the Certificate chain is reasonable. Any such reliance is made solely at the risk of the Relying party.

Assuming that the use of the Certificate is appropriate, Relying Parties shall utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations they wish to perform, as a condition of relying on Certificates in connection with each such operation. Such operations include identifying a Certificate Chain and verifying the digital signatures on all Certificates in the Certificate Chain.

4.6 Certificate Renewal

Certificate renewal is the issuance of a new certificate to the subscriber without changing the public key or any other information in the certificate. Certificate renewal is supported for Class 3 certificates where the key pair is generated on a web server as most web server key generation tools permit the creation of a new Certificate Request for an existing key pair.

4.6.1 Circumstances for Certificate Renewal

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to renew a new certificate to maintain continuity of Certificate usage. A certificate may also be renewed after expiration.

4.6.2 Who May Request Renewal

Only the subscriber for an individual certificate or an authorized representative for an Organizational certificate may request certificate renewal

4.6.3 Processing Certificate Renewal Requests

Renewal procedures ensure that the person or organization seeking to renew an end-user Subscriber Certificate is in fact the Subscriber (or authorized by the Subscriber) of the Certificate.

One acceptable procedure is through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. Subscribers choose and submit with their enrollment information a Challenge Phrase (or the equivalent thereof). Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's reenrollment information, and the enrollment information (including Corporate and Technical contact information[8]) has not changed, a renewal Certificate is automatically issued. After renewal in this fashion, and on at least alternative instances of subsequent renewal thereafter, VeriSign or an RA shall reconfirm the identity of the Subscriber in accordance with the requirements specified in this CPS for the authentication of an original Certificate Application.

In particular, for subsequent renewal requests for Class 3 Organizational certificates, VeriSign reauthenticates the Organization name and domain name included in the certificate. In circumstances where:

- The challenge phrase is correctly used for the subsequent renewal certificate and:
- The certificate Distinguished Name has not been changed, and
- The Corporate and Technical Contact information remains unchanged from that which was previously verified,

VeriSign will not have to reconfirm by telephone, confirmatory postal mail, or comparable procedure to the Certificate Applicant certain information about the organization, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Certificate Applicant is authorized to do so."

Other than this procedure or another VeriSign-approved procedure, the requirements for the authentication of an original Certificate Application shall be used for renewing an end-user Subscriber Certificate.

4.6.4 Notification of New Certificate Issuance to Subscriber

Notification of issuance of certificate renewal to the Subscriber is in accordance with Section 4.3.2

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Conduct constituting Acceptance of a renewed certificate is in accordance with Section 4.4.1

[8] If contact information has changed via an approved formal contact change procedure the certificate shall still qualify for automated renewal.

4.6.6 Publication of the Renewal Certificate by the CA

The renewed certificate is published in VeriSign's publicly accessible repository.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

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

4.7 Certificate Re-Key

Certificate rekey is the application for the issuance of a new certificate that certifies the new public key. Certificate rekey is supported for all certificate Classes.

4.7.1 Circumstances for Certificate Re-Key

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to Re-key the certificate to maintain continuity of Certificate usage. A certificate may also be re-keyed after expiration.

4.7.2 Who May Request Certification of a New Public Key

Only the subscriber for an individual certificate or an authorized representative for an Organizational certificate may request certificate renewal

4.7.3 Processing Certificate Re-Keying Requests

Re-key procedures ensure that the person or organization seeking to renew an end-user Subscriber Certificate is in fact the Subscriber (or authorized by the Subscriber) of the Certificate.

One acceptable procedure is through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. Subscribers choose and submit with their enrollment information a Challenge Phrase (or the equivalent thereof). Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's reenrollment information, and the enrollment information (including contact information[9]) has not changed, a renewal Certificate is automatically issued. Subject to the provisions of Section 3.3.1, after re-keying in this fashion, and on at least alternative instances of subsequent re-keying thereafter, VeriSign or an RA shall reconfirm the identity of the Subscriber in accordance with the requirements specified in this CPS for the authentication of an original Certificate Application.

Other than this procedure or another VeriSign-approved procedure, the requirements for the authentication of an original Certificate Application shall be used for re-keying an end-user Subscriber Certificate.

4.7.4 Notification of New Certificate Issuance to Subscriber

Notification of issuance of a re-keyed certificate to the Subscriber is in accordance with Section 4.3.2

[9] If contact information has changed via an approved formal contact change procedure the certificate shall still qualify for automated renewal.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Conduct constituting Acceptance of a re-keyed certificate is in accordance with Section 4.4.1

4.7.6 Publication of the Re-Keyed Certificate by the CA

The re-keyed certificate is published in VeriSign's publicly accessible repository.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

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

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Certificate modification refers to the application for the issuance of a new certificate due to changes in the information in an existing certificate (other than the subscriber's public key).

Certificate modification is considered a Certificate Application in terms of Section 4.1.

4.8.2 Who May Request Certificate Modification

See Section 4.1.1

4.8.3 Processing Certificate Modification Requests

VeriSign or an RA shall perform identification and authentication of all required Subscriber information in terms of Section 3.2

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See Section 4.4.1

4.8.6 Publication of the Modified Certificate by the CA

See Section 4.4.2

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Only in the circumstances listed below, will an end-user Subscriber certificate be revoked by VeriSign (or by the Subscriber) and published on a CRL. Upon request from a subscriber who

can no longer use (or no longer wishes to use) a certificate for a reason other than one mentioned below, VeriSign will flag the certificate as inactive in its database but will not publish the certificate on a CRL.

An end-user Subscriber Certificate is revoked if:

- VeriSign, a Customer, or a Subscriber has reason to believe or strongly suspects that there has been a Compromise of a Subscriber's private key,
- VeriSign or a Customer has reason to believe that the Subscriber has materially breached a material obligation, representation, or warranty under the applicable Subscriber Agreement,
- The Subscriber Agreement with the Subscriber has been terminated,
- The affiliation between an Enterprise Customer with a Subscriber is terminated or has otherwise ended,
- The affiliation between an organization that is a Subscriber of a Class 3 Organizational ASB Certificate and the organizational representative controlling the Subscriber's private key is terminated or has otherwise ended,
- VeriSign or a Customer has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by the applicable CPS, the Certificate (other than a Class 1 Certificate) was issued to a person other than the one named as the Subject of the Certificate, or the Certificate (other than a Class 1 Certificate) was issued without the authorization of the person named as the Subject of such Certificate,
- VeriSign or a Customer has reason to believe that a material fact in the Certificate Application is false,
- VeriSign or a Customer determines that a material prerequisite to Certificate Issuance was neither satisfied nor waived,
- In the case of Class 3 organizational Certificates, the Subscriber's organization name changes,
- The information within the Certificate, other than Nonverified Subscriber Information, is incorrect or has changed, or
- The continued use of that certificate is harmful to the VTN.

When considering whether certificate usage is harmful to the VTN, VeriSign considers, among other things, the following:

- The nature and number of complaints received
- The identity of the complainant(s)
- Relevant legislation in force
- Responses to the alleged harmful use from the Subscriber

When considering whether the use of a Code Signing Certificate is harmful to the VTN, VeriSign additionally considers, among other things, the following:

- The name of the code being signed
- The behavior of the code
- Methods of distributing the code
- Disclosures made to recipients of the code
- Any additional allegations made about the code

VeriSign may also revoke an Administrator Certificate if the Administrator's authority to act as Administrator has been terminated or otherwise has ended.

VeriSign Subscriber Agreements require end-user Subscribers to immediately notify VeriSign of a known or suspected compromise of its private key.

4.9.2 Who Can Request Revocation

Individual Subscribers can request the revocation of their own individual Certificates. In the case of organizational Certificates, a duly authorized representative of the organization shall be entitled to request the revocation of Certificates issued to the organization. A duly authorized representative of VeriSign or a RA shall be entitled to request the revocation of an RA Administrator's Certificate. The entity that approved a Subscriber's Certificate Application shall also be entitled to revoke or request the revocation of the Subscriber's Certificate.

Only VeriSign is entitled to request or initiate the revocation of the Certificates issued to its own CAs. RAs are entitled, through their duly authorized representatives, to request the revocation of their own Certificates, and their Superior Entities shall be entitled to request or initiate the revocation of their Certificates.

4.9.3 Procedure for Revocation Request

4.9.3.1 Procedure for Requesting the Revocation of an End-User Subscriber Certificate

An end-user Subscriber requesting revocation is required to communicate the request to the VeriSign or the Customer approving the Subscriber's Certificate Application, who in turn will initiate revocation of the certificate promptly. For Enterprise customers, the Subscriber is required to communicate the request to the Enterprise Administrator who will communicate the revocation request to VeriSign for processing. Communication of such revocation request shall be in accordance with CPS § 3.4.

Where an Enterprise Customer initiates revocation of an end-user Subscriber Certificate upon its own initiative, the Managed PKI Customer or ASB Customer instructs VeriSign to revoke the Certificate.

4.9.3.2 Procedure for Requesting the Revocation of a CA or RA Certificate

A CA or RA requesting revocation of its CA or RA Certificate is required to communicate the request to VeriSign. VeriSign will then revoke the Certificate. VeriSign may also initiate CA or RA Certificate revocation.

4.9.4 Revocation Request Grace Period

Revocation requests shall be submitted as promptly as possible within a commercially reasonable time.

4.9.5 Time within Which CA Must Process the Revocation Request

VeriSign takes commercially reasonable steps to process revocation requests without delay.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying Parties shall check the status of Certificates on which they wish to rely. One method by which Relying Parties may check Certificate status is by consulting the most recent CRL from the CA that issued the Certificate on which the Relying Party wishes to rely. Alternatively, Relying Parties may meet this requirement either by checking Certificate status using the applicable web-based repository or by using OCSP (if available). CAs shall provide Relying Parties with information on how to find the appropriate CRL, web-based repository, or OCSP responder (where available) to check for revocation status.

4.9.7 CRL Issuance Frequency

CRLs for end-user Subscriber Certificates are issued at least once per day. CRLs for CA Certificates shall be issued at least quarterly, but also whenever a CA Certificate is revoked. CRLs for Authenticated Content Signing (ACS) root CAs are published annually and also whenever a CA Certificate is revoked. If a Certificate listed in a CRL expires, it may be removed from later-issued CRLs after the Certificate's expiration.

4.9.8 Maximum Latency for CRLs

CRLs are posted to the repository within a commercially reasonable time after generation. This is generally done automatically within minutes of generation.

4.9.9 On-Line Revocation/Status Checking Availability

Online revocation and other Certificate status information are available via a web-based repository and, where offered, OCSP. In addition to publishing CRLs, VeriSign provides Certificate status information through query functions in the VeriSign repository.

Certificate status information is available though web-based query functions accessible through the VeriSign Repository at

- **https://digitalid.verisign.com/services/client/index.html** (for Individual Certificates) and
- **https://digitalid.verisign.com/services/server/search.htm** (for Server and Developer Certificates).

VeriSign also provides OCSP Certificate status information. Enterprise Customers who contract for OCSP services may check Certificate status through the use of OCSP. The URL for the relevant OCSP Responder is communicated to the Enterprise Customer.

4.9.10 On-Line Revocation Checking Requirements

A relying party must check the status of a certificate on which he/she/it wishes to rely. If a Relying Party does not check the status of a Certificate on which the Relying Party wishes to rely by consulting the most recent relevant CRL, the Relying Party shall check Certificate status by consulting the applicable repository or by requesting Certificate status using the applicable OCSP responder (where OCSP services are available).

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable

4.9.12 Special Requirements regarding Key Compromise

VeriSign uses commercially reasonable efforts to notify potential Relying Parties if it discovers, or have reason to believe, that there has been a Compromise of the private key of one of their own CAs or one of the CAs within their subdomains.

