

# **VeriSign Certification Practice Statement**

**Version 3.3**

**Effective Date: November 15, 2006**



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

**History of changes: version 3.3**

Section 1	Added: "This CPS conforms to the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policy and Certification Practice Statement construction."
Section 1.4.1.2 - Table 2	Added: High Assurance with Extended Validation
Section 1.4.1.3	Added: " <b>High assurance with extended validation certificates</b> are Class 3 certificates issued by VeriSign in conformance with the Guidelines for Extended Validation Certificates."
Section 2.2 - Table 3	Added: End-User Subscriber Certificates issued by VeriSign Class 3 Organizational VIP Device CA are not available through public query.
Section 3.1.1	Added: "EV SSL certificate content and profile requirements are discussed in Section 6 of Appendix B3 to this CPS."
Section 3.2.2 – Table 6	Added: "VeriSign's procedures for issuing Extended Validation SSL Certificates are described in Appendix B1 to this CPS."
Section 3.2.6	Added footnote: "Customers of VeriSign's Certificate Interoperability Service (CIS) are encouraged, but not required, to have their own CPS under the Certificate Interoperability Service (CIS) CP Supplement, but in all cases must comply with VeriSign's Certificate Interoperability Service (CIS) CP Supplement, published in the VeriSign Repository"
Section 3.3.1	Deleted: "In particular, for subsequent renewal requests for retail Class 3 Organizational certificates, VeriSign reauthenticates the Organization name and domain name included in the certificate. In circumstances where:..."  Added: "In particular, for subsequent re-key requests for retail Class 3 Organizational certificates through www.verisign.com, VeriSign reauthenticates the Organization name and domain name included in the certificate. In circumstances where:..."
Section 4.6.3	Deleted: "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:..."  Added: "In particular, for subsequent renewal requests for retail Class 3 Organizational certificates through www.verisign.com, VeriSign reauthenticates the Organization name and domain name included in the certificate. In circumstances where:..."
Section 4.9.7	Added footnote: "CRLs for the "VeriSign Class 3 Organizational VIP Device CA" are only issued whenever a certificate issued by that CA is revoked."
Section 6.3.2	Added: "VeriSign operates the "VeriSign Class 3 Organizational VIP Device CA". Organizational end-entity certificates issued by this CA may have a validity period beyond 3 years and up to a maximum of 5 years in circumstances where: <ul style="list-style-type: none"> <li>o The certificate key pair is stored in hardware, and</li> <li>o VeriSign has authenticated the Organization in terms of this CPS and</li> <li>o When used to protect a server using SSL/TLS, the server is only accessible via a private network or intranet. "</li> </ul>
Section 6.3.2 fn - 16	Deleted: "The Distinguished name of these Certificates shall be re-authenticated by VeriSign at least every 25-months."
Section 7.1.2	Added: " EV SSL certificate extension requirements are described in Appendix B3 to this CPS."
Section 7.1.8	Deleted: "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 and/or the Relying party Agreement."  Added: "VeriSign generally populates X.509 Version 3 VTN Certificates with a policy qualifier within the Certificate Policies extension. Generally, such Certificates contain a CPS pointer qualifier that points to the applicable Relying Party Agreement or the VeriSign CPS. In addition, some Certificates contain a User Notice Qualifier which points to the applicable Relying Party Agreement."
Section 9.8	Added: "VeriSign's limitation of liability for EV certificates is further described in Section 37 of Appendix B1 to this CPS."
Section 9.8	Deleted: "They shall also include the following liability caps limiting VeriSign's and the Affiliate's damages concerning a specific Certificate..." Added: They shall also include the following liability caps limiting VeriSign's damages concerning a specific Certificate..."
Definitions	Added definition for "Extended Validation"
Appendix B	Added Appendix B: "Supplemental Validation Procedures for Extended Validation SSL Certificates"
Appendix C	Added Appendix C: Minimum Cryptographic Algorithm and Key Sizes for EV Certificates
Appendix D	Added Appendix D: EV Certificates Required Certificate Extensions

**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 <ul style="list-style-type: none"> <li>• The challenge phrase is correctly used for the subsequent renewal certificate and;</li> <li>• The certificate Distinguished Name has not been changed, and</li> <li>• The Corporate and Technical Contact information remains unchanged from that which was previously verified,</li> </ul> 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 <a href="http://www.verisign.com/netsure">http://www.verisign.com/netsure</a> .  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 <a href="http://www.verisign.com/netsure">http://www.verisign.com/netsure</a> "

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: <a href="http://www.verisign.com/verisign-inc/vrsn-investors/sec-filings/index.html">http://www.verisign.com/verisign-inc/vrsn-investors/sec-filings/index.html</a>

## VeriSign Trust Network Certificate Policies

© 2005 VeriSign, Inc. All rights reserved.  
Printed in the United States of America.

Published date: April 01, 2005

### Trademark Notices

VeriSign is the registered trademarks of VeriSign, Inc. The VeriSign logo, VeriSign Trust Network and NetSure are trademarks and service marks of VeriSign, Inc. Other trademarks and service marks in this document are the property of their respective owners.

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

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

Requests for any other permission to reproduce these VeriSign Certificate Policies (as well as requests for copies from VeriSign) must be addressed to VeriSign, Inc., 487 E. Middlefield Road, Mountain View, CA 94043 USA Attn: Practices Development. Tel: +1 650.961.7500 Fax: +1 650.426.7300 Net: [practices@verisign.com](mailto:practices@verisign.com).

## Table of Contents

1.	INTRODUCTION .....	11
1.1	Overview .....	11
1.2	Document name and Identification .....	12
1.3	PKI Participants .....	12
1.3.1	Certification Authorities .....	12
1.3.2	Registration Authorities .....	13
1.3.3	Subscribers .....	13
1.3.4	Relying Parties .....	14
1.3.5	Other Participants .....	14
1.4	Certificate Usage .....	14
1.4.1	Appropriate Certificate Usages .....	14
1.4.2	Prohibited Certificate Uses .....	15
1.5	Policy Administration .....	16
1.5.1	Organization Administering the Document .....	16
1.5.2	Contact Person .....	16
1.5.3	Person Determining CP Suitability for the Policy .....	16
1.5.4	CPS Approval Procedure .....	16
1.6	Definitions and Acronyms .....	16
2.	Publication and Repository Responsibilities .....	17
2.1	Repositories .....	17
2.2	Publication of Certificate Information .....	17
2.3	Time or Frequency of Publication .....	18
2.4	Access Controls on Repositories .....	18
3.	Identification and Authentication .....	18
3.1	Naming .....	18
3.1.1	Type of Names .....	19
3.1.2	Need for Names to be Meaningful .....	19
3.1.3	Anonymity or pseudonymity of Subscribers .....	20
3.1.4	Rules for Interpreting Various Name Forms .....	21
3.1.5	Uniqueness of Names .....	21
3.1.6	Recognition, Authentication, and Role of Trademarks .....	21
3.2	Initial Identity Validation .....	21
3.2.1	Method to Prove Possession of Private Key .....	21
3.2.2	Authentication of Organization identity .....	21
3.2.3	Authentication of Individual Identity .....	22
3.2.4	Non-Verified Subscriber information .....	23
3.2.5	Validation of Authority .....	24
3.2.6	Criteria for Interoperation .....	24
3.3	Identification and Authentication for Re-key Requests .....	24
3.3.1	Identification and Authentication for Routine Re-key .....	25
3.3.2	Identification and Authentication for Re-key After Revocation .....	25
3.4	Identification and Authentication for Revocation Request .....	26
4.	Certificate Life-Cycle Operational Requirements .....	26
4.1	Certificate Application .....	26
4.1.1	Who Can Submit a Certificate Application? .....	26
4.1.2	Enrollment Process and Responsibilities .....	26
4.2	Certificate Application Processing .....	27
4.2.1	Performing Identification and Authentication Functions .....	27
4.2.2	Approval or Rejection of Certificate Applications .....	27
4.2.3	Time to Process Certificate Applications .....	27
4.3	Certificate Issuance .....	27
4.3.1	CA Actions during Certificate Issuance .....	27
4.3.2	Notifications to Subscriber by the CA of Issuance of Certificate .....	28
4.4	Certificate Acceptance .....	28
4.4.1	Conduct Constituting Certificate Acceptance .....	28
4.4.2	Publication of the Certificate by the CA .....	28
4.4.3	Notification of Certificate Issuance by the CA to Other Entities .....	28

4.5	Key Pair and Certificate Usage .....	28
4.5.1	Subscriber Private Key and Certificate Usage .....	28
4.5.2	Relying Party Public Key and Certificate Usage .....	28
4.6	Certificate Renewal .....	29
4.6.1	Circumstances for Certificate Renewal .....	29
4.6.2	Who May Request Renewal .....	29
4.6.3	Processing Certificate Renewal Requests .....	29
4.6.4	Notification of New Certificate Issuance to Subscriber .....	30
4.6.5	Conduct Constituting Acceptance of a Renewal Certificate .....	30
4.6.6	Publication of the Renewal Certificate by the CA .....	30
4.6.7	Notification of Certificate Issuance by the CA to Other Entities .....	30
4.7	Certificate Re-Key .....	30
4.7.1	Circumstances for Certificate Re-Key .....	30
4.7.2	Who May Request Certification of a New Public Key .....	30
4.7.3	Processing Certificate Re-Keying Requests .....	30
4.7.4	Notification of New Certificate Issuance to Subscriber .....	31
4.7.5	Conduct Constituting Acceptance of a Re-Keyed Certificate .....	31
4.7.6	Publication of the Re-Keyed Certificate by the CA .....	31
4.7.7	Notification of Certificate Issuance by the CA to Other Entities .....	31
4.8	Certificate Modification .....	31
4.8.1	Circumstances for Certificate Modification .....	31
4.8.2	Who May Request Certificate Modification .....	31
4.8.3	Processing Certificate Modification Requests .....	31
4.8.4	Notification of New Certificate Issuance to Subscriber .....	32
4.8.5	Conduct Constituting Acceptance of Modified Certificate .....	32
4.8.6	Publication of the Modified Certificate by the CA .....	32
4.8.7	Notification of Certificate Issuance by the CA to Other Entities .....	32
4.9	Certificate Revocation and Suspension .....	32
4.9.1	Circumstances for Revocation .....	32
4.9.2	Who Can Request Revocation .....	33
4.9.3	Procedure for Revocation Request .....	33
4.9.4	Revocation Request Grace Period .....	33
4.9.5	Time within Which CA Must Process the Revocation Request .....	34
4.9.6	Revocation Checking Requirements for Relying Parties .....	34
4.9.7	CRL Issuance Frequency .....	34
4.9.8	Maximum Latency for CRLs .....	34
4.9.9	On-Line Revocation/Status Checking Availability .....	34
4.9.10	On-Line Revocation Checking Requirements .....	35
4.9.11	Other Forms of Revocation Advertisements Available .....	35
4.9.12	Special Requirements regarding Key Compromise .....	35
4.9.13	Circumstances for Suspension .....	35
4.9.14	Who Can Request Suspension .....	35
4.9.15	Procedure for Suspension Request .....	35
4.9.16	Limits on Suspension Period .....	35
4.10	Certificate Status Services .....	35
4.10.1	Operational Characteristics .....	35
4.10.2	Service Availability .....	35
4.10.3	Optional Features .....	36
4.11	End of Subscription .....	36
4.12	Key Escrow and Recovery .....	36
4.12.1	Key Escrow and Recovery Policy and Practices .....	36
4.12.2	Session Key Encapsulation and Recovery Policy and Practices .....	37
5.	Facility, Management, and Operational Controls .....	37
5.1	Physical Controls .....	37
5.1.1	Site Location and Construction .....	37
5.1.2	Physical Access .....	37
5.1.3	Power and Air Conditioning .....	37

5.1.4	Water Exposures .....	38
5.1.5	Fire Prevention and Protection .....	38
5.1.6	Media Storage .....	38
5.1.7	Waste Disposal .....	38
5.1.8	Off-Site Backup .....	38
5.2	Procedural Controls .....	38
5.2.1	Trusted Roles .....	39
5.2.2	Number of Persons Required per Task .....	39
5.2.3	Identification and Authentication for Each Role .....	39
5.2.4	Roles Requiring Separation of Duties .....	40
5.3	Personnel Controls .....	40
5.3.1	Qualifications, Experience, and Clearance Requirements .....	40
5.3.2	Background Check Procedures .....	40
5.3.3	Training Requirements .....	41
5.3.4	Retraining Frequency and Requirements .....	41
5.3.5	Job Rotation Frequency and Sequence .....	41
5.3.6	Sanctions for Unauthorized Actions .....	41
5.3.7	Independent Contractor Requirements .....	41
5.3.8	Documentation Supplied to Personnel .....	42
5.4	Audit Logging Procedures .....	42
5.4.1	Types of Events Recorded .....	42
5.4.2	Frequency of Processing Log .....	42
5.4.3	Retention Period for Audit Log .....	43
5.4.4	Protection of Audit Log .....	43
5.4.5	Audit Log Backup Procedures .....	43
5.4.6	Audit Collection System (Internal vs. External) .....	43
5.4.7	Notification to Event-Causing Subject .....	43
5.4.8	Vulnerability Assessments .....	43
5.5	Records Archival .....	43
5.5.1	Types of Records Archived .....	43
5.5.2	Retention Period for Archive .....	43
5.5.3	Protection of Archive .....	44
5.5.4	Archive Backup Procedures .....	44
5.5.5	Requirements for Time-Stamping of Records .....	44
5.5.6	Archive Collection System (Internal or External) .....	44
5.5.7	Procedures to Obtain and Verify Archive Information .....	44
5.6	Key Changeover .....	44
5.7	Compromise and Disaster Recovery .....	45
5.7.1	Incident and Compromise Handling Procedures .....	45
5.7.2	Computing Resources, Software, and/or Data Are Corrupted .....	45
5.7.3	Entity Private Key Compromise Procedures .....	45
5.7.4	Business Continuity Capabilities After a Disaster .....	45
5.8	CA or RA Termination .....	46
6.	Technical Security Controls .....	47
6.1	Key Pair Generation and Installation .....	47
6.1.1	Key Pair Generation .....	47
6.1.2	Private Key Delivery to Subscriber .....	47
6.1.3	Public Key Delivery to Certificate Issuer .....	48
6.1.4	CA Public Key Delivery to Relying Parties .....	48
6.1.5	Key Sizes .....	48
6.1.6	Public Key Parameters Generation and Quality Checking .....	48
6.1.7	Key Usage Purposes (as per X.509 v3 Key Usage Field) .....	48
6.2	Private Key Protection and Cryptographic Module Engineering Controls .....	48
6.2.1	Cryptographic Module Standards and Controls .....	49
6.2.2	Private Key (n out of m) Multi-Person Control .....	49
6.2.3	Private Key Escrow .....	49
6.2.4	Private Key Backup .....	49