4.9.13 Circumstances for Suspension

Not applicable

4.9.14 Who Can Request Suspension

Not applicable

4.9.15 Procedure for Suspension Request

Not applicable

4.9.16 Limits on Suspension Period

Not applicable

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The Status of public certificates is available via CRL at VeriSign's website, LDAP directory and via an OCSP responder (where available).

4.10.2 Service Availability

Certificate Status Services are available 24×7 without scheduled interruption.

4.10.3 Optional Features

OCSP is an optional status service feature that is not available for all products and must be specifically enabled for other products

4.11 End of Subscription

A subscriber may end a subscription for a VeriSign certificate by:

- Allowing his/her/its certificate to expire without renewing or re-keying that certificate
- Revoking of his/her/its certificate before certificate expiration without replacing the certificates.

4.12 Key Escrow and Recovery

With the exception of enterprises deploying Managed PKI Key Management Services no VTN participant may escrow CA, RA or end-user Subscriber private keys.

Enterprise customers using Managed PKI Key Management Service can escrow copies of the private keys of Subscribers whose Certificate Applications they approve. VeriSign does not store copies of Subscriber private keys but plays an important role in the Subscriber key recovery process.

4.12.1 Key Escrow and Recovery Policy and Practices

Enterprise customers using the Managed PKI Key Management service (or an equivalent service approved by VeriSign) are permitted to escrow end-user Subscribers' private key. Escrowed private keys shall be stored in encrypted form using the Managed PKI Key Manager software. Except for enterprise customers using the Managed PKI Key Manager Service (or an equivalent service approved by VeriSign), the private keys of CAs or end-user Subscribers shall not be escrowed.

End-user Subscriber private keys shall only be recovered under the circumstances permitted within the Managed PKI Key Management Service Administrator's Guide, under which:

- Enterprise customers using Managed PKI Key Manager shall confirm the identity of any person purporting to be the Subscriber to ensure that a purported Subscriber request for the Subscriber's private key is, in fact, from the Subscriber and not an imposter,
- Enterprise customers shall recover a Subscriber's private key without the Subscriber's authority only for their legitimate and lawful purposes, such as to comply with judicial or administrative process or a search warrant, and not for any illegal, fraudulent, or other wrongful purpose, and
- Such Enterprise customers shall have personnel controls in place to prevent Key Management Service Administrators and other persons from obtaining unauthorized access to private keys.

It is recommended that Enterprise Customers using KMS:

- Notify the subscribers that their private keys are escrowed
- Protect subscribers' escrowed keys from unauthorized disclosure,
- Protect all information, including the administrator's own key(s) that could be used to recover subscribers' escrowed keys.
- Release subscribers' escrowed keys only for properly authenticated and authorized requests for recovery.
- Revoke the Subscriber's Key pair prior to recovering the encryption key.
- Not be required to communicate any information concerning a key recovery to the subscriber except when the subscriber him/herself has requested recovery.
- Not disclose or allow to be disclosed escrowed keys or escrowed key-related information to any third party unless required by the law, government rule, or regulation; by the enterprise's organization policy; or by order of a court of competent jurisdiction.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Private keys are stored on the enterprise's premises in encrypted form[10]. Each Subscriber's private key is individually encrypted with its own triple-DES symmetric key. A Key Escrow Record (KER) is generated, then the triple-DES key is combined with a random session key mask generated in hardware and destroyed. Only the resulting masked session key (MSK) is securely sent and stored at VeriSign. The KER (containing the end user's private key) and the random session key mask are stored in the Key Manager database on the enterprise premises.

Recovery of a private key and digital certificate requires the Managed PKI administrator to securely log on to the Managed PKI Control Center, select the appropriate key pair to recover and click a "recover" hyperlink. Only after an approved administrator clicks the "recover" link is the MSK for that key pair returned from the Managed PKI database operated out of VeriSign's secure data center. The Key Manager combines the MSK with the random session key mask and regenerates the triple-DES key which was used to originally encrypt the private key, allowing recovery of the end user's private key. As a final step, an encrypted PKCS#12 file is returned to the administrator and ultimately distributed to the end user.

[10] In Limited circumstances, and only when expressly authorized through an Enterprise Service Agreement, VeriSign may host an Enterprise's Key Management Service and associated escrowed private keys.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

VeriSign has implemented the VeriSign Physical Security Policy, which supports the security requirements of this CPS. Compliance with these policies is included in the VeriSign's independent audit requirements described in Section 8. The VeriSign Physical Security Policy contains sensitive security information and is only available upon agreement with VeriSign. An overview of the requirements are described below.

5.1.1 Site Location and Construction

VeriSign CA and RA operations are conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems whether covert or overt.

VeriSign also maintains disaster recovery facilities for its CA operations. VeriSign's disaster recovery facilities are protected by multiple tiers of physical security comparable to those of VeriSign's primary facility.

5.1.2 Physical Access

VeriSign CA systems are protected by a minimum of four tiers of physical security, with access to the lower tier required before gaining access to the higher tier.

Progressively restrictive physical access privileges control access to each tier. Sensitive CA operational activity, any activity related to the lifecycle of the certification process such as authentication, verification, and issuance, occur within very restrictive physical tiers. Access to each tier requires the use of a proximity card employee badge. Physical access is automatically logged and video recorded. Additional tiers enforce individual access control through the use of two factor authentication including biometrics. Unescorted personnel, including untrusted employees or visitors, are not allowed into such secured areas.

The physical security system includes additional tiers for key management security which serves to protect both online and offline storage of CSUs and keying material. Areas used to create and store cryptographic material enforce dual control, each through the use of two factor authentication including biometrics. Online CSUs are protected through the use of locked cabinets. Offline CSUs are protected through the use of locked safes, cabinets and containers. Access to CSUs and keying material is restricted in accordance with VeriSign's segregation of duties requirements. The opening and closing of cabinets or containers in these tiers is logged for audit purposes.

5.1.3 Power and Air Conditioning

VeriSign's secure facilities are equipped with primary and backup:

- power systems to ensure continuous, uninterrupted access to electric power and
- heating/ventilation/air conditioning systems to control temperature and relative humidity.

5.1.4 Water Exposures

VeriSign has taken reasonable precautions to minimize the impact of water exposure to VeriSign systems.

5.1.5 Fire Prevention and Protection

VeriSign has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. VeriSign's fire prevention and protection measures have been designed to comply with local fire safety regulations.

5.1.6 Media Storage

All media containing production software and data, audit, archive, or backup information is stored within VeriSign facilities or in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic).

5.1.7 Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance the manufacturers' guidance prior to disposal. Other waste is disposed of in accordance with VeriSign's normal waste disposal requirements.

5.1.8 Off-Site Backup

VeriSign performs routine backups of critical system data, audit log data, and other sensitive information. Offsite backup media are stored in a physically secure manner using a bonded third party storage facility and VeriSign's East Coast disaster recovery facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted Persons include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations that may materially affect:

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, renewal requests, or enrollment information;
- the issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository;
- the handling of Subscriber information or requests.

Trusted Persons include, but are not limited to:

- customer service personnel,
- cryptographic business operations personnel,
- security personnel,
- system administration personnel,
- designated engineering personnel, and
- executives that are designated to manage infrastructural trustworthiness.

VeriSign considers the categories of personnel identified in this section as Trusted Persons having a Trusted Position. Persons seeking to become Trusted Persons by obtaining a Trusted Position must successfully complete the screening requirements set out in this CPS.

5.2.2 Number of Persons Required per Task

VeriSign has established, maintains, and enforces rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks.

Policy and control procedures are in place to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA cryptographic hardware (cryptographic signing unit or CSU) and associated key material, require multiple Trusted Persons.

These internal control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the device. Access to CA cryptographic hardware is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device. Persons with physical access to modules do not hold “Secret Shares” and vice versa.

Other manual operations such as the validation and issuance of Class 3 Certificates, not issued by an automated validation and issuance system, require the participation of at least 2 Trusted Persons, or a combination of at least one trusted person and an automated validation and issuance process.

5.2.3 Identification and Authentication for Each Role

For all personnel seeking to become Trusted Persons, verification of identity is performed through the personal (physical) presence of such personnel before Trusted Persons performing VeriSign HR or security functions and a check of well-recognized forms of identification (e.g., passports and driver’s licenses). Identity is further confirmed through the background checking procedures in CPS § 5.3.1.

VeriSign ensures that personnel have achieved Trusted Status and departmental approval has been given before such personnel are:

- issued access devices and granted access to the required facilities;
- issued electronic credentials to access and perform specific functions on VeriSign CA, RA, or other IT systems.

5.2.4 Roles Requiring Separation of Duties

Roles requiring Separation of duties include (but are not limited to)

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, or renewal requests, or enrollment information;
- the issuance, or revocation of Certificates, including personnel having access to restricted portions of the repository;
- the handling of Subscriber information or requests
- the generation, issuing or destruction of a CA certificate
- the loading of a CA on production

5.3 Personnel Controls

Personnel seeking to become Trusted Persons must present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities

competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts. Background checks are repeated at least every 5 years for personnel holding Trusted Positions.

5.3.1 Qualifications, Experience, and Clearance Requirements

VeriSign requires that personnel seeking to become Trusted Persons present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts.

5.3.2 Background Check Procedures

Prior to commencement of employment in a Trusted Role, VeriSign conducts background checks which include the following:

- confirmation of previous employment,
- check of professional reference,
- confirmation of the highest or most relevant educational degree obtained,
- search of criminal records (local, state or provincial, and national),
- check of credit/financial records,
- search of driver's license records, and
- search of Social Security Administration records.

To the extent that any of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law or other circumstances, VeriSign will utilize a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency.

The factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted Positions or for taking action against an existing Trusted Person generally include (but are not limited to) the following:

- Misrepresentations made by the candidate or Trusted Person,
- Highly unfavorable or unreliable professional references,
- Certain criminal convictions, and
- Indications of a lack of financial responsibility.

Reports containing such information are evaluated by human resources and security personnel, who determine the appropriate course of action in light of the type, magnitude, and frequency of the behavior uncovered by the background check. Such actions may include measures up to and including the cancellation of offers of employment made to candidates for Trusted Positions or the termination of existing Trusted Persons.

The use of information revealed in a background check to take such actions is subject to the applicable federal, state, and local laws.

5.3.3 Training Requirements

VeriSign provides its personnel with training upon hire as well as the requisite on-the-job training needed for them to perform their job responsibilities competently and satisfactorily. VeriSign maintains records of such training. VeriSign periodically reviews and enhances its training programs as necessary.

VeriSign's training programs are tailored to the individual's responsibilities and include the following as relevant:

- Basic PKI concepts,
- Job responsibilities,
- VeriSign security and operational policies and procedures,
- Use and operation of deployed hardware and software,
- Incident and Compromise reporting and handling, and
- Disaster recovery and business continuity procedures.

5.3.4 Retraining Frequency and Requirements

VeriSign provides refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

5.3.5 Job Rotation Frequency and Sequence

Not applicable

5.3.6 Sanctions for Unauthorized Actions

Appropriate disciplinary actions are taken for unauthorized actions or other violations of VeriSign policies and procedures. Disciplinary actions may include measures up to and including termination and are commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Independent Contractor Requirements

In limited circumstances, independent contractors or consultants may be used to fill Trusted Positions. Any such contractor or consultant is held to the same functional and security criteria that apply to a VeriSign employees in a comparable position.

Independent contractors and consultants who have not completed or passed the background check procedures specified in CPS § 5.3.2 are permitted access to VeriSign's secure facilities only to the extent they are escorted and directly supervised by Trusted Persons at all times.

5.3.8 Documentation Supplied to Personnel

VeriSign provides its employees the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

VeriSign manually or automatically logs the following significant events:

- CA key life cycle management events, including:
  - Key generation, backup, storage, recovery, archival, and destruction
  - Cryptographic device life cycle management events.
- CA and Subscriber certificate life cycle management events, including:
  - Certificate Applications, renewal, rekey, and revocation
  - Successful or unsuccessful processing of requests
  - Generation and issuance of Certificates and CRLs.
- Security-related events including:

- Successful and unsuccessful PKI system access attempts
- PKI and security system actions performed by VeriSign personnel
- Security sensitive files or records read, written or deleted
- Security profile changes
- System crashes, hardware failures and other anomalies
- Firewall and router activity
- CA facility visitor entry/exit.

Log entries include the following elements:

- Date and time of the entry
- Serial or sequence number of entry, for automatic journal entries
- Identity of the entity making the journal entry
- Kind of entry.

VeriSign RAs and Enterprise Administrators log Certificate Application information including:

- Kind of identification document(s) presented by the Certificate Applicant
- Record of unique identification data, numbers, or a combination thereof (e.g., Certificate Applicant's drivers license number) of identification documents, if applicable
- Storage location of copies of applications and identification documents
- Identity of entity accepting the application
- Method used to validate identification documents, if any
- Name of receiving CA or submitting RA, if applicable.

5.4.2 Frequency of Processing Log

Audit logs are examined on at least a weekly basis for significant security and operational events. In addition, VeriSign reviews its audit logs for suspicious or unusual activity in response to alerts generated based on irregularities and incidents within VeriSign CA and RA systems.

Audit log processing consists of a review of the audit logs and documentation for all significant events in an audit log summary. Audit log reviews include a verification that the log has not been tampered with, an inspection of all log entries, and an investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews are also documented.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained onsite for at least two (2) months after processing and thereafter archived in accordance with Section 5.5.2.

5.4.4 Protection of Audit Log

Audit logs are protected with an electronic audit log system that includes mechanisms to protect the log files from unauthorized viewing, modification, deletion, or other tampering.

5.4.5 Audit Log Backup Procedures

Incremental backups of audit logs are created daily and full backups are performed weekly.

5.4.6 Audit Collection System (Internal vs. External)

Automated audit data is generated and recorded at the application, network and operating system level. Manually generated audit data is recorded by VeriSign personnel.

5.4.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability Assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. Logical security vulnerability assessments ("LSVAs") are performed, reviewed, and revised following an examination of these monitored events. LSVAs are based on real-time automated logging data and are performed on a daily, monthly, and annual basis. An annual LSVA will be an input into an entity's annual Compliance Audit.

5.5 Records Archival

5.5.1 Types of Records Archived

VeriSign archives:

- All audit data collected in terms of Section 5.4
- Certificate application information
- Documentation supporting certificate applications
- Certificate lifecycle information e.g., revocation, rekey and renewal application information

5.5.2 Retention Period for Archive

Records shall be retained for at least the time periods set forth below following the date the Certificate expires or is revoked.

- Five (5) years for Class 1 Certificates,
- Ten (10) years and six (6) months for Class 2 and Class 3 Certificates

5.5.3 Protection of Archive

VeriSign protects the archive so that only authorized Trusted Persons are able to obtain access to the archive. The archive is protected against unauthorized viewing, modification, deletion, or other tampering by storage within a Trustworthy System. The media holding the archive data and the applications required to process the archive data shall be maintained to ensure that the archive data can be accessed for the time period set forth in this CPS.

5.5.4 Archive Backup Procedures

VeriSign incrementally backs up electronic archives of its issued Certificate information on a daily basis and performs full backups on a weekly basis. Copies of paper-based records shall be maintained in an off-site secure facility.

5.5.5 Requirements for Time-Stamping of Records

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

5.5.6 Archive Collection System (Internal or External)

VeriSign archive collection systems are internal, except for enterprise RA Customers. VeriSign assists its enterprise RAs in preserving an audit trail. Such an archive collection system therefore is external to that enterprise RA.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified when it is restored.

5.6 Key Changeover

VeriSign CA key pairs are retired from service at the end of their respective maximum lifetimes as defined in this CPS. VeriSign CA Certificates may be renewed as long as the cumulative certified lifetime of the CA key pair does not exceed the maximum CA key pair lifetime. New CA key pairs will be generated as necessary, for example to replace CA key pairs that are being retired, to supplement existing, active key pairs and to support new services.

Prior to the expiration of the CA Certificate for a Superior CA, key changeover procedures are enacted to facilitate a smooth transition for entities within the Superior CA's hierarchy from the old Superior CA key pair to new CA key pair(s). VeriSign's CA key changeover process requires that:

- A Superior CA ceases to issue new Subordinate CA Certificates no later than 60 days before the point in time ("Stop Issuance Date") where the remaining lifetime of the Superior CA key pair equals the approved Certificate Validity Period for the specific type(s) of Certificates issued by Subordinate CAs in the Superior CA's hierarchy.
- Upon successful validation of Subordinate CA (or end-user Subscriber) Certificate requests received after the "Stop Issuance Date," Certificates will be signed with a new CA key pair.

The Superior CA continues to issue CRLs signed with the original Superior CA private key until the expiration date of the last Certificate issued using the original key pair has been reached

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Backups of the following CA information shall be kept in off-site storage and made available in the event of a Compromise or disaster: Certificate Application data, audit data, and database records for all Certificates issued. Back-ups of CA private keys shall be generated and maintained in accordance with CP § 6.2.4. VeriSign maintains backups of the foregoing CA information for their own CAs, as well as the CAs of Enterprise Customers within its Subdomain.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to VeriSign Security and VeriSign's incident handling procedures are enacted. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, VeriSign's key compromise or disaster recovery procedures will be enacted.

5.7.3 Entity Private Key Compromise Procedures

Upon the suspected or known Compromise of a VeriSign CA, VeriSign infrastructure or Customer CA private key, VeriSign's Key Compromise Response procedures are enacted by the VeriSign

Security Incident Response Team (VSIRT). This team, which includes Security, Cryptographic Business Operations, Production Services personnel, and other VeriSign management representatives, assesses the situation, develops an action plan, and implements the action plan with approval from VeriSign executive management.

If CA Certificate revocation is required, the following procedures are performed:

- The Certificate's revoked status is communicated to Relying Parties through the VeriSign repository in accordance with CPS § 4.4.9,
- Commercially reasonable efforts will be made to provide additional notice of the revocation to all affected VTN Participants, and
- The CA will generate a new key pair in accordance with CPS § 4.7, except where the CA is being terminated in accordance with CPS § 5.8

5.7.4 Business Continuity Capabilities After a Disaster

VeriSign has implemented a disaster recovery site more than 1000 miles from VeriSign's principal secure facilities. VeriSign has developed, implemented and tested a disaster recovery plan to mitigate the effects of any kind of natural or man-made disaster. This plan is regularly tested, verified, and updated to be operational in the event of a disaster.

Detailed disaster recovery plans are in place to address the restoration of information systems services and key business functions. VeriSign's disaster recovery site has implemented the physical security protections and operational controls required by the VeriSign Security and Audit Requirements Guide to provide for a secure and sound backup operational setup.

In the event of a natural or man-made disaster requiring temporary or permanent cessation of operations from VeriSign's primary facility, VeriSign's disaster recovery process is initiated by the VeriSign Emergency Response Team (VERT).

VeriSign has the capability to restore or recover essential operations within twenty four (24) hours following a disaster with, at a minimum, support for the following functions:

- Certificate issuance,
- Certificate revocation,
- publication of revocation information, and
- provision of key recovery information for Enterprise Customers using Managed PKI Key Manager.

VeriSign's disaster recovery database is synchronized regularly with the production database within the time limits set forth in the Security and Audit Requirements Guide. VeriSign's disaster recovery equipment is protected by physical security protections comparable to the physical security tiers specified in CPS § 5.1.1.

VeriSign's disaster recovery plan has been designed to provide full recovery within one week following disaster occurring at VeriSign's primary site. VeriSign tests its equipment at its primary site to support CA/RA functions following all but a major disaster that would render the entire facility inoperable. Results of such tests are reviewed and kept for audit and planning purposes. Where possible, operations are resumed at VeriSign's primary site as soon as possible following a major disaster.

VeriSign maintains redundant hardware and backups of its CA and infrastructure system software at its disaster recovery facility. In addition, CA private keys are backed up and maintained for disaster recovery purposes in accordance with CPS § 6.2.4.

VeriSign maintains offsite backups of important CA information for VeriSign CAs as well as the CAs of Service Centers, and Enterprise Customers, within VeriSign's Subdomain. Such

information includes, but is not limited to: Certificate Application data, audit data (per Section 4.5), and database records for all Certificates issued.

5.8 CA or RA Termination

In the event that it is necessary for a VeriSign CA, or Enterprise Customer CA to cease operation, VeriSign makes a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination. Where CA termination is required, VeriSign and, in the case of a Customer CA, the applicable Customer, will develop a termination plan to minimize disruption to Customers, Subscribers, and Relying Parties. Such termination plans may address the following, as applicable:

- Provision of notice to parties affected by the termination, such as Subscribers, Relying Parties, and Customers, informing them of the status of the CA,
- Handling the cost of such notice,
- The revocation of the Certificate issued to the CA by VeriSign,
- The preservation of the CA's archives and records for the time periods required in this CPS,
- The continuation of Subscriber and customer support services,
- The continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services,
- The revocation of unexpired unrevoked Certificates of end-user Subscribers and subordinate CAs, if necessary,
- Refunding (if necessary) Subscribers whose unexpired unrevoked Certificates are revoked under the termination plan or provision, or alternatively, the issuance of replacement Certificates by a successor CA,
- Disposition of the CA's private key and the hardware tokens containing such private key, and
- Provisions needed for the transition of the CA's services to a successor CA.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

CA key pair generation is performed by multiple pre-selected, trained and trusted individuals using Trustworthy Systems and processes that provide for the security and required cryptographic strength for the generated keys. For PCA and Issuing Root CAs, the cryptographic modules used for key generation meet the requirements of FIPS 140-1 level 3. For other CAs (including VeriSign CAs and Managed PKI Customer CAs), the cryptographic modules used meet the requirements of at least FIPS 140-1 level 2.

All CA key pairs are generated in pre-planned Key Generation Ceremonies in accordance with the requirements of the Key Ceremony Reference Guide, the CA Key Management Tool User's Guide, and the VeriSign Security and Audit Requirements Guide. The activities performed in each key generation ceremony are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by VeriSign Management.

Generation of RA key pairs is generally performed by the RA using a FIPS 140-1 level 1 certified cryptographic module provided with their browser software.

Enterprise Customers generate the key pair used by their Automated Administration servers. VeriSign recommends that Automated Administration server key pair generation be performed using a FIPS 140-1 level 2 certified cryptographic module.

Generation of end-user Subscriber key pairs is generally performed by the Subscriber. For Class 1 Certificates, Class 2 Certificates, and Class 3 code/object signing Certificates, the Subscriber typically uses a FIPS 140-1 level 1 certified cryptographic module provided with their browser software for key generation. For server Certificates, the Subscriber typically uses the key generation utility provided with the web server software.

For ACS Application IDs, VeriSign generates a key pair on behalf of the Subscriber using a random numbers seed generated on a cryptographic module that meets the requirements of FIPS 140-1 level 3.