6.2.5	Private Key Archival.....	49
6.2.6	Private Key Transfer Into or From a Cryptographic Module.....	49
6.2.7	Private Key Storage on Cryptographic Module.....	50
6.2.8	Method of Activating Private Key.....	50
6.2.9	Method of Deactivating Private Key.....	51
6.2.10	Method of Destroying Private Key.....	51
6.2.11	Cryptographic Module Rating.....	52
6.3	Other Aspects of Key Pair Management.....	52
6.3.1	Public Key Archival.....	52
6.3.2	Certificate Operational Periods and Key Pair Usage Periods.....	52
6.4	Activation Data.....	53
6.4.1	Activation Data Generation and Installation.....	53
6.4.2	Activation Data Protection.....	54
6.4.3	Other Aspects of Activation Data.....	54
6.5	Computer Security Controls.....	54
6.5.1	Specific Computer Security Technical Requirements.....	54
6.5.2	Computer Security Rating.....	54
6.6	Life Cycle Technical Controls.....	55
6.6.1	System Development Controls.....	55
6.6.2	Security Management Controls.....	55
6.6.3	Life Cycle Security Controls.....	55
6.7	Network Security Controls.....	55
6.8	Time-Stamping.....	56
7.	Certificate, CRL, and OCSP Profiles.....	56
7.1	Certificate Profile.....	56
7.1.1	Version Number(s).....	56
7.1.2	Certificate Extensions.....	56
7.1.3	Algorithm Object Identifiers.....	59
7.1.4	Name Forms.....	59
7.1.5	Name Constraints.....	59
7.1.6	Certificate Policy Object Identifier.....	60
7.1.7	Usage of Policy Constraints Extension.....	60
7.1.8	Policy Qualifiers Syntax and Semantics.....	60
7.1.9	Processing Semantics for the Critical Certificate Policies Extension.....	60
7.2	CRL Profile.....	60
7.2.1	Version Number(s).....	60
7.2.2	CRL and CRL Entry Extensions.....	60
7.3	OCSP Profile.....	61
7.3.1	Version Number(s).....	61
7.3.2	OCSP Extensions.....	61
8.	Compliance Audit and Other Assessments.....	61
8.1	Frequency and Circumstances of Assessment.....	61
8.2	Identity/Qualifications of Assessor.....	62
8.3	Assessor's Relationship to Assessed Entity.....	62
8.4	Topics Covered by Assessment.....	62
8.5	Actions Taken as a Result of Deficiency.....	62
8.6	Communications of Results.....	62
9.	Other Business and Legal Matters.....	62
9.1	Fees.....	62
9.1.1	Certificate Issuance or Renewal Fees.....	62
9.1.2	Certificate Access Fees.....	62
9.1.3	Revocation or Status Information Access Fees.....	63
9.1.4	Fees for Other Services.....	63
9.1.5	Refund Policy.....	63
9.2	Financial Responsibility.....	63
9.2.1	Insurance Coverage.....	63
9.2.2	Other Assets.....	63
9.2.3	Extended Warranty Coverage.....	64

9.3	Confidentiality of Business Information .....	64
9.3.1	Scope of Confidential Information.....	64
9.3.2	Information Not Within the Scope of Confidential Information .....	64
9.3.3	Responsibility to Protect Confidential Information .....	64
9.4	Privacy of Personal Information .....	64
9.4.1	Privacy Plan.....	64
9.4.2	Information Treated as Private .....	64
9.4.3	Information Not Deemed Private .....	64
9.4.4	Responsibility to Protect Private Information.....	65
9.4.5	Notice and Consent to Use Private Information.....	65
9.4.6	Disclosure Pursuant to Judicial or Administrative Process .....	65
9.4.7	Other Information Disclosure Circumstances.....	65
9.5	Intellectual Property rights .....	65
9.5.1	Property Rights in Certificates and Revocation Information .....	65
9.5.2	Property Rights in the CP .....	65
9.5.3	Property Rights in Names.....	65
9.5.4	Property Rights in Keys and Key Material .....	66
9.6	Representations and Warranties.....	66
9.6.1	CA Representations and Warranties.....	66
9.6.2	RA Representations and Warranties.....	66
9.6.3	Subscriber Representations and Warranties.....	66
9.6.4	Relying Party Representations and Warranties.....	67
9.6.5	Representations and Warranties of Other Participants .....	67
9.7	Disclaimers of Warranties .....	67
9.8	Limitations of Liability .....	67
9.9	Indemnities .....	68
9.9.1	Indemnification by Subscribers .....	68
9.9.2	Indemnification by Relying Parties.....	68
9.10	Term and Termination.....	68
9.10.1	Term .....	68
9.10.2	Termination.....	68
9.10.3	Effect of Termination and Survival.....	69
9.11	Individual Notices and Communications with Participants .....	69
9.12	Amendments.....	69
9.12.1	Procedure for Amendment.....	69
9.12.2	Notification Mechanism and Period .....	69
9.12.3	Circumstances Under Which OID Must be Changed .....	70
9.13	Dispute Resolution Provisions .....	70
9.13.1	Disputes Among VeriSign, Affiliates, and Customers.....	70
9.13.2	Disputes with End-User Subscribers or Relying Parties .....	70
9.14	Governing Law.....	70
9.15	Compliance with Applicable Law.....	71
9.16	Miscellaneous Provisions.....	71
9.16.1	Entire Agreement .....	71
9.16.2	Assignment.....	71
9.16.3	Severability .....	71
9.16.4	Enforcement (Attorney's Fees and Waiver of Rights).....	71
9.16.5	Force Majeure .....	71
9.17	Other Provisions .....	71
Appendix A.	Table of Acronyms and definitions.....	72
	Table of Acronyms .....	72
	Definitions .....	72
Appendix B1.	Supplemental Validation Procedures for Extended Validation SSL Certificates .....	77
Appendix B2 —	Minimum Cryptographic Algorithm and Key Sizes .....	107
Appendix B3 —	EV Certificates Required Certificate Extensions .....	108

# 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.

This CPS conforms to the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policy and Certification Practice Statement construction.

## 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 to 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<sup>1</sup> 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<sup>2</sup>, 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.

---

<sup>1</sup> 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

<sup>2</sup> Class 4 certificates are not currently issued by the VTN

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 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.<sup>3</sup>

### **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.

---

<sup>3</sup> 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 with Extended Validation	High assurance	Medium assurance	Code/Content Signing	Secure SSL/TLS-sessions	Authentication	Signing and encryption
Class 3 Certificates		✓		✓	✓	✓	✓
Class 3 EV Certificates	✓	✓			✓	✓	✓

**Table 2. Organizational Certificate Usage<sup>4</sup>**

### 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.

**High assurance with extended validation certificates** are Class 3 certificates issued by VeriSign in conformance with the Guidelines for Extended Validation Certificates.

### 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

<sup>4</sup> "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."

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 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](mailto: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.

<b>Certificate Type</b>	<b>Publication Requirements</b>
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.

<b>Certificate Type</b>	<b>Publication Requirements</b>
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 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 <a href="http://directory.verisign.com">directory.verisign.com</a> .
VeriSign OCSP Responder Certificates	Available through query of the VeriSign LDAP directory server at <a href="http://directory.verisign.com">directory.verisign.com</a> .
End-User Subscriber Certificates	Available to relying parties through query functions in the VeriSign repository at: <a href="https://digitalid.verisign.com/services/client/index.html">https://digitalid.verisign.com/services/client/index.html</a> and <a href="https://digitalid.verisign.com/services/server/search.htm">https://digitalid.verisign.com/services/server/search.htm</a> . Also available through query of the VeriSign LDAP directory server at <a href="http://directory.verisign.com">directory.verisign.com</a> .
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.
End-User Subscriber Certificates issued by VeriSign Class 3 Organizational VIP Device CA	Not available through public query

**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.

<b>Attribute</b>	<b>Value</b>
Country (C) =	"US" or not used.
Organization (O) =	"VeriSign, Inc." <sup>5</sup>
Organizational Unit (OU) =	VeriSign CA Certificates may contain multiple OU attributes. Such attributes may contain one or more of the following: <ul style="list-style-type: none"> <li>• CA Name</li> <li>• VeriSign Trust Network</li> <li>• A statement referencing the applicable Relying Party Agreement governing terms of use of the Certificate and</li> <li>• A copyright notice.</li> <li>• Text to describe the type of Certificate.</li> </ul>
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.

<b>Attribute</b>	<b>Value</b>
Country (C) =	2 letter ISO country code or not used.
Organization (O) =	The Organization attribute is used as follows: <ul style="list-style-type: none"> <li>• "VeriSign, Inc." for VeriSign OCSP Responder and optionally for individual Certificates that do not have an organization affiliation.</li> <li>• Subscriber organizational name for web server Certificates and individual Certificates that have an organization affiliation.</li> </ul>
Organizational Unit (OU) =	VeriSign end-user Subscriber Certificates may contain multiple OU attributes. Such attributes may contain one or more of the following: <ul style="list-style-type: none"> <li>• Subscriber organizational unit (for organizational Certificates and individual Certificates that have an organization affiliation)</li> <li>• VeriSign Trust Network</li> <li>• A statement referencing the applicable Relying Party Agreement governing terms of use of the Certificate</li> <li>• A copyright notice</li> <li>• "Authenticated by VeriSign" and "Member, VeriSign Trust Network" in Certificates whose applications were authenticated by VeriSign</li> <li>• "Persona Not Validated" for Class 1 Individual Certificates</li> <li>• Text to describe the type of Certificate.</li> </ul>

<sup>5</sup> An exception to this is the Secure Server CA, which indicates "RSA Data Security, Inc.," but is now a VeriSign CA.

<b>Attribute</b>	<b>Value</b>
	•
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: <ul style="list-style-type: none"> <li>• The OCSP Responder Name (for OCSP Responder Certificates)</li> <li>• Domain name (for web server Certificates)</li> <li>• Organization name (for code/object signing Certificates)</li> <li>• Name (for individual Certificates).</li> </ul>
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.

EV SSL certificate content and profile requirements are discussed in Section 6 of Appendix B3 to this CPS.

### **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.

<b>Certificate Type</b>	<b>Additional Procedures</b>
<b>Extended Validation Certificates</b>	VeriSign’s procedures for issuing Extended Validation SSL Certificates are described in Appendix B1 to this CPS.
<b>OFX Server IDs</b>	VeriSign verifies that the Organization is a bank or financial institution, or classified under one of the following SIC codes: <ul style="list-style-type: none"> <li>• 60xx Depository institutions</li> <li>• 61xx Nondepository credit institutions</li> <li>• 62xx Security, commodity brokers, and services</li> <li>• 63xx Insurance carriers</li> <li>• 64xx Insurance agents, brokers, and services</li> <li>• 67xx Holding and other investment offices</li> <li>• 7372 Prepackaged software</li> <li>• 7373 Computer integrated systems design</li> <li>• 7374 Data processing and preparation</li> <li>• 3661 Telephone and telegraph apparatus</li> <li>• 8721 Accounting, auditing, and bookkeeping.</li> </ul>
<b>Hardware Protected SSL Certificate</b>	VeriSign verifies that the key pair was generated on FIPS 140 certified hardware
<b>Managed PKI for Intranet SSL Certificate</b>	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.
<b>Authenticated Content Signing Certificate</b>	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.

<b>Certificate Class</b>	<b>Authentication of Identity</b>
<b>Class 1</b>	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.
<b>Class 2</b>	Authenticate identity by matching the identity provided by the Subscriber to: <ul style="list-style-type: none"> <li>• 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</li> <li>• information contained in the business</li> </ul>

	<p>records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals</p>
<p><b>Class 3</b></p>	<p>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.</p> <p>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.</p> <p>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.<sup>6</sup></p>

**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.

---

<sup>6</sup> 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.

### **3.2.5 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.

### **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<sup>7</sup>
- 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."

---

<sup>7</sup> Customers of VeriSign's Certificate Interoperability Service (CIS) are encouraged, but not required, to have their own CPS under the Certificate Interoperability Service (CIS) CP Supplement, but in all cases must comply with VeriSign's Certificate Interoperability Service (CIS) CP Supplement, published in the VeriSign Repository

### **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.<sup>8</sup>

In particular, for subsequent re-key requests for retail 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.”

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,

---

<sup>8</sup> 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 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 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<sup>9</sup>) 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 retail Class 3 Organizational certificates, VeriSign reauthenticates the Organization name and domain name included in the certificate. In circumstances where:

---

<sup>9</sup> If contact information has changed via an approved formal contact change procedure the certificate shall still qualify for automated renewal.

- 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

#### **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<sup>10</sup>) 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

#### **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

---

<sup>10</sup> If contact information has changed via an approved formal contact change procedure the certificate shall still qualify for automated renewal.

#### **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 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.<sup>11</sup>

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 through web-based query functions accessible through the VeriSign Repository at

---

<sup>11</sup> CRLs for the "VeriSign Class 3 Organizational VIP Device CA" are only issued whenever a certificate issued by that CA is revoked.

- <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 24x7 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<sup>12</sup>. 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.

### **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 VeriSign's independent audit requirements described in Section 8. 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

---

<sup>12</sup> 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.

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 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 § 4.9.

### **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 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](http://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.

<b><i>Certificate Issued By:</i></b>	<b><i>Validity Period</i></b>
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 <sup>13</sup>
Offline intermediate CA to online CA	Generally 5 years but up to 10 years after renewal <sup>14</sup>

<sup>13</sup> The VeriSign Onsite Administrator CA-Class 3 has a validity beyond 10 years to support legacy systems and shall be revoked when appropriate

<sup>14</sup> 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.

<b>Certificate Issued By:</b>	<b>Validity Period</b>
Online CA to End-user Individual Subscriber	Normally up to 2 years, but under the conditions described below, up to 5 years <sup>15</sup>
Online CA to End-Entity Organizational Subscriber	Normally up to 2 years <sup>16,17</sup>

**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 operates the "VeriSign Class 3 Organizational VIP Device CA". Organizational end-entity certificates issued by this CA may have a validity period beyond 3 years and up to a maximum of 5 years in circumstances where:

- The certificate key pair is stored in hardware, and
- VeriSign has authenticated the Organization in terms of this CPS and
- When used to protect a server using SSL/TLS, the server is only accessible via a private network or intranet .

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.

## **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;

<sup>15</sup> 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.

<sup>16</sup> VeriSign may issue **retail** Organization Certificates with a three year validity.

<sup>17</sup> 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.

- 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:

<b>Field</b>	<b>Value or Value constraint</b>
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.

EV SSL certificate extension requirements are described in Appendix B3 to this CPS.

##### 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.

		<b>CAs</b>	<b>Class 1 and Class 2 End-User Subscribers</b>	<b>Automated Administration tokens and Class 2-3 End-User Subscribers</b>	<b>Dual Key Pair Signature (Managed PKI Key Manager)</b>	<b>Dual Key Pair Encipherment (Managed PKI Key Manager)</b>
<b>Criticality</b>		FALSE	FALSE	FALSE	FALSE	FALSE
<b>0</b>	digitalSignature	Clear	Set	Set	Set	Clear
<b>1</b>	nonRepudiation	Clear	Clear	Clear	Clear	Clear
<b>2</b>	keyEncipherment	Clear	Set	Set	Clear	Set
<b>3</b>	dataEncipherment	Clear	Clear	Clear	Clear	Clear
<b>4</b>	keyAgreement	Clear	Clear	Clear	Clear	Clear
<b>5</b>	keyCertSign	Set	Clear	Clear	Clear	Clear
<b>6</b>	CRLSign	Set	Clear	Clear	Clear	Clear
<b>7</b>	encipherOnly	Clear	Clear	Clear	Clear	Clear
<b>8</b>	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
<b>Criticality</b>	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: 2.16.840.1.113730.4.1	Set	Clear	Clear	Set	Clear	Clear
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 Section 1.2. 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

VeriSign generally populates X.509 Version 3 VTN Certificates with a policy qualifier within the Certificate Policies extension. Generally, such Certificates contain a CPS pointer qualifier that points to the applicable Relying Party Agreement or the VeriSign CPS. In addition, some Certificates contain a User Notice Qualifier which points to the applicable Relying Party Agreement.

### 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 Certificates	Listing of revoked certificates, including the Serial Number of the revoked Certificate and the Revocation Date.

Table 13 – CRL Profile Basic Fields

#### 7.2.1 Version Number(s)

VeriSign supports both X.509 Version 1 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<sup>(sm)</sup> 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 damages concerning a specific Certificate:

<b>Class</b>	<b>Liability Caps</b>
<b>Class 1</b>	One Hundred U.S. Dollars (\$ 100.00 US)
<b>Class 2</b>	Five Thousand U.S. Dollars (\$ 5,000.00 US)
<b>Class 3</b>	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.

VeriSign's limitation of liability for EV certificates is further described in Section 37 of Appendix B1 to this CPS.

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

### **Definitions**

Term	Definition
<b>Administrator</b>	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.
<b>Administrator Certificate</b>	A Certificate issued to an Administrator that may only be used to perform CA or RA functions.
<b>Affiliate</b>	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.
<b>Affiliate Audit Program Guide</b>	A VeriSign document containing requirements for the Compliance Audits of Affiliates, including Certificate Management Control Objectives against which Affiliates will be audited.
<b>Affiliate Practices Legal Requirements Guidebook</b>	A VeriSign document setting forth requirements for Affiliate CPSs, agreements, validation procedures, and privacy policies, as well as other requirements that Affiliates must meet.

<b>Term</b>	<b>Definition</b>
<b>Affiliated Individual</b>	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.
<b>Applicant</b>	The Private Organization or Government Entity that applies for (or seeks renewal of) an EV Certificate naming it as the Subject.
<b>Applicant Representative</b>	An individual person employed by the Applicant for an EV certificate: (i) who signs and submits, or approves an EV Certificate Request on behalf of an Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of an Applicant.
<b>Application Software Vendor</b>	A developer of Internet browser software or other software that displays or uses certificates and distributes root certificates, such as KDE, Microsoft Corporation, Mozilla Corporation, Opera Software ASA, and Red Hat, Inc.
<b>Automated Administration</b>	A procedure whereby Certificate Applications are approved automatically if enrollment information matches information contained in a database.
<b>Automated Administration Software Module</b>	Software provided by VeriSign that performs Automated Administration.
<b>Certificate</b>	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.
<b>Certificate Applicant</b>	An individual or organization that requests the issuance of a Certificate by a CA.
<b>Certificate Application</b>	A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.
<b>Certificate Approver</b>	[defined in Section 10]
<b>Certificate Chain</b>	An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.
<b>Certificate Management Control Objectives</b>	Criteria that an entity must meet in order to satisfy a Compliance Audit.
<b>Certificate Policies (CP)</b>	This document, which is entitled "VeriSign Trust Network Certificate Policies" and is the principal statement of policy governing the VTN.
<b>Certificate Requester: [defined in Section 10]</b>	
<b>Certificate Revocation List (CRL)</b>	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.
<b>Certificate Signing Request</b>	A message conveying a request to have a Certificate issued.
<b>Certification Authority (CA)</b>	An entity authorized to issue, manage, revoke, and renew Certificates in the VTN.
<b>Certification Practice Statement (CPS)</b>	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.
<b>Challenge Phrase</b>	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.
<b>Class</b>	A specified level of assurances as defined within the CP. See CP § 1.1.1.
<b>Client Service Center</b>	A Service Center that is an Affiliate providing client Certificates either in the Consumer or Enterprise line of business.
<b>Compliance Audit</b>	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.
<b>Compromise</b>	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.
<b>Confidential/Private Information</b>	Information required to be kept confidential and private pursuant to CP § 2.8.1.
<b>Contract Signer: [defined in Section 10]</b>	

<b>Term</b>	<b>Definition</b>
<b>CRL Usage Agreement</b>	An agreement setting forth the terms and conditions under which a CRL or the information in it can be used.
<b>Customer</b>	An organization that is either a Managed PKI Customer, Gateway Customer, or ASB Customer.
<b>Demand Deposit Account</b>	A deposit account held at a bank or other financial institution, the funds deposited in which are payable on demand. The primary purpose of demand accounts is to facilitate cashless payments by means of check, bank draft, direct debit, electronic funds transfer, etc. Usage varies among countries, but a demand deposit account is commonly known as: a checking account, a share draft account, a current account, or a checking account.
<b>Enterprise, as in Enterprise Service Center</b>	A line of business that an Affiliate enters to provide Managed PKI services to Managed PKI Customers.
<b>Enterprise EV Certificate:</b>	An EV Certificate that an Managed PKI for SSL Customer authorizes VeriSign to issue at third and higher domain levels that contain the domain that have been verified by VeriSign.
<b>Enterprise RA</b>	A Managed PKI for SSL customer that can request multiple valid EV Certificates for Domains and Organizations verified by VeriSign for domains at third and higher domain levels that contain a domain that was verified by VeriSign in the original EV Certificate, in accordance with the requirements of these Guidelines.
<b>Enterprise Roaming Server</b>	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.
<b>EV Certificate:</b>	A digital certificate that contains information specified in the EV Guidelines and that has been validated in accordance with the Guidelines.
<b>EV OID</b>	An identifying number, called an "object identifier," that is included in the certificatePolicies field of an EV certificate that: (i) indicates which CA policy statement relates to that certificate, and which, (ii) by pre-agreement with one or more Application Software Vendor, marks the certificate as being an EV Certificate.
<b>Exigent Audit/Investigation</b>	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.
<b>Extended Validation</b>	Validation Procedures defined by the Guidelines for Extended Validation Certificates published by a forum consisting of major certification authorities and browser vendors.
<b>Intellectual Property Rights</b>	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.
<b>Intermediate Certification Authority (Intermediate CA)</b>	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.
<b>Key Generation Ceremony</b>	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.
<b>Key Manager Administrator</b>	An Administrator that performs key generation and recovery functions for a Managed PKI Customer using Managed PKI Key Manager.
<b>Key Recovery Block (KRB)</b>	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.
<b>Key Recovery Service</b>	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.
<b>Managed PKI</b>	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.
<b>Managed PKI Administrator</b>	An Administrator that performs validation or other RA functions for an Managed PKI Customer.
<b>Managed PKI Control Center</b>	A web-based interface that permits Managed PKI Administrators to perform Manual Authentication of Certificate Applications
<b>Managed PKI Key Manager</b>	A key recovery solution for those Managed PKI Customers choosing to implement key recovery under a special Managed PKI Agreement.
<b>Managed PKI Key Management Service Administrator's Guide</b>	A document setting forth the operational requirements and practices for Managed PKI Customers using Managed PKI Key Manager.
<b>Manual Authentication</b>	A procedure whereby Certificate Applications are reviewed and approved manually one-by-

<b>Term</b>	<b>Definition</b>
	one by an Administrator using a web-based interface.
<b>NetSure Protection Plan</b>	An extended warranty program, which is described in CP § 1.1.2.2.3.
<b>Nonverified Subscriber Information</b>	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.
<b>Non-repudiation</b>	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.
<b>Offline CA</b>	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.
<b>Online CA</b>	CAs that sign end user Subscriber Certificates are maintained online so as to provide continuous signing services.
<b>Online Certificate Status Protocol (OCSP)</b>	A protocol for providing Relying Parties with real-time Certificate status information.
<b>Operational Period</b>	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.
<b>PKCS #10</b>	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
<b>PKCS #12</b>	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
<b>Policy Management Authority (PMA)</b>	The organization within VeriSign responsible for promulgating this policy throughout the VTN.
<b>Primary Certification Authority (PCA)</b>	A CA that acts as a root CA for a specific Class of Certificates, and issues Certificates to CAs subordinate to it.
<b>Processing Center</b>	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.
<b>Public Key Infrastructure (PKI)</b>	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system. The VTN PKI consists of systems that collaborate to provide and implement the VTN.
<b>Registration Authority (RA)</b>	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.
<b>Regulated Financial Institution</b>	A financial institution that is regulated, supervised, and examined by governmental, national, state or provincial, or local authorities having regulatory authority over such financial institution based on the governmental, national, state or provincial, or local laws under which such financial institution was organized and/or licensed.
<b>Relying Party</b>	An individual or organization that acts in reliance on a certificate and/or a digital signature.
<b>Relying Party Agreement</b>	An agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a Relying Party.
<b>Retail Certificate</b>	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.
<b>Roaming Subscriber</b>	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.
<b>RSA</b>	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
<b>RSA Secure Server Certification Authority (RSA Secure Server CA)</b>	The Certification Authority that issues Secure Server IDs.

<b>Term</b>	<b>Definition</b>
<b>RSA Secure Server Hierarchy</b>	The PKI hierarchy comprised of the RSA Secure Server Certification Authority.
<b>Secret Share</b>	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.
<b>Secret Sharing</b>	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.
<b>Secure Server ID</b>	A Class 3 organizational Certificate used to support SSL sessions between web browsers and web servers.
<b>Secure Sockets Layer (SSL)</b>	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.
<b>Security and Audit Requirements Guide</b>	A VeriSign document that sets forth the security and audit requirements and practices for Processing Centers and Service Centers.
<b>Security and Practices Review</b>	A review of an Affiliate performed by VeriSign before an Affiliate is permitted to become operational.
<b>Service Center</b>	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.
<b>Subdomain</b>	The portion of the VTN under control of an entity and all entities subordinate to it within the VTN hierarchy.
<b>Subject</b>	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.
<b>Subscriber</b>	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.
<b>Subscriber Agreement</b>	An agreement used by a CA or RA setting forth the terms and conditions under which an individual or organization acts as a Subscriber.
<b>Superior Entity</b>	An entity above a certain entity within a VTN hierarchy (the Class 1, 2, or 3 hierarchy).
<b>Supplemental Risk Management Review</b>	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.
<b>Reseller</b>	An entity marketing services on behalf of VeriSign or an Affiliate to specific markets.
<b>Trusted Person</b>	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.
<b>Trusted Position</b>	The positions within a VTN entity that must be held by a Trusted Person.
<b>Trustworthy System</b>	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 government nomenclature.
<b>VeriSign</b>	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.
<b>VeriSign Digital Notarization Service</b>	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.
<b>VeriSign Repository</b>	VeriSign's database of Certificates and other relevant VeriSign Trust Network information accessible on-line.
<b>VeriSign Roaming Server</b>	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.
<b>VeriSign Roaming Service</b>	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.
<b>VeriSign Trust Network (VTN)</b>	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.
<b>VTN Participant</b>	An individual or organization that is one or more of the following within the VTN: VeriSign,

<b>Term</b>	<b>Definition</b>
	an Affiliate, a Customer, a Universal Service Center, a Reseller, a Subscriber, or a Relying Party.
<b><i>VTN Standards</i></b>	The business, legal, and technical requirements for issuing, managing, revoking, renewing, and using Certificates within the VTN.