6.1.2 Private Key Delivery to Subscriber

When end-user Subscriber key pairs are generated by the end-user Subscriber, private key delivery to a Subscriber is not applicable. For ACS Application IDs, private key delivery to a Subscriber is also not applicable.

Where RA or end-user Subscriber key pairs are pre-generated by VeriSign on hardware tokens or smart cards, such devices are distributed to the RA or end-user Subscriber using a commercial delivery service and tamper evident packaging. The data required to activate the device is communicated to the RA or end-user Subscriber using an out of band process. The distribution of such devices is logged by VeriSign.

Where end-user Subscriber key pairs are pre-generated by Enterprise Customers on hardware tokens or smart cards, such devices are distributed to the end-user Subscriber using a commercial delivery service and tamper evident packaging. The required activation data required to activate the device is communicated to the RA or end-user Subscriber using an out of band process. The distribution of such devices is logged by the Enterprise Customer.

For Enterprise Customers using Managed PKI Key Manager for key recovery services, the Customer may generate encryption key pairs (on behalf of Subscribers whose Certificate Applications they approve) and transmit such key pairs to Subscribers via a password protected PKCS # 12 file.

6.1.3 Public Key Delivery to Certificate Issuer

End-user Subscribers and RAs submit their public key to VeriSign for certification electronically through the use of a PKCS#10 Certificate Signing Request (CSR) or other digitally signed package in a session secured by Secure Sockets Layer (SSL). Where CA, RA, or end-user Subscriber key pairs are generated by VeriSign, this requirement is not applicable.

6.1.4 CA Public Key Delivery to Relying Parties

VeriSign makes the CA Certificates for its PCAs and root CAs available to Subscribers and Relying Parties through their inclusion in web browser software. As new PCA and root CA Certificates are generated, VeriSign provides such new Certificates to the browser manufacturers for inclusion in new browser releases and updates.

VeriSign generally provides the full certificate chain (including the issuing CA and any CAs in the chain) to the end-user Subscriber upon Certificate issuance. VeriSign CA Certificates may also be downloaded from the VeriSign LDAP Directory at directory.verisign.com.

6.1.5 Key Sizes

Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs. The current VeriSign Standard for minimum key sizes is the use of key pairs equivalent in strength to 1024 bit RSA for PCAs and CAs, except for the legacy Secure Server CA whose key pair is 1000 bit RSA. VeriSign's third generation (G3) PCAs have 2048 bit RSA key pairs.

VeriSign recommends that Registration Authorities and end-user Subscribers generate 1024 bit RSA key pairs. VeriSign may not approve certain end entity certificates generated with a key pair size of 512 bit or less.

6.1.6 Public Key Parameters Generation and Quality Checking

Not applicable

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

Refer to Section 7.1.2.1.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

VeriSign has implemented a combination of physical, logical, and procedural controls to ensure the security of VeriSign and Enterprise Customer CA private keys. Subscribers are required by contract to take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys.

6.2.1 Cryptographic Module Standards and Controls

For PCA and Issuing Root CA key pair generation and CA private key storage, VeriSign uses hardware cryptographic modules that are certified at or meet the requirements of FIPS 140-1 Level 3.

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

VeriSign has implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations. VeriSign uses "Secret Sharing" to split the activation data needed to make use of a CA private key into separate parts called "Secret Shares" which are held by trained and trusted individuals called "Shareholders." A threshold number of Secret Shares (m) out of the total number of Secret Shares created and distributed for a particular hardware cryptographic module (n) is required to activate a CA private key stored on the module.

The threshold number of shares needed to sign a CA certificate is 3. It should be noted that the number of shares distributed for disaster recovery tokens may be less than the number distributed for operational tokens, while the threshold number of required shares remains the same. Secret Shares are protected in accordance with this CPS.

6.2.3 Private Key Escrow

CA private keys are not escrowed. Escrow of private keys for end user subscribers is explained in more detail in Section 4.12.

6.2.4 Private Key Backup

VeriSign creates backup copies of CA private keys for routine recovery and disaster recovery purposes. Such keys are stored in encrypted form within hardware cryptographic modules and associated key storage devices. Cryptographic modules used for CA private key storage meet the requirements of this CPS. CA private keys are copied to backup hardware cryptographic modules in accordance with this CPS.

Modules containing onsite backup copies of CA private keys are subject to the requirements of CPS. Modules containing disaster recovery copies of CA private keys are subject to the requirements of this CPS.

VeriSign does not store copies of RA private keys. For the backup of end-user Subscriber private keys, see Section 6.2.3 and Section 4.12. For ACS Application IDs, VeriSign does not store copies of Subscriber private keys.

6.2.5 Private Key Archival

When VeriSign CA key pairs reach the end of their validity period, such CA key pairs will be archived for a period of at least 5 years. Archived CA key pairs will be securely stored using hardware cryptographic modules that meet the requirements of this CPS. Procedural controls prevent archived CA key pairs from being returned to production use. Upon the end of the archive period, archived CA private keys will be securely destroyed in accordance with this CPS.

VeriSign does not archive copies of RA and Subscriber private keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

VeriSign generates CA key pairs on the hardware cryptographic modules in which the keys will be used. In addition, VeriSign makes copies of such CA key pairs for routine recovery and disaster recovery purposes. Where CA key pairs are backed up to another hardware cryptographic module, such key pairs are transported between modules in encrypted form.

6.2.7 Private Key Storage on Cryptographic Module

CA or RA private keys held on hardware cryptographic modules shall be stored in encrypted form.

6.2.8 Method of Activating Private Key

All VeriSign subdomain Participants shall protect the activation data for their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use.

6.2.8.1 Class 1 Certificates

The Standard for Class 1 private key protection is for Subscribers to take commercially reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization. In addition, VeriSign recommends that Subscribers use a password in accordance with Section 6.4.1 or security of equivalent strength to authenticate the Subscriber before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password, or a network logon password.

6.2.8.2 Class 2 Certificates

The Standard for Class 2 Private Key protection is for Subscribers to:

- Use a password in accordance with Section 6.4.1 or security of equivalent strength to authenticate the Subscriber before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password, a network logon password, or a password in conjunction with the VeriSign Roaming Service; and
- Take commercially reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization.

When deactivated, private keys shall be kept in encrypted form only.

6.2.8.3 Class 3 Certificates other than Administrator Certificates

The Standard for Class 3 private key protection (other than Administrators) is for Subscribers to:

- Use a smart card, biometric access device, or password in conjunction with the VeriSign Roaming Service, or security of equivalent strength to authenticate the Subscriber before the activation of the private key; and
- Take commercially reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization.

Use of a password along with a smart card or biometric access device in accordance with Section 6.4.1 is recommended. When deactivated, private keys shall be kept in encrypted form only.

6.2.8.4 Administrators' Private Keys (Class 3)

The Standard for Administrators' private key protection requires them to:

- Use a smart card, biometric access device, password in accordance with Section 6.4.1, or security of equivalent strength to authenticate the Administrator before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password, or a network logon password; and
- Take commercially reasonable measures for the physical protection of the Administrator's workstation to prevent use of the workstation and its associated private key without the Administrator's authorization.

VeriSign recommends that Administrators use a smart card, biometric access device, or security of equivalent strength along with the use of a password in accordance with Section 6.4.1 to authenticate the Administrator before the activation of the private key.

When deactivated, private keys shall be kept in encrypted form only.

6.2.8.5 Enterprise RAs using a Cryptographic Module (with Automated Administration or with Managed PKI Key Manager Service)

The Standard for private key protection for Administrators using such a cryptographic module requires them to:

- Use the cryptographic module along with a password in accordance with Section 6.4.1 to authenticate the Administrator before the activation of the private key; and
- Take commercially reasonable measures for the physical protection of the workstation housing the cryptographic module reader to prevent use of the workstation and the private key associated with the cryptographic module without the Administrator's authorization.

6.2.8.6 Private Keys Held by Processing Centers (Class 1-3)

An online CA's private key shall be activated by a threshold number of Shareholders, as defined in Section 6.2.2, supplying their activation data (stored on secure media). Once the private key is activated, the private key may be active for an indefinite period until it is deactivated when the CA goes offline. Similarly, a threshold number of Shareholders shall be required to supply their activation data in order to activate an offline CA's private key. Once the private key is activated, it shall be active only for one time.

6.2.9 Method of Deactivating Private Key

VeriSign CA private keys are deactivated upon removal from the token reader. VeriSign RA private keys (used for authentication to the RA application) are deactivated upon system log off. VeriSign RAs are required to log off their workstations when leaving their work area.

Client Administrators, RA, and end-user Subscriber private keys may be deactivated after each operation, upon logging off their system, or upon removal of a smart card from the smart card reader depending upon the authentication mechanism employed by the user. In all cases, end-user Subscribers have an obligation to adequately protect their private key(s) in accordance with this CPS. The private key associated with an ACS Application ID is deleted immediately after it has been used for code signing.

6.2.10 Method of Destroying Private Key

At the conclusion of a VeriSign CA's operational lifetime, one or more copies of the CA private key are archived in accordance with CPS § 6.2.5. Remaining copies of the CA private key are securely destroyed. In addition, archived CA private keys are securely destroyed at the conclusion of their archive periods. CA key destruction activities require the participation of multiple trusted individuals.

Where required, VeriSign destroys CA private keys in a manner that reasonably ensures that there are no residuals remains of the key that could lead to the reconstruction of the key. VeriSign utilizes the zeroization function of its hardware cryptographic modules and other appropriate means to ensure the complete destruction of CA private keys. When performed, CA key destruction activities are logged. The private key associated with an ACS Application ID is deleted immediately after it has been used for code signing.

6.2.11 Cryptographic Module Rating

See Section 6.2.1

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

VeriSign CA, RA and end-user Subscriber Certificates are backed up and archived as part of VeriSign's routine backup procedures.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Operational Period of a Certificate ends upon its expiration or revocation. The Operational Period for key pairs is the same as the Operational Period for the associated Certificates, except that they may continue to be used for decryption and signature verification. The maximum

Operational Periods for VeriSign Certificates for Certificates issued on or after the effective date of this CPS are set forth in Table 8 below.

In addition, VeriSign CAs stop issuing new Certificates at an appropriate date prior to the expiration of the CA's Certificate such that no Certificate issued by a Subordinate CA expires after the expiration of any Superior CA Certificates.

Certificate Issued By:	***Validity Period***
PCA self-signed (1024 bit)	Up to 30 years
PCA self-signed (2048 bit)	Up to 50 years
PCA to Offline intermediate CA	Generally 10 years but up to 15 years after renewal
PCA to online CA	Generally 5 years but up to 10 years after renewal[11]
Offline intermediate CA to online CA	Generally 5 years but up to 10 years after renewal[12]
Online CA to End-user Individual Subscriber	Normally up to 2 years, but under the conditions described below, up to 5 years[13]
Online CA to End-Entity Organizational Subscriber	Normally up to 2 years[1415]

Table 8 – Certificate Operational Periods

Except as noted in this section, VeriSign Subdomain Participants shall cease all use of their key pairs after their usage periods have expired.

Certificates issued by CAs to end-user Subscribers may have Operational Periods longer than two years, up to five years, if the following requirements are met:

- The Certificates are individual Certificates,
- Subscribers' key pairs reside on a hardware token, such as a smart card,
- Subscribers are required to undergo reauthentication at least every 25 months under Section 3.2.3,
- Subscribers shall prove possession of the private key corresponding to the public key within the Certificate at least every 25 months under Section 3.2.3,
- If a Subscriber is unable to complete reauthentication procedures successfully or is unable to prove possession of such private key when required by the foregoing, the CA shall revoke the Subscriber's Certificate.