# Appendix B1

## Supplemental Validation Procedures for Extended Validation SSL Certificates

### TABLE OF CONTENTS

	<u>Page</u>
<b>A. INTRODUCTION .....</b>	<b>80</b>
1. Introduction.....	80
<b>B. BASIC CONCEPT OF THE EV CERTIFICATE .....</b>	<b>80</b>
2. Purpose of EV Certificates .....	80
(a) Primary Purposes .....	80
(b) Secondary Purposes.....	81
(c) Excluded Purposes.....	81
3. EV Certificate Warranties and Representations.....	81
(a) By VeriSign .....	81
(b) By the Subscriber.....	82
<b>C. COMMUNITY AND APPLICABILITY.....</b>	<b>82</b>
4. Issuance of EV Certificates .....	82
(a) Compliance .....	83
(b) EV Policies.....	83
(c) Insurance .....	83
5. Obtaining EV Certificates .....	84
(a) Private Organization Subjects.....	84
(b) Government Entity Subjects .....	84
(c) Excluded Subjects .....	84
<b>D. EV CERTIFICATE CONTENT AND PROFILE .....</b>	<b>85</b>
6. EV Certificate Content Requirements .....	85
(a) Subject Organization Information.....	85
7. EV Certificate Policy Identification Requirements .....	87
(a) EV Subscriber Certificates.....	87
(b) EV Subordinate CA Certificates.....	87
(c) Root CA Certificates .....	87
8. Maximum Validity Period.....	87
(a) For EV Certificate.....	87
(b) For Validated Data.....	87
9. Other Technical Requirements for EV Certificates.....	87
<b>E. EV CERTIFICATE REQUEST REQUIREMENTS.....</b>	<b>87</b>
10. General Requirements .....	87
(a) Documentation Requirements .....	87
(b) Role Requirements .....	88
11. EV Certificate Request Requirements.....	88
(a) General .....	88
(b) Request and Certification.....	88
(c) Information Requirements.....	89
12. Subscriber Agreement Requirements .....	89
(a) General .....	89
(b) Agreement Requirements .....	90
<b>F. INFORMATION VERIFICATION REQUIREMENTS.....</b>	<b>90</b>
13. General Overview.....	90
14. Verification of Applicant's Legal Existence and Identity .....	91
15. Verification of Applicant's Legal Existence and Identity – Assumed Name.....	91
16. Verification of Applicant's Physical Existence .....	91
(a) Address of Applicant's Place of Business.....	91
(b) Telephone Number for Applicant's Place of Business.....	92
17. Verification of Applicant's Operational Existence .....	93
18. Verification of Applicant's Domain Name .....	93
19. Verification of Name, Title and Authority of Contract Signer & Certificate Approver.....	94
20. Verification of Signature on Subscriber Agreement and EV Certificate Requests .....	96
(a) Verification Requirements.....	96
21. Verification of Approval of EV Certificate Request.....	97
22. Verification of Certain Information Sources.....	97
(a) Verified Legal Opinion.....	97
(b) Verified Accountant Letter.....	97

	(c)	Independent Confirmation From Applicant .....	98
	(d)	Qualified Independent Information Sources (QIIS) .....	99
	(e)	Qualified Government Information Sources (QGIS) .....	99
23.		Other Verification Requirements .....	9
	(a)	High Risk Status .....	99
	(b)	Denied Lists and Other Legal Black Lists .....	100
24.		Final Cross-Correlation and Due Diligence .....	100
25.		Certificate Renewal Verification Requirements .....	100
<b>G.</b>		<b>CERTIFICATE STATUS CHECKING AND REVOCATION ISSUES .....</b>	<b>100</b>
		26. EV Certificate Status Checking .....	100
		27. EV Certificate Revocation .....	101
		28. EV Certificate Problem Reporting and Response Capability .....	102
<b>H.</b>		<b>EMPLOYEE AND THIRD PARTY ISSUES.....</b>	<b>102</b>
		29. Trustworthiness and Competence.....	102
		30. Delegation of Functions to Registration Authorities and Subcontractors .....	102
<b>I.</b>		<b>DATA AND RECORD ISSUES .....</b>	<b>103</b>
		31. Documentation and Audit Trail Requirements.....	103
		32. Document Retention.....	104
	(a)	Audit Log Retention .....	104
	(b)	Retention of Documentation .....	104
		33. Reuse and Updating Information and Documentation .....	104
	(a)	Use of Documentation to Support Multiple EV Certificates.....	104
	(b)	Use of Pre-Existing Information or Documentation.....	104
		34. Data Security.....	104
<b>J.</b>		<b>COMPLIANCE.....</b>	<b>104</b>
		35. Audit Requirements .....	104
	(a)	Pre-Issuance Readiness Audit.....	104
	(b)	Regular Self Audits .....	104
	(c)	Annual Independent Audit.....	105
	(d)	Auditor Qualifications .....	105
	(e)	Root Key Generation .....	105
<b>K.</b>		<b>OTHER CONTRACTUAL COMPLIANCE .....</b>	<b>106</b>
		36. Privacy Issues .....	106
		37. Limitations on EV Certificate Liability .....	106
	(a)	CA Liability .....	106

## A. INTRODUCTION

### 1. Introduction

These procedures for Extended Validation Certificates document supplemental procedures to VeriSign's currently published CPS procedures for issuing Extended Validation Certificates ("EV Certificates") in terms of the Guidelines for Extended Validation Certificates ("Guidelines"). The Guidelines describe certain of the minimum requirements that a Certificate Authority (CA) must meet in order to issue Extended Validation Certificates ("EV Certificates"). Organization information from Valid EV Certificates may be displayed in a special manner by certain software applications (e.g., browser software) in order to provide users with a trustworthy confirmation of the identity of the entity that controls the website they are accessing.

## B. BASIC CONCEPT OF THE EV CERTIFICATE

### 2. Purpose of EV Certificates.

EV Certificates are intended for use in establishing web-based data communication conduits via TLS/SSL protocols.

#### (a) Primary Purposes

Per the guidelines, the primary purposes of an EV Certificate are to:

- Identify the legal entity that controls a website: Provide a reasonable assurance to the user of an Internet browser that the website the user is accessing is controlled by a specific legal entity identified in the EV Certificate by name, address of Place of Business, Jurisdiction of Incorporation, and Registration Number; and
- Enable/encrypted communications with a website: Facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a website.

#### (b) Secondary purposes

The secondary purpose of an EV Certificate are to help establish the legitimacy of a business claiming to operate a website by confirming its legal and physical existence, and to provide a vehicle that can be used to assist in addressing problems related to phishing and other forms of online identity fraud. By providing more reliable third-party verified identity and address information regarding the owner of a website, EV Certificates may help to:

- Make it more difficult to mount phishing and other online identity fraud attacks using SSL certificates;
- Assist companies that may be the target of phishing attacks or online identity fraud by providing them with a tool to better identify themselves and their legitimate websites to users; and
- Assist law enforcement in investigations of phishing and other online identity fraud, including where appropriate, contacting, investigating, or taking legal action against the Subject.

### **(c) Excluded Purposes**

EV Certificates focus only on the identity of the Subject named in the Certificate, and not on the behavior of the Subject. As such, an EV Certificate is ***not*** intended to provide any assurances, or otherwise represent or warrant:

- That the Subject named in the EV Certificate is actively engaged in doing business;
- That the Subject named in the EV Certificate complies with applicable laws;
- That the Subject named in the EV Certificate is trustworthy, honest, or reputable in its business dealings; or
- That it is “safe” to do business with the Subject named in the EV Certificate.

## **3. EV Certificate Warranties and Representations**

### **(a) By VeriSign**

Beneficiaries of EV Certificates may be:

- The Subscriber entering into the Subscriber Agreement for the EV Certificate;
- The Subject named in the EV Certificate;
- All Application Software Vendors with whom VeriSign or its Root CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Vendors;
- All Relying Parties that actually rely on such EV Certificate during the period when it is Valid.

When VeriSign issues an EV Certificate, it represents and warrants to the EV Certificate Beneficiaries, during the period when the EV Certificate is Valid, that the it has followed the requirements of the Guidelines and its EV Policies in issuing the EV Certificate and in verifying the accuracy of the information contained in the EV Certificate (“EV Certificate Warranty”). This EV Certificate Warranty specifically includes, but is not limited to, the following warranties:

- Legal Existence: VeriSign has confirmed with the Incorporating Agency in the Subject’s Jurisdiction of Incorporation that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate legally exists as a valid organization or entity in the Jurisdiction of Incorporation;
- Identity: VeriSign has confirmed that, as of the date the EV Certificate was issued, the legal name of the Subject named in the EV Certificate matches the name on the official government records of the Incorporating Agency in the Subject’s Jurisdiction of Incorporation, and if an assumed name is also included, that the assumed name is properly registered by the Subject in the jurisdiction of its Place of Business;
- Right to Use Domain Name: VeriSign has taken all steps reasonably necessary in terms of the Guidelines to verify that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate owns or has the exclusive right to use the domain name listed in the EV Certificate;
- Authorization for EV Certificate: VeriSign has taken all steps reasonably necessary in terms of the Guidelines to verify that the Subject named in the EV Certificate has authorized the issuance of the EV Certificate;
- Accuracy of Information: VeriSign has taken all steps reasonably necessary to verify that all of the other information in the EV Certificate is accurate, as of the date the EV Certificate was issued;

- Subscriber Agreement: The Subject named in the EV Certificate has entered into a legally valid and enforceable Subscriber Agreement with VeriSign that satisfies the requirements of the Guidelines;
- Status: VeriSign will follow the requirements of these Guidelines and maintain a 24 x 7 online-accessible Repository with current information regarding the status of the EV Certificate as Valid or revoked; and
- Revocation: VeriSign will follow the requirements of the Guidelines and promptly revoke the EV Certificate upon the occurrence of any revocation event as specified in the Guidelines and this Appendix.

EV Certificates focus only on the identity of the Subject named in the Certificate, and not on the behavior of the Subject. As such, when issuing an EV Certificate, VeriSign does not provide any assurances, or otherwise represent or warrant:

- That the Subject named in the EV Certificate is actively engaged in doing business;
- That the Subject named in the EV Certificate complies with applicable laws;
- That the Subject named in the EV Certificate is trustworthy, honest, or reputable in its business dealings; or
- That it is “safe” to do business with the Subject named in the EV Certificate.

### **(b) By the Subscriber**

VeriSign will require, as part of the Subscriber Agreement, that the Subscriber make the commitments and warranties set forth in Subscriber Agreement Requirements section of these Guidelines, for the benefit of VeriSign and the EV Certificate Beneficiaries.

## **C. COMMUNITY AND APPLICABILITY**

### **4. Issuance of EV Certificates**

When issuing EV Certificates, VeriSign satisfies the following requirements as required by the Guidelines:

#### **(a) Compliance**

VeriSign shall at all times:

- (1) Comply with all law applicable to its business and the certificates it issues in each jurisdiction where it operates;
- (2) Comply with the requirements of the EV Guidelines;
- (3) Comply with the requirements of (i) the then-current WebTrust Program for CAs, and (ii) the then-current WebTrust EV Program, or an equivalent for both (i) and (ii) as approved by the CA/Browser Forum; and
- (4) Be licensed as a CA in each jurisdiction where it operates if licensing is required by the law of such jurisdiction for the issuance of EV Certificates.

## **(b) EV Policies**

### **(1) Implementation**

The VeriSign CPS together with this Appendix B to the VeriSign CPS:

- (A) Implement the requirements of the Guidelines as they are revised from time-to-time;
- (B) Implement the requirements of (i) the then current WebTrust Program for CAs, and (ii) the then-current WebTrust EV Program, or an equivalent for both (i) and (ii) as approved by the CA/Browser Forum;
- (C) Specify the VeriSign's entire root certificate hierarchy including all roots that its EV Certificates depend on for proof of those EV Certificates' authenticity. VeriSign's root hierarchy structure is available at <http://www.verisign.com/repository/hierarchy/hierarchy.pdf>

### **(2) Disclosure**

VeriSign publicly discloses its EV Policies through this CPS that is available on a 24x7 basis from the VeriSign online repository. VeriSign's CPS is structured according to the RFC 3647 format.

### **(3) Commitment to Comply with Guidelines**

VeriSign conforms to the current version of the **CA/Browser Forum Guidelines for Extended Validation Certificates** ("Guidelines") published at <http://www.cabforum.org>. In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document.

In addition, VeriSign will include (directly or by reference) the applicable requirements of these Guidelines in all contracts with subordinate CAs, RAs, Enterprise RAs, and subcontractors, that involve or relate to the issuance or maintenance of EV Certificates. VeriSign MUST enforce compliance with such terms.

## **(c) Insurance**

VeriSign maintains the following insurance, with companies with companies rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide, related to its performance and obligations under the EV Guidelines as follows:

- o Commercial General Liability insurance (occurrence form) with policy limits of at least \$2 million in coverage, and
- o Professional Liability/Errors & Omissions insurance, with policy limits of at least \$5 million in coverage, and including coverage for (i) claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining EV Certificates, and (ii) claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, and trademark infringement), and invasion of privacy and advertising injury

## **5. Obtaining EV Certificates**

In terms of the Guidelines, EV Certificates can only be issued to Private Organizations and Government Entities that satisfy the requirements specified below:

### **(a) Private Organization Subjects**

VeriSign may issue EV Certificates to Private Organizations that satisfy the following requirements:

- (1) The organization **MUST** be a legally recognized entity whose existence was created by a filing with (or an act of) the Incorporating Agency, or Governing Body in its Jurisdiction of Incorporation (e.g., by issuance of a certificate of incorporation);
- (2) The organization **MUST** have designated with the Incorporating Agency, or Governing Body a Registered Agent, Registered Office (as required under the laws of the Jurisdiction of Incorporation) or equivalent;
- (3) The organization **MUST** not be designated on the records of the Incorporating Agency, or Governing Body by labels such as "inactive," "invalid," "not current," or the equivalent;
- (4) The organization's Jurisdiction of Incorporation and/or its Place of Business **MUST NOT** be in any country where VeriSign is prohibited from doing business or issuing a certificate by the laws of VeriSign's jurisdiction; and
- (5) The organization **MUST NOT** be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of VeriSign's jurisdiction.

### **(b) Government Entity Subjects**

VeriSign may issue EV Certificates to Government Entities that satisfy the following requirements:

- (1) The legal existence of the Government Entity is established by the law of the Jurisdiction of Incorporation. Government agencies and entities (for example State owned Universities) may be verified via the appropriate Government Entity established by the law of the Jurisdiction of Incorporation;
- (2) The Government Entity **MUST NOT** be in any country where VeriSign is prohibited from doing business or issuing a certificate by the laws of VeriSign's jurisdiction; and
- (3) The Government Entity **MUST NOT** be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of VeriSign's jurisdiction.