VeriSign also operates a Secure Server CA as a legacy self-signed issuing root CA which is part of the VeriSign Trust Network and has an operational period of up to 15 years. End-user Subscriber Certificates issued by this CA meet the requirements for CA to end-user Subscriber Certificates specified in Table 8 above.

[11] The VeriSign Onsite Administrator CA-Class 3 has a validity beyond 10 years to support legacy systems and shall be revoked when appropriate

[12] If 5-year end-user subscriber certificates are issued, the online CA certificate's operational period will be 10 years with no option to renew. Re-key will be required after 5 years.

[13] If 5-year end-user subscriber certificates are issued, the online CA certificate's operational period will be 10 years with no option to renew. Re-key will be required after 5 years.

14 VeriSign may issue Organization Certificates with a three year validity. The Distinguished name of these Certificates shall be re-authenticated by VeriSign at least every 25-months.

[15] Organizational end-entity certificates used solely to support the operation of a portion of the VTN may be issued with a validity period of 5 year and up to a maximum of 10 years after renewal.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Activation data (Secret Shares) used to protect tokens containing VeriSign CA private keys is generated in accordance with the requirements of CPS § 6.2.2 and the Key Ceremony Reference Guide. The creation and distribution of Secret Shares is logged.

VeriSign RAs are required to select strong passwords to protect their private keys. VeriSign's password selection guidelines require that passwords:

- be generated by the user;
- have at least eight characters;
- have at least one alphabetic and one numeric character;
- have at least one lower-case letter;
- not contain many occurrences of the same character;
- not be the same as the operator's profile name; and
- not contain a long substring of the user's profile name.

VeriSign strongly recommends that Enterprise Administrators, RAs, and end-user Subscribers choose passwords that meet the same requirements. VeriSign also recommends the use of two factor authentication mechanisms (e.g., token and passphrase, biometric and token, or biometric and passphrase) for private key activation.

6.4.2 Activation Data Protection

VeriSign Shareholders are required to safeguard their Secret Shares and sign an agreement acknowledging their Shareholder responsibilities.

VeriSign RAs are required to store their Administrator/RA private keys in encrypted form using password protection and their browser's "high security" option.

VeriSign strongly recommends that Client Administrators, RAs and end-user Subscribers store their private keys in encrypted form and protect their private keys through the use of a hardware token and/or strong passphrase. The use of two factor authentication mechanisms (e.g., token and passphrase, biometric and token, or biometric and passphrase) is encouraged.

6.4.3 Other Aspects of Activation Data

6.4.3.1 Activation Data Transmission

To the extent activation data for private keys are transmitted, VTN Participants shall protect the transmission using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. To the extent Windows or network logon user name/password combination is used as activation data for an end-user Subscriber, the passwords transferred across a network shall be protected against access by unauthorized users.

6.4.3.2 Activation Data Destruction

Activation data for CA private keys shall be decommissioned using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of the private keys protected by such activation data. After the record retention periods in Section 5.5.2 lapse, VeriSign shall decommission activation data by overwriting and/or physical destruction.

6.5 Computer Security Controls

VeriSign performs all CA and RA functions using Trustworthy Systems that meet the requirements of VeriSign's Security and Audit Requirements Guide. Enterprise Customers must use Trustworthy Systems.

6.5.1 Specific Computer Security Technical Requirements

VeriSign ensures that the systems maintaining CA software and data files are Trustworthy Systems secure from unauthorized access. In addition, VeriSign limits access to production servers to those individuals with a valid business reason for such access. General application users do not have accounts on production servers.

VeriSign's production network is logically separated from other components. This separation prevents network access except through defined application processes. VeriSign uses firewalls to protect the production network from internal and external intrusion and limit the nature and source of network activities that may access production systems.

VeriSign requires the use of passwords that have a minimum character length and a combination of alphanumeric and special characters. VeriSign requires that passwords be changed on a periodic basis.

Direct access to VeriSign databases supporting VeriSign's CA Operations is limited to Trusted Persons in VeriSign's Production Operations group having a valid business reason for such access.

6.5.2 Computer Security Rating

A version of VeriSign's core Processing Center software has satisfied the EAL 4 assurance requirements of ISO/IEC 15408-3:1999, *Information technology - Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements*, based on an independent laboratory's Common Criteria evaluation of the software against the VeriSign Processing Center Security Target. VeriSign may, from time to time, evaluate new releases of the Processing Center software under the Common Criteria.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Applications are developed and implemented by VeriSign in accordance with VeriSign systems development and change management standards. VeriSign also provides software to its Enterprise Customers for performing RA and certain CA functions. Such software is developed in accordance with VeriSign system development standards.

VeriSign developed software, when first loaded, provides a method to verify that the software on the system originated from VeriSign, has not been modified prior to installation, and is the version intended for use.

6.6.2 Security Management Controls

VeriSign has mechanisms and/or policies in place to control and monitor the configuration of its CA systems. VeriSign creates a hash of all software packages and VeriSign software updates. This hash is used to verify the integrity of such software manually. Upon installation and periodically thereafter, VeriSign validates the integrity of its CA systems.

6.6.3 Life Cycle Security Controls

No stipulation

6.7 Network Security Controls

VeriSign performs all its CA and RA functions using networks secured in accordance with the Security and Audit Requirements Guide to prevent unauthorized access and other malicious activity. VeriSign protects its communications of sensitive information through the use of encryption and digital signatures.

6.8 Time-Stamping

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

VeriSign Certificates conform to (a) ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 and (b) RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 ("RFC 3280").

At a minimum, X.509 Certificates shall contain the basic fields and indicated prescribed values or value constraints in Table 9 below:

Field	***Value or Value constraint***
Serial Number	Unique value per Issuer DN
Signature Algorithm	Object identifier of the algorithm used to sign the certificate (See CP § 7.1.3)
Issuer DN	See Section 7.1.4
Valid From	Universal Coordinate Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 3280.
Valid To	Universal Coordinate Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 3280.
Subject DN	See CP § 7.1.4
Subject Public Key	Encoded in accordance with RFC 3280
Signature	Generated and encoded in accordance with RFC 3280

Table 9 – Certificate Profile Basic Fields

7.1.1 Version Number(s)

VeriSign Certificates are X.509 Version 3 Certificates although certain Root Certificates are permitted to be X.509 Version 1 Certificates to support legacy systems. CA certificates shall be X.509 Version 1 or Version 3 CA Certificates. End-user Subscriber Certificates shall be X.509 Version 3.

7.1.2 Certificate Extensions

VeriSign populates X.509 Version 3 VTN Certificates with the extensions required by Section 7.1.2.1-7.1.2.8. Private extensions are permissible, but the use of private extensions is not warranted under this CP and the applicable CPS unless specifically included by reference.

7.1.2.1 Key Usage

X.509 Version 3 Certificates are generally populated in accordance with RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002. The KeyUsage extension in X.509 Version 3 Certificates are generally configured so as to set and clear bits and the criticality field in accordance with Table 10 below. The criticality field of the KeyUsage extension is generally set to FALSE.

		CAs	***Class 1 and Class 2 End-User Subscribers***	***Automated Administration tokens and Class 2-3 End-User Subscribers***	***Dual Key Pair Signature (Managed PKI Key Manager)***	***Dual Key Pair Encipherment (Managed PKI Key Manager)***
Criticality		FALSE	FALSE	FALSE	FALSE	FALSE
0	digitalSignature	Clear	Set	Set	Set	Clear
1	nonRepudiation	Clear	Clear	Clear	Clear	Clear
2	keyEncipherment	Clear	Set	Set	Clear	Set
3	dataEncipherment	Clear	Clear	Clear	Clear	Clear
4	keyAgreement	Clear	Clear	Clear	Clear	Clear
5	keyCertSign	Set	Clear	Clear	Clear	Clear
6	CRLSign	Set	Clear	Clear	Clear	Clear
7	encipherOnly	Clear	Clear	Clear	Clear	Clear
8	decipherOnly	Clear	Clear	Clear	Clear	Clear

Table 10 – Settings for KeyUsage Extension

Note: Although the nonRepudiation bit is not set in the KeyUsage extension, VeriSign nonetheless supports nonrepudiation services for these Certificates. The nonRepudiation bit is not required to be set in these Certificates because the PKI industry has not reached a consensus as to what the nonRepudiation bit means. Until such a consensus emerges, the nonRepudiation bit will not be meaningful for potential Relying Parties. Moreover, the most commonly used applications do not recognize the nonRepudiation bit. Therefore, setting the bit will not help Relying Parties make a trust decision. Consequently, this CPS requires that the nonRepudiation bit be cleared, although it may be set in the case of dual key pair signature Certificates issued through Managed PKI Key Manager

7.1.2.2 Certificate Policies Extension

CertificatePolicies extension of X.509 Version 3 Certificates are populated with the object identifier for the VTN CP in accordance with CP Section 7.1.6 and with policy qualifiers set forth in CP Section 7.1.8. The criticality field of this extension shall be set to FALSE.

7.1.2.3 Subject Alternative Names

The subjectAltName extension of X.509 Version 3 Certificates are populated in accordance with RFC 3280. The criticality field of this extension shall be set to FALSE.

7.1.2.4 Basic Constraints

VeriSign X.509 Version 3 CA Certificates BasicConstraints extension shall have the CA field set to TRUE. End-user Subscriber Certificates BasicConstraints extension, shall be populated with a value of an empty sequence. The criticality field of this extension shall be set to TRUE for CA Certificates, but otherwise set to FALSE.

VeriSign X.509 Version 3 CA Certificates shall have a "pathLenConstraint" field of the BasicConstraints extension set to the maximum number of CA certificates that may follow this Certificate in a certification path. CA Certificates issued to an online Enterprise Customer issuing end-user Subscriber Certificates shall have a "pathLenConstraint" field set to a value of "0" indicating that only an end-user Subscriber Certificate may follow in the certification path.

7.1.2.5 Extended Key Usage

VeriSign makes use of the ExtendedKeyUsage extension for the specific types of VeriSign X.509 Version 3 Certificates listed in Table 11 below. For other types of Certificates, VeriSign does not usually use the Extended Key Usage extension.

Certificate Type	Certificate Type
Certification Authority (CA)	Class 3 International Server CA
OCSP Responder	Class 1-3 Public Primary OCSP Responders Secure Server OCSP Responder
Class 3 Web Server Certificates	Secure Server IDs Global Server IDs
Authenticated Content Signing Certificates (ACS)	Authenticated Content Signing Certificates
Individual Certificates	Class 1 Individual Certificates Class 2 Individual Certificates

Table 11 – Certificates Using the Extended Key Usage Extension

For these Certificates, VeriSign populates the ExtendedKeyUsage extension in accordance with Table 12 below.

	Class 3 International Server CA	OCSP Responders	Secure Server IDs	Global Server IDs	Authenticated Content Signing Certificates	Class 1 and 2 Individual Certificates
Criticality	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
ServerAuth	Set	Clear	Set	Set	Clear	Clear
ClientAuth	Set	Clear	Set	Set	Clear	Set
CodeSigning	Clear	Clear	Clear	Clear	Set	Clear
EmailProtection	Clear	Clear	Clear	Clear	Clear	Set
ipsecEndSystem	Clear	Clear	Clear	Clear	Clear	Clear
ipsecTunnel	Clear	Clear	Clear	Clear	Clear	Clear
ipsecUser	Clear	Clear	Clear	Clear	Clear	Clear
TimeStamping	Clear	Clear	Clear	Clear	Clear	Clear
OCSP Signing	Clear	Set	Clear	Clear	Clear	Clear
Microsoft Server Gated Crypto (SGC) OID: 1.3.6.1.4.1.311.10.3.3	Clear	Clear	Clear	Set	Clear	Clear
Netscape SGC - OID:	Set	Clear	Clear	Set	Clear	Clear

	Class 3 International Server CA	OCSP Responders	Secure Server IDs	Global Server IDs	Authenticated Content Signing Certificates	Class 1 and 2 Individual Certificates
2.16.840.1.113730.4.1						
VeriSign SGC Identifier for CA Certificates – OID: 2.16.840.1.113733.1.8.1	Set	Clear	Clear	Clear	Clear	Clear

Table 12 – Settings for ExtendedKeyUsage Extension

7.1.2.6 CRL Distribution Points

Most VeriSign X.509 Version 3 end user Subscriber Certificates and Intermediate CA Certificates include the cRLDistributionPoints extension containing the URL of the location where a Relying Party can obtain a CRL to check the CA Certificate's status. The criticality field of this extension is set to FALSE.