### **(c) Excluded Subjects**

Until additional criteria for validation are defined by the Guidelines, VeriSign can **NOT** issue EV Certificates to any person or any organization or entity that does not satisfy the requirements above, including but not limited to the following:

- (1) General partnerships
- (2) Unincorporated associations
- (3) Sole proprietorships
- (4) Individuals (natural persons)

## **D. EV CERTIFICATE CONTENT AND PROFILE**

### **6. EV Certificate Content Requirements**

This section sets forth minimum requirements for the content of the EV Certificate as they relate to the identity of VeriSign and the Subject of the EV Certificate.

#### **(a) Subject Organization Information**

Subject to the requirements of the Guidelines, the EV Certificate include the following information about the Subject organization in the fields listed (“Subject Organization Information”):

##### **(1) Organization name**

The validated organization name is included in the organizationName field (OID 2.5.4.10 )

This field contains the Subject’s full legal organization name as listed in the official records of the Incorporating Agency in the Subject’s Jurisdiction of Incorporation. In addition, an assumed name or d/b/a name used by the Subject MAY be included at the beginning of this field, provided that it is followed by the full legal organization name in parenthesis. If the combination of the full legal organization name and the assumed or d/b/a name exceeds 64 bytes as defined by RFC 3280, the VeriSign will use only the full legal organization name in the certificate.

##### **(2) Domain name**

The validated domain name is included in the subject: commonName field (OID 2.5.4.3) and/or SubjectAlternativeName as a DNS Name.

This field contains one or more host domain name(s) owned or controlled by the Subject and to be associated with Subject’s publicly accessible server. Such server may be owned and operated by the Subject or another entity (e.g., a hosting service). Wildcard certificates are not allowed for EV certificates.

##### **(3) Jurisdiction of Incorporation**

VeriSign will include the Subject’s validated jurisdiction of incorporation using the fields shown in Table 1 below.

Address Part	Required/Optional	Certificate Field
City or Town	If any	jurisdictionOfIncorporationLocalityName (1.3.6.1.4.1.311.60.2.1.1) ASN.1 - X520LocalityName as specified in RFC 3280
State or province (if any)	If any	jurisdictionOfIncorporationStateOrProvinceName (1.3.6.1.4.1.311.60.2.1.2) ASN.1 - X520StateOrProvinceName as specified in RFC 3280
Country	Required	jurisdictionOfIncorporationCountryName ASN.1 - X520countryName as specified in RFC 3280

**Table 1. Jurisdiction of Incorporation Certificate Fields**

These fields contain information only to the level of the Incorporating Agency – e.g., the Jurisdiction of Incorporation for an Incorporating Agency at the country level would include country information but may not include state or province or city or town information; the Jurisdiction of Incorporation for an Incorporating Agency at the state or province level would include both country and state or province information, but may not include city or town information; and so forth. Country information MUST be specified using the applicable ISO country code. State or province information, and City or town information (where applicable) for the Subject’s Jurisdiction of Incorporation MUST be specified using the full name of the applicable jurisdiction.

**(4) Registration Number**

VeriSign EV Certificates include the unique Registration Number assigned to the Subject by the Incorporating Agency in its Jurisdiction of Incorporation (for Private Organization Subjects only) in the serialNumber field (OID 2.5.4.5), unless the jurisdiction does not assign a unique registration number, in which case the field will include the date of incorporation.

**(5) Physical Address of Place of Business**

VeriSign EV certificates will include an address of a verified physical location of the Subject’s Place of Business, in terms of the table below.

Address Part	Required/Optional	Certificate Field
Number & street	Optional	streetAddress (OID 2.5.4.9)
City or Town	Required	localityName (OID 2.5.4.7)
State or province (if any)	Required	stateOrProvinceName (OID 2.5.4.8)
Country	Required	countryName (OID 2.5.4.6)
Postal code (optional)	Optional	postalCode (2.5.4.17)

**Table 2. Physical address of Place of Business Certificate Fields**

## **7. EV Certificate Policy Identification Requirements**

### **(a) EV Subscriber Certificates**

Each EV Certificate issued by VeriSign to a Subscriber will include VeriSign's EV OID in the certificate's certificatePolicies extension. VeriSign's EV OID used for this purpose is 2.16.840.1.113733.1.7.23.6

### **(b) EV Subordinate CA Certificate**

The VeriSign Class 3 High Assurance CA contains VeriSign's EV OID as well as the special anyPolicy OID (2.5.29.32.0) in the certificatePolicies extension

### **(c) Root CA Certificates**

VeriSign's Root CA Certificate for EV Certificates is the VeriSign Class 3 Primary Certification Authority. This Root CA does not contain the certificatePolicies or extendedKeyUsage fields

## **8. Maximum Validity Period**

### **(a) For EV Certificate**

The maximum validity period for an EV Certificate is twenty seven (27) months.

### **(b) For Validated Data**

The maximum validity period for validated data that can be used to support issuance of an EV Certificate (before revalidation is required) is as follows:

- Legal existence and identity – one (1) year;
- Assumed name – one (1) year;
- Address of Place of Business – one (1) year, but thereafter data may be refreshed by checking a Qualified Independent Information Source, even where a site visit was originally required;
- Telephone number for Place of Business – one (1) year;
- Bank account verification – one (1) years;
- Domain name – one (1) year;
- Identity and authority of Certificate Approver – one (1) year, unless a contract is in place between VeriSign and the Applicant that specifies a different term, in which case, the term specified in such contract will control. For example, the contract may use terms that allow the assignment of roles that are perpetual until revoked, or until agreement expires or terminated

## **9. Other Technical Requirements for EV Certificates**

See Appendix B2 and Appendix B3 attached.

## **E. EV CERTIFICATE REQUEST REQUIREMENTS**

### **10. General Requirements**

#### **(a) Documentation Requirements**

Prior to the issuance of an EV Certificate, VeriSign obtains from the Applicant the following documentation, in compliance with the requirements of these Guidelines:

- EV Certificate Request
- Subscriber Agreement

- o Additional documentation required by VeriSign to satisfy its verification obligations under the Guidelines

## **(b) Role Requirements**

The following Applicant roles are required for the issuance of an EV Certificate

- o **Certificate Requester** – A Certificate Requester is a natural person who is employed and authorized by the Applicant, or an authorized agent who has express authority to represent the Applicant or a third party (such as an ISP or hosting company) that completes and submits an EV Certificate Request on behalf of the Applicant.
- o **Certificate Approver** – The EV Certificate Request MUST be approved by an authorized Certificate Approver. A Certificate Approver is a natural person who is employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve EV Certificate Requests submitted by other Certificate Requesters.

In the VTN a Certificate Approver is the equivalent of the Corporate for Retail certificates and a Managed PKI for SSL administrator for certificates obtained through VeriSign's Managed PKI for SSL accounts.

- o **Contract Signer** – A Subscriber Agreement applicable to the requested EV Certificate MUST be signed by an authorized Contract Signer. A Contract Signer is a natural person who is employed by the Applicant, or an authorized agent who has express authority to represent the Applicant who has authority on behalf of the Applicant to sign Subscriber Agreements on behalf of the Applicant.

Within the VTN, a Contract Signer is the equivalent of the Corporate Contact for Retail certificates and a Managed PKI for SSL Account Organization Contact for VeriSign's Managed PKI for SSL accounts.

One person MAY be authorized by the Applicant to fill one, two, or all three of these roles, provided that in all cases the Certificate Approver and Contract Signer must be an employee of Applicant. An Applicant MAY also authorize more than one person to fill each of these roles.

## **11. EV Certificate Request Requirements**

### **(a) General**

Prior to the issuance of an EV Certificate, the VeriSign obtains from the Applicant (via a Certificate Requester authorized to act on Applicant's behalf) a properly completed and signed EV Certificate Request that complies with these Guidelines.

### **(b) Request and Certification**

The EV Certificate Request contains a request from or on behalf of the Applicant for the issuance of an EV Certificate, and a certification by or on behalf of the Applicant that all of the information contained therein is true and correct.

### **(c) Information Requirements**

The EV Certificate Request MAY include all factual information about the Applicant to be included in the EV Certificate, and such additional information as is necessary for VeriSign to comply with these Guidelines and VeriSign's own policies. In cases where the EV Certificate Request does not contain all necessary information about the Applicant, VeriSign MUST

obtain the remaining information from either the Certificate Approver or Contract Signer, before it can process the EV Certificate request.

Before issuing an EV Certificate VeriSign must obtain the following information:

- . Organization Name: Applicant's formal legal organization name to be included in EV Certificate, as recorded with the Incorporating Agency in Applicant's Jurisdiction of Incorporation (for Private Organizations), or as specified in the law of Applicant's Jurisdiction of Incorporation (for Government Entities);
- . Assumed Name (Optional): Applicant's assumed name (e.g., d/b/a name) to be included in the EV Certificate, as recorded in the jurisdiction of Applicant's Place of Business, if applicable;
- . Domain Name: Applicant's fully qualified domain name to be included in the EV Certificate;
- . Jurisdiction of Incorporation: Applicant's Jurisdiction of Incorporation to be included in EV Certificate, and consisting of:
  - (a) City or town (if any),
  - (b) State or province (if any), and
  - (c) Country.
- . Incorporating Agency: The name of the Applicant's Incorporating Agency;
- . Registration Number: The unique registration number assigned to Applicant by the Incorporating Agency in Applicant's Jurisdiction of Incorporation and to be included in EV Certificate (for Private Organization Applicants only).
- . Applicant Address: The address of Applicant's Place of Business, including –
  - (a) Building number and street,
  - (b) City or town,
  - (c) State or province (if any),
  - (d) Country,
  - (e) Postal code (zip code), and
  - (f) Main telephone number.
- . Certificate Approver: Name and contact information of the Certificate Approver submitting and signing, or that has authorized the Certificate Requester to submit and sign, the EV Certificate Application on behalf of the Applicant; and
- . Certificate Requester: Name and contact information of the Certificate Requester submitting the EV Certificate Request on behalf of the Applicant, if other than the Certificate Approver.

## **12. Subscriber Agreement Requirements**

### **(a) General**

Prior to the issuance of the EV Certificate, VeriSign obtains the Applicant's agreement to a legally enforceable Subscriber Agreement for the express benefit of Relying Parties and Application Software Vendors. The Subscriber Agreement must be signed by an authorized Contract Signer acting on behalf of the Applicant, and must apply to the EV Certificate to be issued pursuant to the EV Certificate Request. A separate Subscriber Agreement may be used for each EV Certificate Request for retail certificates, or a single Subscriber Agreement may be used to cover multiple future EV Certificate Requests and resulting EV Certificates for managed PKI for SSL accounts.

## **(b) Agreement Requirements**

The Applicant's agreement to the Subscriber Agreement shall, at a minimum, specifically name both the Applicant and the individual Contract Signer signing the Agreement on the Applicant's behalf. The Subscriber Agreement shall contain, among other things, provisions imposing on the Applicant the following obligations and warranties:

- Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to VeriSign, both in the EV Certificate Request and as otherwise requested by VeriSign in connection with the issuance of the EV Certificate(s) to be supplied by VeriSign;
- Protection of Private Key: An obligation and warranty by the subscriber or a subcontractor (e.g. hosting provider) to take all reasonable measures necessary to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested EV Certificate(s) (and any associated access information or device – e.g., password or token);
- Acceptance of EV Certificate: An obligation and warranty that it will not install and use the EV Certificate(s) until it has reviewed and verified the accuracy of the data in each EV Certificate;
- Use of EV Certificate: An obligation and warranty to install the EV Certificate only on the server accessible at the domain name listed on the EV Certificate, and to use the EV Certificate solely in compliance with all applicable laws, solely for authorized company business, and solely in accordance with the Subscriber Agreement;
- Reporting and Revocation Upon Compromise: An obligation and warranty to promptly cease using an EV Certificate and its associated Private Key, and promptly request VeriSign to revoke the EV Certificate, in the event that: (a) any information in the EV Certificate is or becomes incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key listed in the EV Certificate;
- Termination of Use of EV Certificate: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key listed in an EV Certificate upon expiration or revocation of that EV Certificate.

## **F. INFORMATION VERIFICATION REQUIREMENTS**

### ***13. General Overview***

This part of VeriSign's procedures for issuing EV Certificates sets forth the Verification Requirements required in the Guidelines and the procedures used by VeriSign to satisfy the requirements.

Before issuing an EV Certificate, VeriSign ensures that all Subject organization information in the EV Certificate conforms to the requirements of, and has been verified in accordance with, the Guidelines and matches the information confirmed and documented by VeriSign pursuant to its verification processes.

### ***14. Verification of Applicant's Legal Existence and Identity***

To verify Applicant's legal existence and identity, VeriSign verifies that the Applicant is a legally recognized entity, in existence and validly formed (e.g., incorporated) directly with the

Incorporating Agency in Applicant's Jurisdiction of Incorporation, and that it is "active," "valid," "current," or the equivalent.

VeriSign verifies that the Applicant's formal legal name as recorded with the Incorporating Agency in Applicant's Jurisdiction of Incorporation matches Applicant's name in the EV Certificate Request.

VeriSign obtains and records the specific unique Registration Number assigned to Applicant by the Incorporating Agency in the Applicant's Jurisdiction of Incorporation.

VeriSign will further obtain and record the identity and address of the Applicant's Registered Agent or Registered Office (as applicable) in the Applicant's Jurisdiction of Incorporation.

### **15. Verification of Applicant's Legal Existence and Identity – Assumed Name**

If, in addition to the Applicant's formal legal name as recorded with the Incorporating Agency in Applicant's Jurisdiction of Incorporation, Applicant's identity as asserted in the EV Certificate is to contain any assumed name or "d/b/a" name under which Applicant conducts business, VeriSign will verify, through use of a Qualified Government Information Source operated by or on behalf of such government agency, or by direct contact with such government agency, that: (i) the Applicant has registered its use of the assumed name or "d/b/a" name with the appropriate state, or local government agency for such filings in the jurisdiction of its Place of Business (as verified in accordance with these Guidelines), and (ii) that such filing continues to be valid.

Alternatively, VeriSign may verify the assumed name through use of a Qualified Independent Information Source provided that the QIIS has verified the assumed name with the appropriate government agency, or by relying on a Verified Legal Opinion, or a Verified Accountant's Opinion that indicates the assumed name under which Applicant conducts business, the government agency such assumed name is registered with, and that such filing continues to be valid

### **16. Verification of Applicant's Physical Existence**

#### **(a) Address of Applicant's Place of Business**

To verify Applicant's physical existence and business presence, the VeriSign verifies that the physical address provided by Applicant is an address where Applicant conducts business operations (e.g., not a mail drop or P.O. Box), and is the address of Applicant's Place of Business.

The primary method VeriSign uses to obtain such verification is by requiring the Applicant to obtain a verified legal opinion or a Verified Accountant's Opinion letter attesting to this fact.

In the absence of a verified legal opinion, VeriSign may verify the address independently following the below procedure.

(A) For Applicants whose Place of Business is in the same country as the Applicant's Jurisdiction of Incorporation:

- (1) For Applicants listed at the same Place of Business address in the current version of at least one (1) Qualified Independent Information Source, the VeriSign confirms that the Applicant's address as listed in the EV Certificate Request is a valid business address for Applicant by reference to such Qualified Independent Information Sources, and may rely on Applicant's representation that such address is its Place of Business;

- (2) For Applicants who are not listed at the same Place of Business address in the current version of at least one (1) Qualified Independent Information Source, the VeriSign may confirm that the is in fact Applicant's business address by obtaining documentation of a site visit to the business address. When used, the site visit will be performed by a reliable individual or firm. The documentation of the site visit will:
- (a) Verify that the Applicant's business is located at the exact address stated in the EV Certificate Request (e.g., via permanent signage, employee confirmation, etc.);
  - (b) Identify the type of facility (e.g., office in a commercial building, private residence, storefront, etc.) and whether it appears to be a permanent business location;
  - (c) Indicate whether there is a permanent sign (that cannot be moved) that identifies the Applicant
  - (d) Indicate whether there is evidence that Applicant is conducting ongoing business activities at the site (e.g., that it is not just a mail drop, P.O. box, etc.), and
  - (e) Include one or more photos of (i) the exterior of the site (showing signage indicating the Applicant's name, if present, and showing the street address if possible), and (ii) the interior reception area or workspace.
- (B) For Applicants whose Place of Business is not in the same country as the Applicant's Jurisdiction of Incorporation, VeriSign requires a Verified Legal Opinion that indicates the address of Applicant's Place of Business and that business operations are conducted there.

### **(b) Telephone Number for Applicant's Place of Business**

To further verify Applicant's physical existence and business presence, as well as to assist in confirming other verification requirements, VeriSign verifies a telephone number that is a main phone number for Applicant's Place of Business.

VeriSign may require a verified legal opinion, or a Verified Accountant's Opinion attesting to the telephone number.

In the absence of a verified legal opinion, VeriSign may verify Applicant's telephone number by:

- (A) Confirming the telephone number is listed as the Applicant's telephone number for the verified address of its Place of Business in records provided by the applicable phone company or alternatively in at least one (1) Qualified Independent Information Source; or
- (B) During a site visit, the person who is conducting the site visit **MUST** confirm the Applicant's main telephone number by calling it and obtaining an affirmative response sufficient to enable a reasonable person to conclude that the Applicant is reachable by telephone at the number dialed.

During the telephone verification process detailed in Section 21 below VeriSign shall call this number and obtain an affirmative response sufficient to enable a reasonable person to conclude that the Applicant is reachable by telephone at the number dialed.

## **17. Verification of Applicant's Operational Existence**

Verification Requirements. If the records of the incorporating agency indicates that the Applicant has been in existence for less than three (3) years, and the applicant's address cannot be verified

using the records of the incorporating agency, or other Qualified Independent Information Source, VeriSign verifies that the Applicant has the ability to engage in business.

The primary method VeriSign uses to verify operational existence is by requiring the Applicant to obtain a verified legal opinion letter, or a Verified Accountant's Opinion attesting to the fact that the Applicant has an active current Demand Deposit Account with a regulated financial institution.

In the absence of a verified legal opinion, VeriSign may verify the Applicant's operational existence by performing one of the following:

- (1) A successfully completed site visit, or
- (2) Verify the Applicant has an active current Demand Deposit Account with a regulated financial institution, by receiving authenticated documentation directly from a regulated financial institution verifying that the Applicant has an active current Demand Deposit Account with the institution.

### **18. Verification of Applicant's Domain Name**

VeriSign verifies Applicant's registration of the domain name(s) to be listed in the EV Certificate, satisfy the following requirements:

- (1) The domain name is registered with an Internet Corporation for Assigned Names and Numbers (ICANN)-approved registrar or a registry listed by the Internet Assigned Numbers Authority (IANA);
- (2) Domain registration information in the WHOIS database SHOULD be public and SHOULD show the name, physical address, and administrative contact information for the organization.
- (3) The Applicant is the registered holder of the domain name or has been granted the exclusive right to use the domain name by the registered holder of the domain name
- (4) The Applicant is aware of its registration or exclusive control of the domain name;

VeriSign performs a WHOIS inquiry on the Internet for the domain name supplied by the Applicant, to verify that the Applicant is the entity to whom the domain name is registered. Where the WHOIS record indicates otherwise, VeriSign will require the WHOIS record to be updated to reflect the Applicant as the registered holder of the domain.

In cases where Applicant is not the registered holder of the domain name, or domain registration information cannot be obtained from WHOIS, VeriSign may obtain positive confirmation from the registered domain holder that the applicant has been granted the exclusive right to use the requested Fully Qualified Domain Name (FQDN). In these circumstances, VeriSign also verifies the Applicant's exclusive right to use the domain name using one of the following methods:

- (A) Relying on a Verified Legal Opinion to the effect that the Applicant has the exclusive right to use the specified domain name in identifying itself on the Internet; or
- (B) Relying on a representation from the Contract Signer, or the Certificate Approver if expressly authorized in a mutually agreed upon contract, coupled with a practical demonstration by the Applicant establishing that it controls the confirmed domain name by making an agreed-upon change in information found online on a web page identified by a uniform resource identifier containing the Applicant's FQDN.

In cases where the registered domain holder cannot be contacted, VeriSign shall:

- Rely on a Verified Legal Opinion to the effect that the Applicant has the exclusive right to use the specified domain name in identifying itself on the Internet, **and**
- Rely on a representation from the Contract Signer, or the Certificate Approver if expressly authorized in a mutually agreed upon contract, coupled with a practical demonstration by the Applicant establishing that it controls the confirmed domain name by making an agreed-upon change in information found online on a web page identified by a uniform resource identifier containing the Applicant's FQDN;

The primary method VeriSign uses to verify the Applicant is aware that it has exclusive control and/or ownership of the domain name is by requiring the Applicant to obtain a verified legal opinion letter attesting to this fact.

In the absence of a verified legal opinion, VeriSign may verify the Applicant is aware that it has exclusive control and/or ownership of the domain name by obtaining a Confirmation from Corporate Contact verifying that the Applicant is aware that it has exclusive control of the domain name.

### **19. Verification of Name, Title, and Authority of Contract Signer and Certificate Approver**

For both the Contract Signer and the Certificate Approver, the VeriSign verifies the following:

- (1) Name, Title and Agency. VeriSign verifies the name and title of the Contract Signer and the Certificate Approver, as applicable, as well as the fact that they are agents representing the Applicant.
- (2) Authorization of Contract Signer. VeriSign verifies, through a source other than the Contract Signer, that the Contract Signer is expressly authorized by the Applicant to enter into the Subscriber Agreement (and any other relevant contractual obligations) on behalf of the Applicant, including a contract that designates one or more Certificate Approvers on behalf of Applicant ("Signing Authority").
- (3) Authorization of Certificate Approver. VeriSign verifies, through a source other than the Certificate Approver, that the Certificate Approver is expressly authorized by the Applicant to do the following, as of the date of the EV Certificate Request:
  - (a) Submit, and if applicable authorize a Certificate Requester to submit, the EV Certificate Request on behalf of the Applicant; and
  - (b) Provide, and if applicable authorize a Certificate Requester to provide, the information requested from the Applicant by VeriSign for issuance of the EV Certificate; and
  - (c) Approve EV Certificate Requests submitted by a Certificate Requester

Where the Contract Signer and Certificate Approver are the same person then the authorization of the Contract Signer shall include authorization as Certificate Approver.

The primary method VeriSign uses to verify the name, title, and authorization of the Contract Signer is to obtain a verified legal opinion letter or a Verified Accountant's Opinion letter attesting to these facts.

In cases where a Certificate Approver is a different person from the Contract Signer VeriSign verifies the name, title, agency status (as appropriate) and authorization of the Certificate Approver with the authorized Contract Signer.

In the absence of a verified legal opinion, VeriSign may verify agency of the Certificate Approver and/or employment of the Contract Signer by:

- (A) Contacting the Applicant's Human Resources Department by phone or mail (at the phone number or address for Applicant's Place of Business, verified in accordance with these Guidelines) and obtaining confirmation that the Contract Signer and/or the Certificate Approver, as applicable, is an employee; or
- (B) Obtaining an Independent Confirmation From Applicant verifying that the Contract Signer and/or the Certificate Approver, as applicable, is either an employee or has been otherwise been appointed as an agent of Applicant.

In the absence of a verified legal opinion or a Verified Accountant's Opinion, VeriSign may verify the Authority of the Contract Signer by using one of the following methods:

- (1) **Corporate Resolution:** The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, may be verified by reliance on a properly authenticated corporate resolution that confirms that the person has been granted such Signing Authority, provided that such resolution is (1) certified by the appropriate corporate officer (e.g., secretary), and (2) VeriSign can reliably verify that the certification was validly signed by such person, and that such person does have the requisite authority to provide such certification.
- (2) **Independent Confirmation from Applicant:** The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, may be verified by obtaining an Independent Confirmation from Applicant.
- (3) **Contract between CA and Applicant:** The EV Authority of the Certificate Approver may be verified by reliance on a contract between VeriSign and the Applicant that designates the Certificate Approver with such EV Authority, provided the contract is signed by the Contract Signer and provided that the agency and Signing Authority of the Contract Signer has been verified.
- (4) **Pre-Authorized Certificate Approver.** Where VeriSign and the Applicant contemplate the submission of multiple future EV Certificate Requests, for example in relation to Managed PKI for SSL accounts, then, after VeriSign:
  - o Has verified the name and title of the Contract Signer and that he/she is an employee or agent of the Applicant, and
  - o Has verified the Signing Authority of such Contract Signer in accordance with one of the procedures in this Section 19;

the Applicant may agree in writing, signed by the Contract Signer on behalf of the Applicant, to expressly authorize one or more designated Certificate Approver(s) to exercise EV Authority with respect to each future EV Certificate Application submitted on behalf of the Applicant and properly authenticated as originating with, or otherwise being approved by, such Certificate Approver(s).

In these circumstances the Applicant shall be obligated under the Subscriber Agreement for all EV Certificates issued at the request of, or approved by, such Certificate Approver(s) until such EV Authority is revoked, and MUST include mutually agreed-upon provisions for (i) authenticating the Certificate Approver when EV Certificate Requests are approved, (ii) periodic re-confirmation of the EV Authority of the Certificate Approver, (iii) secure procedure by which the Applicant can notify VeriSign that the EV Authority of any such Certificate Approver is revoked, and (iv) such other appropriate precautions as are reasonably necessary.

## **20. Verification of Signature on Subscriber Agreement and EV Certificate Requests**

For retail EV SSL certificates, The Subscriber Agreement for each EV Certificate Request MUST be signed by an authorized Contract Signer on behalf of the applicant. If the Certificate requester is not also an authorized Certificate Approver, or an Authorized Contract Signer, an authorized Certificate Approver or Contract Signer MUST independently approve the EV Certificate Request. In all cases, the signature MUST be a legally valid and enforceable seal or handwritten signature (for a paper Subscriber Agreement and/or EV Certificate Request), or a legally valid and enforceable electronic signature (for an electronic Subscriber Agreement and/or EV Certificate Request), that binds the Applicant to the terms of each respective document.

### **(a) Verification Requirements**

Before issuing a retail EV SSL certificate, VeriSign authenticates the signature of the Contract Signer on the Subscriber Agreement on each request by contacting the Contract Signer directly using a verified telephone number for the Applicant, and asking to speak to the Contract Signer, followed by a response from someone who identifies themselves as such person confirming that he/she did sign the applicable document on behalf of the Applicant, or by using a manner that makes it reasonably certain that the person named as the signer in the applicable document is, in fact, the person who signed the document on behalf of the Applicant.

Before approving a Managed PKI for SSL account to approve EV SSL certificates from its Requestors, VeriSign authenticates the signature of the Contract Signer/Corporate Contact for that account on the Subscriber Agreement by contacting the authorized Contract Signer directly using a verified telephone number for the Applicant, and asking to speak to the Contract Signer, followed by a response from someone who identifies themselves as such person confirming that he/she did sign the applicable document on behalf of the Applicant. Thereafter, any certificate approver authorized by the applicant in terms of these EV procedures, will be able to approve certificate requests in compliance with these procedures and the Guidelines without an additional signature from the Contract Signer.

Before adding an EV domain to a Managed PKI for SSL account VeriSign shall confirm directly with the Applicant, or the Certificate Signer, that the Applicant has knowledge of the domain.

In the absence of a telephone call as described above VeriSign may use one of the alternative methods of authenticating the signature of the Contract Signer:

- (1) A letter mailed to the Applicant's or Registered Agent's address, as verified through independent means in accordance with these Guidelines, c/o of the Certificate Requester or Contract Signer, as applicable, followed by a phone or mail response from someone who identifies themselves as such person confirming that he/she did sign the applicable document on behalf of the Applicant.
- (2) Use of a signature process that establishes the name and title of the signer in a secure manner, such as through use of an appropriately secure login process that identifies the signer before signing, or through use of a digital signature made with reference to an appropriately verified certificate.
- (3) Notarization by a notary, provided that VeriSign independently verifies that such notary is a legally qualified notary in the jurisdiction of the Certificate Requester or Contract Signer.

## **21. Verification of Approval of EV Certificate Request**

Before VeriSign may issue the requested EV Certificate, VeriSign verifies that an authorized Certificate Approver reviewed and approved the EV Certificate Request. VeriSign verifies this for retail EV SSL Certificates by contacting the Certificate Approver by phone or mail (at a verified phone number or address) and obtaining oral or written confirmation that the Certificate Approver has reviewed and approved the EV Certificate Request.