7.1.2.7 Authority Key Identifier

VeriSign generally populates the Authority Key Identifier extension of X.509 Version 3 end user Subscriber Certificates and Intermediate CA Certificates . When the certificate issuer contains the Subject Key Identifier extension, the Authority Key Identifier is composed of the 160-bit SHA-1 hash of the public key of the CA issuing the Certificate. Otherwise, the Authority Key Identifier extension includes the issuing CA's subject distinguished name and serial number. The criticality field of this extension is set to FALSE.

7.1.2.8 Subject Key Identifier

Where VeriSign populates X.509 Version 3 VTN Certificates with a subjectKeyIdentifier extension, the keyIdentifier based on the public key of the Subject of the Certificate is generated in accordance with one of the methods described in RFC 3280. Where this extension is used, the criticality field of this extension is set to FALSE.

7.1.3 Algorithm Object Identifiers

VeriSign Certificates are signed using one of following algorithms.

- sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
- md5WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 4}
- md2WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 2}

Certificate signatures produced using these algorithms shall comply with RFC 3279. Use of sha-1WithRSAEncryption shall be given strong preference over md5WithRSAEncryption. md2WithRSAEncryption is no longer used to sign end entity certificates, but is used to sign CRLs for certain legacy CA and End-User Subscriber Certificates.

7.1.4 Name Forms

VeriSign populates VTN Certificates with an Issuer and Subject Distinguished Name in accordance with Section 3.1.1.

In addition, VeriSign includes within end-user Subscriber Certificates an additional Organizational Unit field that contains a notice stating that the terms of use of the Certificate are set forth in a URL which is a pointer to the applicable Relying Party Agreement. Exceptions to the foregoing requirement are permitted only when space, formatting, or interoperability limitations within Certificates make such an Organizational Unit impossible to use in conjunction with the application for which the Certificates are intended.

7.1.5 Name Constraints

No stipulation

7.1.6 Certificate Policy Object Identifier

Where the Certificate Policies extension is used, Certificates contain the object identifier for the Certificate Policy corresponding to the appropriate Class of Certificate as set forth in the VTN CP Section1.2. For legacy Certificates issued prior to the publication of the VTN CP which include the Certificate Policies extension, Certificates refer to the VeriSign CPS.

7.1.7 Usage of Policy Constraints Extension

No stipulation

7.1.8 Policy Qualifiers Syntax and Semantics

Where the Certificate Policies extension is used, Certificates contain the object identifier for the Certificate Policy corresponding to the appropriate Class of Certificate as set forth in Section 1.2 of the VTN CP. For legacy Certificates issued prior to the publication of the VTN CP which include the Certificate Policies extension Certificates refer to the VeriSign CPS.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.2 CRL Profile

CRLs contain the basic fields and contents specified in Table 13 below:

Field	Value or Value constraint
Version	See Section 7.2.1.
Signature Algorithm	Algorithm used to sign the CRL. VeriSign CRLs are signed using sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) or md5WithRSAEncryption (OID: 1.2.840.113549.1.1.4) in accordance with RFC 3279.
Issuer	Entity who has signed and issued the CRL.
Effective Date	Issue date of the CRL. CRLs are effective upon issuance.
Next Update	Date by which the next CRL will be issued. CRL issuance frequency is in accordance with the requirements of Section 4.4.7.
Revoked	Listing of revoked certificates, including the Serial Number of the revoked

Field	Value or Value constraint
Certificates	Certificate and the Revocation Date.

Table 13 – CRL Profile Basic Fields

7.2.1 Version Number(s)

VeriSign supports both X.509 Version1 and Version 2 CRLs. Version 2 CRLs comply with the requirements of RFC 3280.

7.2.2 CRL and CRL Entry Extensions

No stipulation

7.3 OCSP Profile

OCSP (Online Certificate Status Protocol) is a way to obtain timely information about the revocation status of a particular certificate. VeriSign uses OCSP to validate:

- Class 2 Enterprise certificates, and
- Class 3 organization certificates where it has been incorporated into VeriSign's Trusted Global Validation protocol (TGV).

OCSP responders conform to RFC 2560.

7.3.1 Version Number(s)

Version 1 of the OCSP specification as defined by RFC2560 is supported.

7.3.2 OCSP Extensions

VeriSign's TGV Service used to validate Class 3 Organizational certificates uses secure timestamp and validity period to establish the current freshness of each OCSP response. VeriSign does not use a nonce to establish the current freshness of each OCSP response and clients should not expect a nonce in the response to a request that contains a nonce. Instead, clients should use the local clock to check for response freshness.

8. Compliance Audit and Other Assessments

An annual WebTrust for Certification Authorities examination is performed for VeriSign's data center operations and key management operations supporting VeriSign's public and Managed PKI CA services including the VTN Root CAs, Class 3 Organizational CAs, Class 2 Organizational and Individual CAs, and Class 1 Individual CAs specified in Section 1.3.1. Customer-specific CAs are not specifically audited as part of the audit of VeriSign's operations unless required by the Customer. VeriSign shall be entitled to require that Enterprise Customers undergo a compliance audit under this CPS and audit programs for these types of Customers.

In addition to compliance audits, VeriSign shall be entitled to perform other reviews and investigations to ensure the trustworthiness of VeriSign's Subdomain of the VTN, which include, but are not limited to:

- VeriSign shall be entitled, within its sole and exclusive discretion, to perform at any time an "Exigent Audit/Investigation" on a Customer in the event VeriSign has reason to believe that the audited entity has failed to meet VTN Standards, has experienced an incident or compromise, or has acted or failed to act, such that the audited entity's

failure, the incident or compromise, or the act or failure to act poses an actual or potential threat to the security or integrity of the VTN.

- VeriSign shall be entitled to perform “Supplemental Risk Management Reviews” on a Customer following incomplete or exceptional findings in a Compliance Audit or as part of the overall risk management process in the ordinary course of business.

VeriSign shall be entitled to delegate the performance of these audits, reviews, and investigations to a third party audit firm. Entities that are subject to an audit, review, or investigation shall provide reasonable cooperation with VeriSign and the personnel performing the audit, review, or investigation.

8.1 Frequency and Circumstances of Assessment

Compliance Audits are conducted at least annually at the sole expense of the audited entity.

8.2 Identity/Qualifications of Assessor

VeriSign’s CA compliance audits are performed by a public accounting firm that:

- Demonstrates proficiency in public key infrastructure technology, information security tools and techniques, security auditing, and the third-party attestation function, and
- Is accredited by the American Institute of Certified Public Accountants (AICPA), which requires the possession of certain skill sets, quality assurance measures such as peer review, competency testing, standards with respect to proper assignment of staff to engagements, and requirements for continuing professional education.

8.3 Assessor's Relationship to Assessed Entity

Compliance audits of VeriSign’s operations are performed by a public accounting firm that is independent of VeriSign.

8.4 Topics Covered by Assessment

The scope of VeriSign’s annual WebTrust for Certification Authorities (or equivalent) audit includes CA environmental controls, key management operations and Infrastructure/Administrative CA controls, certificate life cycle management and CA business practices disclosure.

8.5 Actions Taken as a Result of Deficiency

With respect to compliance audits of VeriSign’s operations, significant exceptions or deficiencies identified during the Compliance Audit will result in a determination of actions to be taken. This determination is made by VeriSign management with input from the auditor. VeriSign management is responsible for developing and implementing a corrective action plan. If VeriSign determines that such exceptions or deficiencies pose an immediate threat to the security or integrity of the VTN, a corrective action plan will be developed within 30 days and implemented within a commercially reasonable period of time. For less serious exceptions or deficiencies, VeriSign Management will evaluate the significance of such issues and determine the appropriate course of action.

8.6 Communications of Results

A copy of VeriSign’s WebTrust for CA audit report can be found at http://www.verisign.com/repository .

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

VeriSign, is entitled to charge end-user Subscribers for the issuance, management, and renewal of Certificates.

9.1.2 Certificate Access Fees

VeriSign does not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties.

9.1.3 Revocation or Status Information Access Fees

VeriSign does not charge a fee as a condition of making the CRLs required by this CP available in a repository or otherwise available to Relying Parties. VeriSign is, however, entitled to charge a fee for providing customized CRLs, OCSP services, or other value-added revocation and status information services. VeriSign does not permit access to revocation information, Certificate status information, or time stamping in their repositories by third parties that provide products or services that utilize such Certificate status information without VeriSign's prior express written consent.

9.1.4 Fees for Other Services

VeriSign does not charge a fee for access to this CPS. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works, shall be subject to a license agreement with the entity holding the copyright to the document.

9.1.5 Refund Policy

Within VeriSign's Subdomain, the following refund policy (reproduced at http://www.verisign.com/repository/refund/) is in effect:

VeriSign 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 that 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 or the NetSure(sm) Protection Plan relating to the subscriber or the subscriber's certificate. After VeriSign revokes the subscriber's certificate, VeriSign will promptly credit the subscriber's credit card account (if the certificate was paid for via credit card) or otherwise reimburse the subscriber via check, for the full amount of the applicable fees paid for the certificate. To request a refund, please call customer service at +1 650 426-3400. This refund policy is not an exclusive remedy and does not limit other remedies that may be available to subscribers.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Enterprise Customers are encouraged to maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention. VeriSign maintains such errors and omissions insurance coverage.

9.2.2 Other Assets

Enterprise Customers shall have sufficient financial resources to maintain their operations and perform their duties, and they must be reasonably able to bear the risk of liability to Subscribers and Relying Parties. VeriSign's financial resources are set forth in disclosures appearing at: http://www.verisign.com/verisign-inc/vrsn-investors/sec-filings/index.html

9.2.3 Extended Warranty Coverage

The NetSure Protection Plan is an extended warranty program that provides VeriSign SSL and code signing certificate subscribers with protection against loss or damage that is due to a defect in VeriSign's issuance of the certificate or other malfeasance caused by VeriSign's negligence or breach of its contractual obligations, provided that the subscriber of the certificate has fulfilled its obligations under the applicable service agreement. For general information concerning the NetSure Protection Plan, and a discussion of which Certificates are covered by it, see http://www.verisign.com/netsure.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

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

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

9.3.2 Information Not Within the Scope of Confidential Information

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

9.3.3 Responsibility to Protect Confidential Information

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

VeriSign has implemented a privacy policy, which is located at: http://www.verisign.com/truste/index.html, in compliance with CP § 2.8.

9.4.2 Information Treated as Private

Any information about Subscribers that is not publicly available through the content of the issued certificate, certificate directory and online CRLs is treated as private

9.4.3 Information Not Deemed Private

Subject to local laws, all information made public in a certificate is deemed not private.

9.4.4 Responsibility to Protect Private Information

VTN participants receiving private information shall secure it from compromise and disclosure to third parties and shall comply with all local privacy laws in their jurisdiction.

9.4.5 Notice and Consent to Use Private Information

Unless where otherwise stated in this CPS, the applicable Privacy Policy or by agreement, private information will not be used without the consent of the party to whom that information applies. This section is subject to applicable privacy laws

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

VeriSign shall be entitled to disclose Confidential/Private Information if, in good faith, VeriSign believes that:

- disclosure is necessary in response to subpoenas and search warrants.
- disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents.

This section is subject to applicable privacy laws.

9.4.7 Other Information Disclosure Circumstances

No Stipulation

9.5 Intellectual Property rights

The allocation of Intellectual Property Rights among VeriSign Subdomain Participants other than Subscribers and Relying Parties is governed by the applicable agreements among such VeriSign Subdomain Participants. The following subsections of Section 9.5 apply to the Intellectual Property Rights in relation to Subscribers and Relying Parties.

9.5.1 Property Rights in Certificates and Revocation Information

CAs retain all Intellectual Property Rights in and to the Certificates and revocation information that they issue. VeriSign and Customers grant permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to the Relying Party Agreement referenced in the Certificate. VeriSign and Customers shall grant permission to use revocation information to perform Relying Party functions subject to the applicable CRL Usage Agreement, Relying Party Agreement, or any other applicable agreements.

9.5.2 Property Rights in the CPS

VTN Participants acknowledge that VeriSign retains all Intellectual Property Rights in and to this CPS.

9.5.3 Property Rights in Names

A Certificate Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to such Certificate Applicant.

9.5.4 Property Rights in Keys and Key Material

Key pairs corresponding to Certificates of CAs and end-user Subscribers are the property of the CAs and end-user Subscribers that are the respective Subjects of these Certificates, subject to the rights of enterprise Customers using Managed PKI Key Manager, regardless of the physical medium within which they are stored and protected, and such persons retain all Intellectual Property Rights in and to these key pairs. Without limiting the generality of the foregoing, VeriSign's root public keys and the root Certificates containing them, including all PCA public keys and self-signed Certificates, are the property of VeriSign. VeriSign licenses software and hardware manufacturers to reproduce such root Certificates to place copies in trustworthy hardware devices or software. Finally, Secret Shares of a CA's private key are the property of the CA, and the CA retains all Intellectual Property Right in and to such Secret Shares even though they cannot obtain physical possession of the those shares or the CA from VeriSign.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

VeriSign warrants that:

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application or issuing the Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate,
- Their Certificates meet all material requirements of this CPS, and
- Revocation services and use of a repository conform to the applicable CPS in all material aspects.

Subscriber Agreements may include additional representations and warranties.

9.6.2 RA Representations and Warranties

RAs warrant that:

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application as a result of a failure to exercise reasonable care in managing the Certificate Application,
- Their Certificates meet all material requirements of this CPS, and
- Revocation services (when applicable) and use of a repository conform to the applicable CPS in all material aspects.

Subscriber Agreements may include additional representations and warranties.

9.6.3 Subscriber Representations and Warranties

Subscribers warrant that:

- 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 or revoked) at the time the digital signature is created,
- Their private key is protected and that no unauthorized person has ever had access to the Subscriber's private key,
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true,
- All information supplied by the Subscriber and contained in the Certificate is true,
- The Certificate is being used exclusively for authorized and legal purposes, consistent with this CPS, and
- The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

Subscriber Agreements may include additional representations and warranties.

9.6.4 Relying Party Representations and Warranties

Relying Party Agreements require Relying Parties to acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in terms of this CPS.

Relying Party Agreements may include additional representations and warranties.

9.6.5 Representations and Warranties of Other Participants

No stipulation

9.7 Disclaimers of Warranties

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall disclaim VeriSign's possible warranties, including any warranty of merchantability or fitness for a particular purpose, outside the context of the NetSure Protection Plan.

9.8 Limitations of Liability

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall limit VeriSign's liability outside the context of the NetSure Protection Plan. Limitations of liability shall include an exclusion of indirect, special, incidental, and consequential damages. They shall also include the following liability caps limiting VeriSign's and the Affiliate's damages concerning a specific Certificate:

Class	Liability Caps
Class 1	One Hundred U.S. Dollars ($ 100.00 US)
Class 2	Five Thousand U.S. Dollars ($ 5,000.00 US)
Class 3	One Hundred Thousand U.S. Dollars ($ 100,000.00 US)

Table 14 – Liability Caps

The liability caps in Table 14 limit damages recoverable outside the context of the NetSure Protection Plan. Amounts paid under the NetSure Protection Plan are subject to their own liability caps. The liability caps under the NetSure Protection Plan for different kinds of Certificates range from $1,000 US to $1,000,000 US. *See* the NetSure Protection Plan for more detail at **http://www.verisign.com/repository/netsure/**.

The liability (and/or limitation thereof) of Subscribers shall be as set forth in the applicable Subscriber agreements.

The liability (and/or limitation thereof) of enterprise RAs and the applicable CA shall be set out in the agreement(s) between them.

The liability (and/or limitation thereof) of Relying Parties shall be as set forth in the applicable Relying Party Agreements.

9.9 Indemnities

9.9.1 Indemnification by Subscribers

To the extent permitted by applicable law, Subscriber are required to indemnify VeriSign for:

- Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application,
- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party,
- The Subscriber's 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, or
- The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

The applicable Subscriber Agreement may include additional indemnity obligations.

9.9.2 Indemnification by Relying Parties

To the extent permitted by applicable law, Relying Party Agreements shall require Relying Parties to indemnify VeriSign for:

- The Relying Party's failure to perform the obligations of a Relying Party,
- The Relying Party's reliance on a Certificate that is not reasonable under the circumstances, or
- The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

The applicable Relying Party Agreement may include additional indemnity obligations.

9.10 Term and Termination

9.10.1 Term

The CPS becomes effective upon publication in the VeriSign repository. Amendments to this CPS become effective upon publication in the VeriSign repository.

9.10.2 Termination

This CPS as amended from time to time shall remain in force until it is replaced by a new version.

9.10.3 Effect of Termination and Survival

Upon termination of this CPS, VeriSign subdomain participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, VeriSign subdomain participants shall use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

9.12 Amendments

9.12.1 Procedure for Amendment

Amendments to this CPS may be made by the VeriSign Policy Management Authority (PMA). Amendments shall either be in the form of a document containing an amended form of the CPS or an update. Amended versions or updates shall be linked to the Practices Updates and Notices section of the VeriSign Repository located at: **https://www.verisign.com/repository/updates**. Updates supersede any designated or conflicting provisions of the referenced version of the CPS. The PMA shall determine whether changes to the CPS require a change in the Certificate policy object identifiers of the Certificate policies corresponding to each Class of Certificate.

9.12.2 Notification Mechanism and Period

VeriSign and the PMA reserve the right to amend the CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. The PMA's decision to designate amendments as material or non-material shall be within the PMA's sole discretion

Proposed amendments to the CPS shall appear in the Practices Updates and Notices section of the VeriSign Repository, which is located at: **https://www.verisign.com/repository/updates**.

The PMA solicits proposed amendments to the CPS from other VeriSign subdomain participants. If the PMA considers such an amendment desirable and proposes to implement the amendment, the PMA shall provide notice of such amendment in accordance with this section.

Notwithstanding anything in the CPS to the contrary, if the PMA believes that material amendments to the CPS are necessary immediately to stop or prevent a breach of the security of the VTN or any portion of it, VeriSign and the PMA shall be entitled to make such amendments by publication in the VeriSign Repository. Such amendments will be effective immediately upon publication. Within a reasonable time after publication, VeriSign shall provide notice to Affiliates of such amendments.

9.12.2.1 Comment Period

Except as otherwise stated, the comment period for any material amendments to the CPS shall be fifteen (15) days, starting on the date on which the amendments are posted on the VeriSign Repository. Any VeriSign subdomain participant shall be entitled to file comments with the PMA up until the end of the comment period.

9.12.2.2 Mechanism to Handle Comments

The PMA shall consider any comments on the proposed amendments. The PMA shall either (a) allow the proposed amendments to become effective without amendment, (b) amend the proposed amendments and republish them as a new amendment when required, or (c) withdraw the proposed amendments. The PMA is entitled to withdraw proposed amendments by notifying Affiliates and providing notice in the Practices Updates and Notices section of the VeriSign Repository. Unless proposed amendments are amended or withdrawn, they shall become effective upon the expiration of the comment period.

9.12.3 Circumstances under Which OID Must be Changed

If the PMA determines that a change is necessary in the object identifier corresponding to a Certificate policy, the amendment shall contain new object identifiers for the Certificate policies corresponding to each Class of Certificate. Otherwise, amendments shall not require a change in Certificate policy object identifier.

9.13 Dispute Resolution Provisions

9.13.1 Disputes among VeriSign, Affiliates, and Customers

Disputes among VeriSign subdomain participants shall be resolved pursuant to provisions in the applicable agreements among the parties.

9.13.2 Disputes with End-User Subscribers or Relying Parties

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall contain a dispute resolution clause. Disputes involving VeriSign require an initial negotiation period of sixty (60) days followed by litigation in the federal or state court encompassing Santa Clara County, California, in the case of claimants who are U.S. residents, or, in the case of all other claimants, arbitration administered by the International Chamber of Commerce (“ICC”) in accordance with the ICC Rules of Conciliation and Arbitration, unless otherwise approved by VeriSign.

9.14 Governing Law

Subject to any limits appearing in applicable law, 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, USA. This choice of law is made to ensure uniform procedures and interpretation for all VTN Participants, no matter where they are located.

This governing law provision applies only to this CPS. Agreements incorporating the CPS by reference may have their own governing law provisions, provided that this Section 9.14 governs the enforceability, construction, interpretation, and validity of the terms of the CPS separate and apart from the remaining provisions of any such agreements, subject to any limitations appearing in applicable law.

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

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Not applicable

9.16.2 Assignment

Not applicable

9.16.3 Severability

In the event that a clause or provision of this CPS is held to be unenforceable by a court of law or other tribunal having authority, the remainder of the CPS shall remain valid.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

Not applicable

9.16.5 Force Majeure

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall include a force majeure clause protecting VeriSign.

9.17 Other Provisions

Not applicable

Appendix A. Table of Acronyms and definitions

Table of Acronyms

Term	Definition
ANSI	The American National Standards Institute.
ACS	Authenticated Content Signing.
BIS	The United States Bureau of Industry and Science of the United States Department of Commerce.
CA	Certification Authority.
CP	Certificate Policy.
CPS	Certification Practice Statement.
CRL	Certificate Revocation List.
EAL	Evaluation assurance level (pursuant to the Common Criteria).
FIPS	United State Federal Information Processing Standards.
ICC	International Chamber of Commerce.
KRB	Key Recovery Block.
LSVA	Logical security vulnerability assessment.
OCSP	Online Certificate Status Protocol.
PCA	Primary Certification Authority.
PIN	Personal identification number.
PKCS	Public-Key Cryptography Standard.
PKI	Public Key Infrastructure.
PMA	Policy Management Authority.
RA	Registration Authority.
RFC	Request for comment.
SAS	Statement on Auditing Standards (promulgated by the American Institute of Certified Public Accountants).
S/MIME	Secure multipurpose Internet mail extensions.
SSL	Secure Sockets Layer.
VTN	VeriSign Trust Network.