In the case of EV certificates issued through a Managed PKI for SSL account that has been verified for EV, verification of approval is obtained by the use of a valid Digital Certificate issued to a Certificate Approver (Managed PKI for SSL administrator) to login to the Applicant's account, together with an indication of approval from the Certificate Approver of the certificate request.

## **22. Verification of Certain Information Sources**

### **(a) Verified Legal Opinion**

- (1) Verification Requirements. Before relying on any legal opinion, VeriSign verifies that such legal opinion meets the following requirements ("Verified Legal Opinion"):
  - (A) Status of Author. VeriSign verifies that the legal opinion is authored by a legal practitioner retained by and representing the Applicant (or an in-house legal practitioner employed by the Applicant) (Legal Practitioner) who is either:
    - (i) A lawyer (or solicitor, barrister, advocate, or equivalent) licensed to practice law in the Applicant's Jurisdiction of Incorporation or any jurisdiction where the Applicant maintains an office or physical facility. VeriSign verifies the professional status of the author of the legal opinion by directly contacting the authority responsible for registering or licensing such Legal Practitioner(s) in the applicable jurisdiction; or
    - (ii) A notary that is a member of the International Union of Latin Notaries, and is licensed to practice in the country of Applicant's Jurisdiction of Incorporation or any jurisdiction where the Applicant maintains an office or physical facility (and that such jurisdiction recognizes the role of the Latin Notary).
  - (B) Basis of Opinion. VeriSign verifies that the Legal Practitioner is acting on behalf of the Applicant and that the conclusions of the Verified Legal Opinion are based on the Legal Practitioner's stated familiarity with the relevant facts and the exercise of the Legal Practitioner's professional judgment and expertise.
  - (C) Authenticity. VeriSign confirms the authenticity of the Verified Legal Opinion by calling or sending a copy of the legal opinion back to the Legal Practitioner at the address, phone number, facsimile, or (if available) e-mail address for the Legal Practitioner listed with the authority responsible for registering or licensing such Legal Practitioner and obtaining confirmation from the Legal Practitioner or the Legal Practitioner's assistant that the legal opinion is authentic.

### **(b) Verified Accountant Opinion Letter**

- (1) Verification Requirements. Before relying on any accountant letter submitted VeriSign verifies that such accountant letter meets the following requirements ("Verified Accountant Letter"):
  - (A) Status of Author. VeriSign shall directly contact the authority responsible for registering or licensing such Accounting Practitioner (s) in the applicable jurisdiction to establish that the accountant letter is authored by an independent professional accountant, who is a certified public accountant, chartered accountant, or equivalent licensed by a full member of the International Federation of Accountants (IFAC) to practice accounting in the country of the

Applicant's Jurisdiction of Incorporation or any jurisdiction where the Applicant maintains an office or physical facility.

- (B) Basis of Opinion. The Accounting Practitioner is acting on behalf of the Applicant and that the conclusions of the Verified Accountant Letter are based on the Accounting Practitioner's stated familiarity with the relevant facts and the exercise of the Accounting Practitioner's professional judgment and expertise.
- (C) Authenticity. To confirm the authenticity of the accountant's opinion, the VeriSign will call or send a copy of the accountant letter back to the Accounting Practitioner at the address, phone number, facsimile, or (if available) e-mail address for the Accounting Practitioner listed with the authority responsible for registering or licensing such Accounting Practitioners and obtain confirmation from the Accounting Practitioner or the Accounting Practitioner's assistant that the accountant letter is authentic.

### **(c) Independent Confirmation from Applicant**

An "Independent Confirmation From Applicant" is a confirmation of a particular fact (e.g., knowledge of its exclusive control of a domain name, confirmation of the employee or agency status of a Contract Signer or Certificate Approver, confirmation of the EV Authority of a Certificate Approver, etc.) that is:

- (i) Received by VeriSign from a person employed by the Applicant (other than the person who is the subject of the inquiry) that has the appropriate authority to confirm such a fact ("Confirming Person"), and who represents that he/she has confirmed such fact;
- (ii) Received by VeriSign in a manner that authenticates and verifies the source of the confirmation; and
- (iii) Binding on the Applicant.

An Independent Confirmation from Applicant may be obtained via the following procedure:

- (1) Confirmation Request: VeriSign will initiate an appropriate out-of-band communication requesting verification or confirmation of the particular fact in issue ("Confirmation Request") as follows:
  - (A) Addressee: The Confirmation Request MUST be directed to:
    - (i) A position within Applicant's organization that qualifies as a Confirming Person (e.g., Secretary, President, CEO, CFO, COO, CIO, CSO, Director, etc.) and is identified by name and title in a current Qualified Government Information Source (e.g., an SEC filing) or a Qualified Independent Information Source, a Verified Legal Opinion, or a Verified Accountant's Opinion; or
    - (ii) Applicant's Registered Agent or Registered Office in the Jurisdiction of Incorporation as listed in the official records of the Incorporating Agency, with instructions that it be forwarded to an appropriate Confirming Person.
  - (B) Means of Communication: The Confirmation Request MUST be directed to the Confirming Person in a manner reasonably likely to reach such person. The following options are acceptable:
    - (i) By paper mail, addressed to the Confirming Person at:
      - (a) The address of Applicant's Place of Business as verified by VeriSign in accordance with these procedures; or

- (b) The business address for such Confirming Person specified in a current government-operated Qualified Information Source (e.g., an SEC filing), a Qualified Independent Information Source, a Verified Legal Opinion, or a Verified Accountant's Opinion; or
  - (c) The address of Applicant's Registered Agent or Registered Office listed in the official records of the Jurisdiction of Incorporation.
  - (ii) By e-mail addressed to the Confirming Person at the business e-mail address for such person listed in a current Qualified Government Information Source or a Qualified Independent Information Source, a Verified Legal Opinion, or a Verified Accountant's Opinion; or
  - (iii) By telephone call to the Confirming Person, where such person is contacted by calling the main phone number of Applicant's Place of Business (verified in accordance with these Guidelines) and asking to speak to such person, and a person taking the call identifies himself as such person; or
  - (iv) By facsimile to the Confirming Person at the Place of Business. The facsimile number must be listed in a current Qualified Government Information Source or a Qualified Independent Information Source, a Verified Legal Opinion, or a Verified Accountant's Opinion. The cover page must be clearly addressed to the Confirming Person.
- (2) Confirmation Response: VeriSign must receive a response to the Confirmation Request from a Confirming Person that confirms the particular fact in issue. Such response may be provided by telephone, by e-mail, or by paper mail, so long as VeriSign can reliably verify that it was provided by a Confirming Person in response to the Confirmation Request.

**(d) Qualified Independent Information Sources (QIIS)**

Commercial Information Sources used by VeriSign for verifying EV certificate application information meet the databases requirements required by the Guidelines.

**(e) Qualified Government Information Source (QGIS)**

Government Information Sources used by VeriSign for verifying EV certificate application information meet the databases requirements required by the Guidelines.

**23. Other Verification Requirements**

**(a) High Risk Status**

VeriSign takes reasonable steps to identify Applicants that are likely to be at a high risk e.g., if they may possibly be targeted for fraudulent attacks ("High Risk Applicants"), and conducts such additional verification activity and takes such additional precautions as are reasonably necessary to ensure that such Applicants are properly verified under these Guidelines.

VeriSign maintains an internal database that includes previously revoked SSL certificates, including EV Certificates and previously rejected EV Certificate Requests, due to suspected phishing or other fraudulent usage. This information is used to flag suspicious new EV Certificate Requests. If an Applicant is flagged as a High Risk Applicant, VeriSign performs reasonably appropriate additional authentication and verification to be certain beyond reasonable doubt that the Applicant and the target in question are the same organization.

**(b) Denied Lists and Other Legal Black Lists**

VeriSign will not issue any EV Certificate to the Applicant, without first taking appropriate steps for obtaining clearance from the relevant government agency, if either the Applicant, the Contract

Signer, or Certificate Approver or if the Applicant's Jurisdiction of Incorporation or Place of Business is:

- (a) Identified on any government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under the laws of the country of VeriSign's jurisdiction(s) of operation; and
- (b) Has its Jurisdiction of Incorporation or Place of Business in any country with which the laws of VeriSign's jurisdiction prohibit doing business

VeriSign takes reasonable steps to verify EV Certificate applications with the following lists and regulations:

- (A) VeriSign takes reasonable steps to verify with the following US Government Denied lists and regulations:
- (B) BIS Denied Persons List
- (C) BIS Denied Entities List
- (D) US Treasury Department List of Specially Designated Nationals and Blocked Persons
- (E) US Government export regulations

## ***24. Final Cross-Correlation and Due Diligence***

VeriSign requires that after all of the verification processes and procedures are completed, an EV verification specialist who is not responsible for the collection of information reviews that VeriSign has performed all verification steps. That person may also be responsible for placing the final verification call to the Contract Signer and, if successful, issue the certificate.

This is not required of Managed PKI for SSL customers.

## ***25. Certificate Renewal Verification Requirements.***

Before renewing an EV Certificate, VeriSign performs all authentication and verification tasks required by the Guidelines and this procedure to ensure that the renewal request is properly authorized by the Applicant and that the information displayed in the EV Certificate is still accurate and valid.

## **G. CERTIFICATE STATUS CHECKING AND REVOCATION ISSUES**

### ***26. EV Certificate Status Checking.***

VeriSign maintains an online 24/7 Repository mechanism whereby Internet browsers can automatically check online the current status of all certificates.

- (1) For EV Certificates:
  - (A) CRLs are updated and reissued at least every seven (7) days, and with a maximum expiration time of ten (10) days; or
  - (B) VeriSign's Online Certificate Status Protocol (OCSP) is updated at least every four (4) days, and with a maximum expiration time of ten (10) days.
- (2) For VeriSign's subordinate CA Certificate for EV:
  - (A) CRLs. Are updated and reissued at least every twelve (12) months, and with a maximum expiration time of twelve (12) months; or
  - (B) OCSP. If used, VeriSign's OCSP for CA Certificates for EV will be updated at least every twelve (12) months, and with a maximum expiration time of twelve (12) months.

VeriSign operates and maintains its CRL and/or OCSP capability with resources sufficient to provide a commercially reasonable response time for the number of queries generated by all of the EV Certificates issued by it.

Revocation entries on a CRL or OCSP are not removed until after the expiration date of the revoked EV Certificate.

### **27. EV Certificate Revocation.**

In addition to any revocation circumstances listed in section 4.9.1 of this CPS, VeriSign will revoke an EV Certificate it has issued upon the occurrence of any of the following events:

- (1) The Subscriber requests revocation of its EV Certificate;
- (2) The Subscriber indicates that the original EV Certificate Request was not authorized and does not retroactively grant authorization;
- (3) VeriSign obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the EV Certificate) has been compromised, or that the EV Certificate has otherwise been misused;
- (4) VeriSign receives notice or otherwise becomes aware that a Subscriber violates any of its material obligations under the Subscriber Agreement;
- (5) VeriSign receives notice or otherwise becomes aware that a court or arbitrator has revoked a Subscriber's right to use the domain name listed in the EV Certificate, or that the Subscriber has failed to renew its domain name;
- (6) VeriSign receives notice or otherwise becomes aware of a material change in the information contained in the EV Certificate;
- (7) A determination, in VeriSign's sole discretion, that the EV Certificate was not issued in accordance with the terms and conditions of these Guidelines or VeriSign's EV Policies;
- (8) If VeriSign determines that any of the information appearing in the EV Certificate is not accurate.
- (9) VeriSign ceases operations for any reason and has not arranged for another EV CA to provide revocation support for the EV Certificate;
- (10) VeriSign's right to issue EV Certificates under these Guidelines expires or is revoked or terminated [*unless VeriSign makes arrangements to continue maintaining the CRL/OCSP Repository*];
- (11) VeriSign's Private Key for its EV issuing CA Certificate has been compromised;
- (13) VeriSign receives notice or otherwise become aware that a Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of VeriSign's jurisdiction of operation.

### **28. EV Certificate Problem Reporting and Response Capability.**

VeriSign provides Subscribers, Relying Parties, Application Software Vendors, and other third parties with an online form to report complaints or suspected Private Key compromise, EV Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to EV Certificates ("Certificate Problem Reports"), and a 24x7 capability to accept and acknowledge such Reports, at: <https://www.verisign.com/support/ssl-support/ev-misuse/index.html>

VeriSign will begin investigation of all Certificate Problem Reports within twenty-four (24) business hours and decide whether revocation or other appropriate action is warranted based on at least the following criteria:

- (i) The nature of the alleged problem;
- (ii) Number of Certificate Problem Reports received about a particular EV Certificate or website;
- (iii) The identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered); and
- (iv) Relevant legislation in force.

VeriSign takes reasonable steps to provide continuous 24/7 ability to internally respond to any high priority Certificate Problem Report, and where appropriate, forward such complaints to law enforcement and/or revoke an EV Certificate that is the subject of such a complaint.

## **H. EMPLOYEE AND THIRD PARTY ISSUES**

### ***29. Trustworthiness and Competence***

In addition to the procedures described in Sections 5.2 and 5.3 of Verisign's CPS, any person employed by VeriSign for engagement in the EV Certificate process, whether as an employee, agent, or an independent contractor, is subject to following additional procedures:

- (A) The personal (physical) presence of such person before trusted persons including Notary publics, or persons who perform human resource or security functions, and
- (B) The verification of well-recognized forms of government-issued photo identification (e.g., passports and/or driver's licenses).

VeriSign requires all Validation Specialists to pass an internal examination on the EV Certificate validation criteria outlined in these Guidelines.

### ***30. Delegation of Functions to Registration Authorities and Subcontractors***

VeriSign may delegate the performance of all or any part of a requirement of these procedures and the Guidelines to a registration agent (RA) or subcontractor, except for the performance of the Final Cross-Correlation and Due Diligence requirements of Section 24 of these Guidelines.