Definitions

Term	Definition
Administrator	A Trusted Person within the organization of a Processing Center, Service Center, Managed PKI Customer, or Gateway Customer that performs validation and other CA or RA functions.
Administrator Certificate	A Certificate issued to an Administrator that may only be used to perform CA or RA functions.
Affiliate	A leading trusted third party, for example in the technology, telecommunications, or financial services industry, that has entered into an agreement with VeriSign to be a VTN distribution and services channel within a specific territory.
Affiliate Audit Program Guide	A VeriSign document containing requirements for the Compliance Audits of Affiliates, including Certificate Management Control Objectives against which Affiliates will be audited.
Affiliate Practices Legal Requirements Guidebook	A VeriSign document setting forth requirements for Affiliate CPSs, agreements, validation procedures, and privacy policies, as well as other requirements that Affiliates must meet.
Affiliated Individual	A natural person that is related to a Managed PKI Customer, Managed PKI Lite Customer, or Gateway Customer entity (i) as an officer, director, employee, partner, contractor, intern, or other person within the entity, (ii) as a member of a VeriSign registered community of interest, or (iii) as a person maintaining a relationship with the entity where the entity has business or other records providing appropriate assurances of the identity of such person.

Term	Definition
Automated Administration	A procedure whereby Certificate Applications are approved automatically if enrollment information matches information contained in a database.
Automated Administration Software Module	Software provided by VeriSign that performs Automated Administration.
Certificate	A message that, at least, states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key, identifies the Certificate's Operational Period, contains a Certificate serial number, and is digitally signed by the CA.
Certificate Applicant	An individual or organization that requests the issuance of a Certificate by a CA.
Certificate Application	A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.
Certificate Chain	An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.
Certificate Management Control Objectives	Criteria that an entity must meet in order to satisfy a Compliance Audit.
Certificate Policies (CP)	This document, which is entitled "VeriSign Trust Network Certificate Policies" and is the principal statement of policy governing the VTN.
Certificate Revocation List (CRL)	A periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates in accordance with CP § 3.4. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation.
Certificate Signing Request	A message conveying a request to have a Certificate issued.
Certification Authority (CA)	An entity authorized to issue, manage, revoke, and renew Certificates in the VTN.
Certification Practice Statement (CPS)	A statement of the practices that VeriSign or an Affiliate employs in approving or rejecting Certificate Applications and issuing, managing, and revoking Certificates, and requires its Managed PKI Customers and Gateway Customers to employ.
Challenge Phrase	A secret phrase chosen by a Certificate Applicant during enrollment for a Certificate. When issued a Certificate, the Certificate Applicant becomes a Subscriber and a CA or RA can use the Challenge Phrase to authenticate the Subscriber when the Subscriber seeks to revoke or renew the Subscriber's Certificate.
Class	A specified level of assurances as defined within the CP. See CP § 1.1.1.
Client Service Center	A Service Center that is an Affiliate providing client Certificates either in the Consumer or Enterprise line of business.
Compliance Audit	A periodic audit that a Processing Center, Service Center, Managed PKI Customer, or Gateway Customer undergoes to determine its conformance with VTN Standards that apply to it.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
Confidential/Private Information	Information required to be kept confidential and private pursuant to CP § 2.8.1.
CRL Usage Agreement	An agreement setting forth the terms and conditions under which a CRL or the information in it can be used.
Customer	An organization that is either a Managed PKI Customer, Gateway Customer, or ASB Customer.
Enterprise, as in Enterprise Service Center	A line of business that an Affiliate enters to provide Managed PKI services to Managed PKI Customers.
Enterprise Roaming Server	A server residing at the site of a Managed PKI Customer used in conjunction with the VeriSign Roaming Service to hold Roaming Subscribers' encrypted private keys and portions of symmetric keys used to encrypt and decrypt Roaming Subscribers' private keys.
Exigent Audit/Investigation	An audit or investigation by VeriSign where VeriSign has reason to believe that an entity's failure to meet VTN Standards, an incident or Compromise relating to the entity, or an actual or potential threat to the security of the VTN posed by the entity has occurred.
Intellectual Property Rights	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.
Intermediate Certification Authority (Intermediate CA)	A Certification Authority whose Certificate is located within a Certificate Chain between the Certificate of the root CA and the Certificate of the Certification Authority that issued the end-user Subscriber's Certificate.
Key Generation Ceremony	A procedure whereby a CA's or RA's key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.
Key Manager Administrator	An Administrator that performs key generation and recovery functions for a Managed PKI

Term	Definition
	Customer using Managed PKI Key Manager.
Key Recovery Block (KRB)	A data structure containing a Subscriber's private key that is encrypted using an encryption key. KRBs are generated using Managed PKI Key Manager software.
Key Recovery Service	A VeriSign service that provides encryption keys needed to recover a Key Recovery Block as part of a Managed PKI Customer's use of Managed PKI Key Manager to recover a Subscriber's private key.
Managed PKI	VeriSign's fully integrated managed PKI service that allows enterprise Customers of VeriSign and its Affiliates to distribute Certificates to individuals, such as employees, partners, suppliers, and customers, as well as devices, such as servers, routers, and firewalls. Managed PKI permits enterprises to secure messaging, intranet, extranet, virtual private network, and e-commerce applications.
Managed PKI Administrator	An Administrator that performs validation or other RA functions for an Managed PKI Customer.
Managed PKI Control Center	A web-based interface that permits Managed PKI Administrators to perform Manual Authentication of Certificate Applications
Managed PKI Key Manager	A key recovery solution for those Managed PKI Customers choosing to implement key recovery under a special Managed PKI Agreement.
Managed PKI Key Management Service Administrator's Guide	A document setting forth the operational requirements and practices for Managed PKI Customers using Managed PKI Key Manager.
Manual Authentication	A procedure whereby Certificate Applications are reviewed and approved manually one-by-one by an Administrator using a web-based interface.
NetSure Protection Plan	An extended warranty program, which is described in CP § 1.1.2.2.3.
Nonverified 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.
Non-repudiation	An attribute of a communication that provides protection against a party to a communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the identity associated with the sender is unknown. Note: only an adjudication by a court, arbitration panel, or other tribunal can ultimately prevent repudiation. For example, a digital signature verified with reference to a VTN Certificate may provide proof in support of a determination of Non-repudiation by a tribunal, but does not by itself constitute Non-repudiation.
Offline CA	VeriSign PCAs, Issuing Root CAs and other designated intermediate CAs that are maintained offline for security reasons in order to protect them from possible attacks by intruders by way of the network. These CAs do not directly sign end user Subscriber Certificates.
Online CA	CAs that sign end user Subscriber Certificates are maintained online so as to provide continuous signing services.
Online Certificate Status Protocol (OCSP)	A protocol for providing Relying Parties with real-time Certificate status information.
Operational Period	The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKCS #12	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
Policy Management Authority (PMA)	The organization within VeriSign responsible for promulgating this policy throughout the VTN.
Primary Certification Authority (PCA)	A CA that acts as a root CA for a specific Class of Certificates, and issues Certificates to CAs subordinate to it.
Processing Center	An organization (VeriSign or certain Affiliates) that creates a secure facility housing, among other things, the cryptographic modules used for the issuance of Certificates. In the Consumer and Web Site lines of business, Processing Centers act as CAs within the VTN and perform all Certificate lifecycle services of issuing, managing, revoking, and renewing Certificates. In the Enterprise line of business, Processing Centers provide lifecycle services on behalf of their Managed PKI Customers or the Managed PKI Customers of the Service Centers subordinate to them.
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic

Term	Definition
	system. The VTN PKI consists of systems that collaborate to provide and implement the VTN.
Registration Authority (RA)	An entity approved by a CA to assist Certificate Applicants in applying for Certificates, and to approve or reject Certificate Applications, revoke Certificates, or renew Certificates.
Relying Party	An individual or organization that acts in reliance on a certificate and/or a digital signature.
Relying Party Agreement	An agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a Relying Party.
Retail Certificate	A Certificate issued by VeriSign or an Affiliate, acting as CA, to individuals or organizations applying one by one to VeriSign or an Affiliate on its web site.
Roaming Subscriber	A Subscriber using the VeriSign Roaming Service whose private key is encrypted and decrypted with a symmetric key that is split between the VeriSign Roaming Server and an Enterprise Roaming Server.
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
RSA Secure Server Certification Authority (RSA Secure Server CA)	The Certification Authority that issues Secure Server IDs.
RSA Secure Server Hierarchy	The PKI hierarchy comprised of the RSA Secure Server Certification Authority.
Secret Share	A portion of a CA private key or a portion of the activation data needed to operate a CA private key under a Secret Sharing arrangement.
Secret Sharing	The practice of splitting a CA private key or the activation data to operate a CA private key in order to enforce multi-person control over CA private key operations under CP § 6.2.2.
Secure Server ID	A Class 3 organizational Certificate used to support SSL sessions between web browsers and web servers.
Secure Sockets Layer (SSL)	The industry-standard method for protecting Web communications developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a Transmission Control Protocol/Internet Protocol connection.
Security and Audit Requirements Guide	A VeriSign document that sets forth the security and audit requirements and practices for Processing Centers and Service Centers.
Security and Practices Review	A review of an Affiliate performed by VeriSign before an Affiliate is permitted to become operational.
Service Center	An Affiliate that does not house Certificate signing units for the issuance of Certificates for the purpose of issuing Certificates of a specific Class or type, but rather relies on a Processing Center to perform issuance, management, revocation, and renewal of such Certificates.
Subdomain	The portion of the VTN under control of an entity and all entities subordinate to it within the VTN hierarchy.
Subject	The holder of a private key corresponding to a public key. The term “Subject” can, in the case of an organizational Certificate, refer to the equipment or device that holds a private key. A Subject is assigned an unambiguous name, which is bound to the public key contained in the Subject’s Certificate.
Subscriber	In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organizational Certificate, an organization that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. A Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate.
Subscriber Agreement	An agreement used by a CA or RA setting forth the terms and conditions under which an individual or organization acts as a Subscriber.
Superior Entity	An entity above a certain entity within a VTN hierarchy (the Class 1, 2, or 3 hierarchy).
Supplemental Risk Management Review	A review of an entity by VeriSign following incomplete or exceptional findings in a Compliance Audit of the entity or as part of the overall risk management process in the ordinary course of business.
Reseller	An entity marketing services on behalf of VeriSign or an Affiliate to specific markets.
Trusted Person	An employee, contractor, or consultant of an entity within the VTN responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices as further defined in CP § 5.2.1.
Trusted Position	The positions within a VTN entity that must be held by a Trusted Person.
Trustworthy System	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a “trusted system” as recognized in classified

Term	Definition
	government nomenclature.
VeriSign	Means, with respect to each pertinent portion of this CPS, VeriSign, Inc. and/or any wholly owned VeriSign subsidiary responsible for the specific operations at issue.
VeriSign Digital Notarization Service	A service offered to Managed PKI Customers that provides a digitally signed assertion (a Digital Receipt) that a particular document or set of data existed at a particular point in time.
VeriSign Repository	VeriSign's database of Certificates and other relevant VeriSign Trust Network information accessible on-line.
VeriSign Roaming Server	A server residing at VeriSign's Processing Center used in conjunction with the VeriSign Roaming Service to hold portions of symmetric keys used to encrypt and decrypt Roaming Subscribers' private keys.
VeriSign Roaming Service	The service offered by VeriSign that enables a Subscriber to download his or her private key and perform private key operations on different client terminals.
VeriSign Trust Network (VTN)	The Certificate-based Public Key Infrastructure governed by the VeriSign Trust Network Certificate Policies, which enables the worldwide deployment and use of Certificates by VeriSign and its Affiliates, and their respective Customers, Subscribers, and Relying Parties.
VTN Participant	An individual or organization that is one or more of the following within the VTN: VeriSign, an Affiliate, a Customer, a Universal Service Center, a Reseller, a Subscriber, or a Relying Party.
VTN Standards	The business, legal, and technical requirements for issuing, managing, revoking, renewing, and using Certificates within the VTN.