VeriSign MAY contractually authorize its Managed PKI for SSL customers for EV Certificates to perform the approval function and authorize VeriSign to issue EV Certificates at third and higher domain levels that contain domain(s) and Organization names that have been verified by VeriSign in terms of these procedures and the Guidelines. In such case, the Subject shall be considered an Enterprise RA, and the following shall apply:

- (i) No Enterprise RA MAY authorize VeriSign to issue an Enterprise EV Certificate for a domain not previously verified by VeriSign in terms of these EV procedures as belonging to a business that is owned or directly controlled by the Enterprise RA;
- (ii) In all cases, the Subject of an Enterprise EV Certificate MUST be an organization verified by VeriSign in accordance with these Guidelines;
- (iii) VeriSign MUST impose these limitations as a contractual requirement with the Enterprise RA and monitor compliance by an authorized Managed PKI for SSL Customer Administrator;
- (iv) The Final Cross-Correlation and Due Diligence requirements of Section 24 of these Guidelines MAY be performed by the Enterprise RA; and

(v) VeriSign contractually obligates each such RA, subcontractor, and Enterprise RA to comply with all applicable requirements in the Guidelines and these procedures and to perform them as required of VeriSign itself. VeriSign shall enforce compliance with such terms.

## **I. DATA AND RECORD ISSUES**

### **31. Documentation and Audit Trail Requirements**

- (a) VeriSign records every action taken to process an EV Certificate Request and to issue an EV Certificate, including all information generated or received in connection with an EV Certificate Request, and every action taken to process the Request, including time, date, and personnel involved in the action. These records are available as auditable proof of VeriSign's practices. This also applies to all registration agents (RAs) and subcontractors as well.
- (b) The foregoing record requirements include, but are not limited to, an obligation to record the following events:
  - (i) CA key lifecycle management events, including:
    - (a) Key generation, backup, storage, recovery, archival, and destruction; and
    - (b) Cryptographic device lifecycle management events
  - (ii) CA and Subscriber EV Certificate lifecycle management events, including:
    - (a) EV Certificate Requests, renewal and re-key requests, and revocation;
    - (b) All verification activities required by these Guidelines
    - (c) Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
    - (d) Acceptance and rejection of EV Certificate Requests;
    - (e) Issuance of EV Certificates; and
    - (f) Generation of EV Certificate revocation lists (CRLs); and OCSP entries
  - (iii) Security events, including:
    - (a) Successful and unsuccessful PKI system access attempts;
    - (b) PKI and security system actions performed;
    - (c) Security profile changes;
    - (d) System crashes, hardware failures, and other anomalies;
    - (e) Firewall and router activities; and
    - (f) Entries to and exits from CA facility
  - (iv) Log entries MUST include the following elements:
    - (a) Date and time of entry;
    - (b) Identity of the persona and entity making the journal entry; and
    - (c) Description of entry

### **32. Document Retention**

#### **(a) Audit Log Retention**

Audit logs for EV Certificates are made available to independent auditors upon request. Audit logs are retained for at least seven (7) years.

#### **(b) Retention of Documentation**

VeriSign retains all documentation relating to all EV Certificate Requests and verification thereof, and all EV Certificates and revocation thereof, for at least seven (7) year(s) after any EV Certificate based on that documentation ceases to be valid. VeriSign maintains current an

internal database of all previously revoked EV Certificates and previously rejected EV Certificate Requests due to suspected phishing or other fraudulent usage or concerns. Such information is flagged suspicious EV Certificate Requests.

### **33. Reuse and Updating Information and Documentation**

#### **(a) Use of Documentation to Support Multiple EV Certificates**

VeriSign may issue multiple EV Certificates listing the same Subject and based on a single EV Certificate Request, subject to the aging and updating requirement in (b) below.

#### **(b) Use of Pre-Existing Information or Documentation**

- (1) Each EV Certificate issued by VeriSign MUST be supported by a valid current EV Certificate Request and a Subscriber Agreement signed by the Applicant Representative on behalf of the Applicant.
- (2) The age of information used by VeriSign to verify such an EV Certificate Request MUST not exceed the Maximum Validity Period for such information set forth in these procedures and the Guidelines, based on the earlier of the date the information was obtained (e.g., the date of a confirmation phone call) or the date the information was last updated by the source (e.g., if an online database was accessed by VeriSign on July 1, but contained data last updated by the vendor on February 1, then the date of information would be considered to be February 1).
- (3) In the case of outdated information, the VeriSign repeats the verification processes required in these Guidelines.

### **34. Data Security**

Sections 5 and 6 of the VeriSign CPS describe VeriSigns Security Controls.

## **J. COMPLIANCE**

### **35. Audit Requirements**

#### **(a) Pre-Issuance Readiness Audit**

Before issuing EV Certificates VeriSign shall successfully complete a point-in-time readiness assessment audit against the WebTrust EV Program, or a point-in-time readiness assessment audit against equivalent audit procedures approved by the CA/Browser Forum.

#### **(b) Regular Self Audits**

During the period in which it issues EV Certificates, VeriSign will control its service quality by performing ongoing self audits against a randomly selected sample of at least three percent (3%) of the EV Certificates it has issued in the period beginning immediately after the last sample was taken.

#### **(c) Annual Independent Audit**

VeriSign undergoes an annual (i) WebTrust Program for CAs audit and (ii) WebTrust EV Program audit, or an equivalent for both (i) and (ii) as approved by the CA/Browser Forum. Such audits MUST cover all CA obligations under these Guidelines regardless of whether they are performed directly by VeriSign or delegated to an RA or subcontractor.

The audit report is made publicly available by VeriSign.

#### **(d) Auditor Qualifications**

All audits required under the Guidelines MUST be performed by a Qualified Auditor. A Qualified Auditor MUST:

- (1) Be an independent public accounting firm that has proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function and be currently licensed to perform WebTrust for CA audits and WebTrust EV Program audits, or to perform such alternate equivalent audits approved by the CA/Browser Forum as will be performed; and
- (2) Be a member of the American Institute of Certified Public Accountants (AICPA), or by a non-US equivalent that requires that audits be completed under defined standards that include 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; and
- (3) Maintain Professional Liability/Errors & Omissions insurance, with policy limits of at least \$1 million in coverage

#### **(e) Root Key Generation**

For CA root keys generated after the release of these Guidelines, VeriSign's Qualified Auditor may witness the root key generation ceremony in order to observe the process and the controls over the integrity and confidentiality of VeriSign root keys produced. The Qualified Auditor MUST then issue a report opining that VeriSign, during its root key and certificate generation process:

- o Documented its Root CA key generation and protection procedures in its Certificate Policy , version, date and its Certification Practices Statement , version, date (CP and CPS);
- o Included appropriate detailed procedures and controls in a documented plan of procedures to be performed for the generation of the root certification authority key pair (the "Root Key Generation Script") for the Root CA;
- o Maintained effective controls to provide reasonable assurance that the Root CA was generated and protected in conformity with the procedures described in its CP/CPS and with its Root Key Generation Script; and
- o Performed, during the root key generation process, all the procedures required by its Root Key Generation Script.
- o A video of the entire key generation ceremony will be recorded for auditing purposes.

### **K. OTHER CONTRACTUAL COMPLIANCE**

#### ***36. Privacy Issues***

VeriSign will comply with all applicable privacy laws and regulations, as well as its published privacy policy, in the collection, use and disclosure of non-public personal information as part of the EV Certificate vetting process.

#### ***37. Limitations on EV Certificate Liability***

##### **(a) CA Liability**

- (1) Subscribers and Relying Parties

In cases where VeriSign has issued and managed the EV Certificate in compliance with the Guidelines and its CPS, VeriSign shall not be liable to the EV Certificate Subscribers or Relying Parties or any other third parties for any losses suffered as a result of use or reliance on such EV Certificate. In cases where VeriSign has not issued or managed the EV Certificate in complete compliance with the Guidelines and this CPS, VeriSign's liability to the Subscriber for legally recognized and provable claims for losses or damages suffered as a result of the use or reliance on such EV Certificate shall be the greater of (a) the damages recoverable under the Netsure Protection plan or (b) \$2,000. VeriSign's liability to Relying Parties or any other third parties for legally recognized and provable claims for losses or damages suffered as a result of the use or reliance on such EV Certificate shall not exceed \$2,000.

(2) Indemnification of Application Software Vendors

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, VeriSign understands and acknowledges that the Application Software Vendors who have a root certificate distribution agreement in place with VeriSign do not assume any obligation or potential liability of VeriSign under these Guidelines or that otherwise might exist because of the issuance or maintenance of EV Certificates or reliance thereon by Relying Parties or others. VeriSign shall defend, indemnify, and hold harmless each Application Software Vendor for any and all claims, damages, and losses suffered by such Application Software Vendor related to an EV Certificate issued by VeriSign, regardless of the cause of action or legal theory involved. This shall not apply, however, to any claim, damages, or loss suffered by such Application Software Vendor related to an EV Certificate issued by VeriSign where such claim, damage, or loss was directly caused by such Application Software Vendor's software displaying as not trustworthy an EV Certificate that is still valid, or displaying as trustworthy: (1) an EV Certificate that has expired, or (2) an EV Certificate that has been revoked (but only in cases where the revocation status is currently available from VeriSign online, and the browser software either failed to check such status or ignored an indication of revoked status).

## Appendix B2

### Minimum Cryptographic Algorithm and Key Sizes for EV Certificates

#### 1. Root CA Certificates

	<b>Certificate issued on or before 31 Dec 2010</b>	<b>Certificate issued after 31 Dec 2010</b>
<b>Digest algorithm</b>	MD5 (NOT RECOMMENDED), SHA-1	SHA-1*, SHA-256, SHA-384 or SHA-512
<b>RSA</b>	1024 bit	2048 bit
<b>ECC</b>	224, 233, 256 or 283 bits	224, 233, 256 or 283 bits

#### 2. Subordinate CA Certificates

	<b>Certificate issued on or before 31 Dec 2010</b>	<b>Certificate issued after 31 Dec 2010</b>
<b>Digest algorithm</b>	SHA-1	SHA-1*, SHA-256, SHA-384 or SHA-512
<b>RSA</b>	1024 bit or 2048 bit	2048bit
<b>ECC</b>	224, 233, 256 or 283 bits	224, 233, 256 or 283 bits

#### 3. Subscriber Certificates

	<b>Certificate issued on or before 31 Dec 2010</b>	<b>Certificate issued after 31 Dec 2010</b>
<b>Digest algorithm</b>	SHA-1	SHA1*, SHA-256, SHA-384 or SHA-512
<b>RSA</b>	1024 bit or 2048 bit (Note: subscriber certificates containing a 1024 bit RSA key MUST expire on or before 31 Dec 2010)	2048 bit
<b>ECC</b>	224, 233, 256 or 283 bits	224, 233, 256 or 283 bits

\*SHA-1 should be used until SHA-256 is supported widely by browsers used by a majority of relying parties worldwide.

## Appendix B3

### EV Certificates Required Certificate Extensions

#### 1. Root CA Certificate

Root certificates generated after October 2006 MUST be X.509 v3.

##### (a) basicConstraints

If the certificate is v3 and is created after October 2006, this extension MUST appear as a critical extension in all CA certificates that contain Public Keys used to validate digital signatures on certificates. The CA field MUST be set true. The pathLenConstraint field SHOULD NOT be present.

##### (b) keyUsage

If the certificate is v3 and is created after October 2006, this extension MUST be present and MUST be marked critical. Bit positions for CertSign and cRLSign MUST be set. All other bit positions SHOULD NOT be set.

All other fields and extensions set in accordance to RFC 3280.

#### 2. Subordinate CA Certificate

##### (a) certificatePolicies

MUST be present and SHOULD NOT be marked critical. The set of policy identifiers MUST include the identifier for VeriSign's extended validation policy if the certificate is issued to a subordinate CA that is not controlled by VeriSign.

certificatePolicies:policyIdentifier (Required)

- o anyPolicy if subordinate CA is controlled by Root CA
- o explicit EV policy OID(s) if subordinate CA is not controlled by Root CA

The following fields MUST be present if the Subordinate CA is not controlled by VeriSign.

certificatePolicies:policyQualifiers:policyQualifierId

- o id-qt 2 [RFC 3280]

certificatePolicies:policyQualifiers:qualifier

- o URI to the Certificate Practice Statement

##### (b) cRLDistributionPoint

MUST be present and MUST NOT be marked critical. If present, it MUST contain the HTTP URL of VeriSign's CRL service.

##### (c) authorityInformationAccess

SHOULD be present and MUST NOT be marked critical. SHALL contain the HTTP URL of VeriSign's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). An HTTP accessMethod MAY be included for VeriSign's certificate (accessMethod = 1.3.6.1.5.5.7.48.2).

##### (d) basicConstraints

This extension MUST appear as a critical extension in all CA certificates that contain Public Keys used to validate digital signatures on certificates. The CA field MUST be set true. The pathLenConstraint field MAY be present.

**(e) keyUsage**

This extension MUST be present and MUST be marked critical. Bit positions for CertSign and cRLSign MUST be set. All other bit positions MUST NOT be set.

All other fields and extensions set in accordance to RFC 3280.

**3. Subscriber Certificate**

**(a) certificate Policies**

MUST be present and SHOULD NOT be marked critical. The set of policyIdentifiers MUST include the identifier for VeriSign's extended validation policy.

certificatePolicies:policyIdentifier (Required)

o EV policy OID

certificatePolicies:policyQualifiers:policyQualifierId (Required)

o id-qt 2 [RFC 3280]

certificatePolicies:policyQualifiers:qualifier (Required)

o URI to the Certificate Practice Statement

**(b) cRLDistributionPoint**

SHOULD be present and MUST NOT be marked critical. If present, it will contain the HTTP URL of VeriSign's CRL service. This extension MUST be present if the certificate does not specify OCSP responder locations in an authorityInformationAccess extension. See section 26(b) for details.

**(c) authorityInformationAccess**

SHOULD be present and MUST NOT be marked critical. SHALL contain the HTTP URL of VeriSign's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). An HTTP accessMethod MAY be included for VeriSign's certificate (accessMethod = 1.3.6.1.5.5.7.48.2). This extension MUST be present if the certificate does not contain a cRLDistributionPoint extension. See section 26(b) for details.

**(d) basicConstraints (optional)**

If present, the CA field MUST be set false.

**(e) keyUsage (optional)**

If present, bit positions for CertSign and cRLSign MUST NOT be set.

All other fields and extensions set in accordance to RFC 3280.