

DIGITÁLIS ALÁÍRÁS TELEPÍTÉSE SORÁN ALKALMAZOTT HITELESÍTÉSI SZOLGÁLTATÁSOK

A Technologix Studio Kft. által telepített digitális aláírás megoldások a következő technikai és szolgáltatási feltételek, valamint on-line hitelesítési szolgáltató közrevonásával történik.

A Technologix Studio Kft. a VeriSign® Inc. / Symantec® corporation Enterprise partnere, és jogosult a szolgáltatások telepítésére és viszonteladói értékesítésére.

Az értékesített szolgáltatások során alkalmazott digitális aláírás termékek:

- VeriSign® / GeoTrust® My Credential™ for Adobe®
- VeriSign® / GeoTrust® True Credentials™ for Adobe®

A VeriSign® Inc. által kínált hitelesítési és digitális aláírás szolgáltatás a magyar törvényi előírásoknak minden tekintetben megfelel. A VeriSign® Inc. által szolgáltatott hitelesítés az alábbi dokumentumokban leírt módon történik, az Európai normáknak megfelelően.

Csatolt dokumentumok:

VeriSign® Trust Network™ European Directive – CP Version 1.1 (pdf csatolmány)
VeriSign® Certification Practice Statement - Version 3.8.1 (pdf csatolmány)



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



VeriSign SARL
Route des Arsenaux 41
CH-1705 Fribourg
Switzerland



VeriSign UK Ltd.
2nd Floor, Waterfront
Chancellors Road,
London W9 9XR
United Kingdom

Budapest, 2010-03-01

VeriSign Trust Network European Directive CP



Version 1.1

Effective Date: September 30, 2005



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

VeriSign Trust Network European Directive Supplemental Policies

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

Revision date: August 2005

Trademark Notice

VeriSign is a registered trademark and OnSite is a registered service mark of VeriSign, Inc. The VeriSign logo, VeriSign Trust Network, NetSure, and Go Secure! 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 Trust Network European Directive Supplemental Policies on a nonexclusive, royalty-free basis, provided that (i) the foregoing copyright notice and the first two paragraphs of this Trademark Notice 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 Trust Network European Directive Supplemental Policies (as well as requests for copies from VeriSign) must be addressed to VeriSign, Inc., 487 East Middlefield Road, Mountain View, CA 94043 USA Attn: Practices Development. Tel: +1 650.961.7500 Fax: +1 650.429.5113 Net: practices@verisign.com.

TABLE OF CONTENTS

1. Introduction	1
1.1 Overview.....	3
1.2 Identification.....	8
1.3 Community and Applicability.....	8
1.3.1 Certification Authorities.....	8
1.3.2 Registration Authorities.....	9
1.3.3 End Entities.....	9
1.3.4 Applicability.....	10
1.3.4.1 Suitable Applications.....	10
1.3.4.2 Restricted Applications.....	10
1.3.4.3 Prohibited Applications.....	10
1.4 Contact Details.....	10
1.4.1 Specification Administration Organization.....	10
1.4.2 Contact Person.....	11
1.4.3 Person Determining CPS Suitability for the Policy.....	11
2. General Provisions	11
2.1 Obligations (DL1-2).....	11
2.1.1 CA Obligations.....	11
2.1.2 RA Obligations.....	13
2.1.3 Subscriber Obligations.....	14
2.1.4 Relying Party Obligations.....	15
2.1.5 Repository Obligations.....	15
2.2 Liability (DL1-2).....	15
2.2.1 Certification Authority Liability.....	15
2.2.1.1 Certification Authority Warranties to Subscribers and Relying Parties.....	15
2.2.1.2 Certification Authority Disclaimers of Warranties.....	16
2.2.1.3 Certification Authority Limitations of Liability.....	16
2.2.1.4 Force Majeure.....	16
2.2.2 Registration Authority Liability.....	16
2.2.3 Subscriber Liability.....	16
2.2.4 Relying Party Liability.....	16
2.3 Financial Responsibility (DL1-2).....	17
2.3.1 Indemnification by Subscribers and Relying Parties.....	17
2.3.2 Fiduciary Relationships.....	17
2.3.3 Administrative Processes.....	17
2.4 Interpretation and Enforcement (DL1-2).....	17
2.4.1 Governing Law.....	17
2.4.2 Severability, Survival, Merger, Notice.....	18
2.4.3 Dispute Resolution Procedures.....	18
2.5 Fees (DL1-2).....	18
2.6 Publication and Repository (DL1-2).....	18
2.6.1 Publication of CA Information.....	18
2.6.2 Frequency of Publication.....	19

2.6.3	Access Controls	19
2.6.4	Repositories	19
2.7	Compliance Audit (DL1-2)	19
2.8	Confidentiality and Privacy (DL1-2)	20
2.8.1	Types of Information to be Kept Confidential and Private	20
2.8.2	Types of Information Not Considered Confidential or Private	21
2.8.3	Disclosure of Certificate Revocation/Suspension Information	21
2.8.4	Release to Law Enforcement Officials	21
2.8.5	Release as Part of Civil Discovery	21
2.8.6	Disclosure Upon Owner's Request	21
2.8.7	Other Information Release Circumstances	21
2.9	Intellectual Property Rights (DL1-2)	21
2.9.1	Property Rights in Certificates and Revocation Information	21
2.9.2	Property Rights in the CP	22
2.9.3	Property Rights in Names	22
2.9.4	Property Rights in Keys and Key Material	22
3.	Identification and Authentication	22
3.1	Initial Registration	22
3.1.1	Types of Names (DL1-2)	22
3.1.2	Need for Names to be Meaningful (DL1-2)	22
3.1.3	Rules for Interpreting Various Name Forms (DL1-2)	22
3.1.4	Uniqueness of Names (DL1-2)	22
3.1.5	Name Claim Dispute Resolution Procedure (DL1-2)	22
3.1.6	Recognition, Authentication, and Role of Trademarks (DL1-2)	23
3.1.7	Method to Prove Possession of Private Key (DL1-2)	23
3.1.8	Authentication of Organization Identity (DL1-2)	23
3.1.9	Authentication of Individual Identity (DL1-2)	23
3.2	Routine Rekey (Renewal) (DL1-2)	24
3.3	Rekey After Revocation (DL1-2)	24
3.4	Revocation Request (DL1-2)	24
4.	Operational Requirements	25
4.1	Certificate Application (DL1-2)	25
4.1.1	Certificate Applications for End-User Subscriber Certificates	25
4.1.2	Certificate Applications for CA or RA Certificates	25
4.2	Certificate Issuance (DL1-2)	26
4.2.1	Issuance of End-User Subscriber Certificates	26
4.2.2	Issuance of CA and RA Certificates	26
4.3	Certificate Acceptance (DL1-2)	27
4.4	Certificate Suspension and Revocation (DL1-2)	27
4.4.1	Circumstances for Revocation	27
4.4.2	Who Can Request Revocation	27
4.4.3	Procedure for Revocation Request	27
4.4.4	Revocation Request Grace Period	27
4.4.5	Circumstances for Suspension	28
4.4.6	Who Can Request Suspension	28
4.4.7	Procedure for Suspension Request	28

4.4.8	Limits on Suspension Period	28
4.4.9	CRL Issuance Frequency (If Applicable).....	28
4.4.10	Certificate Revocation List Checking Requirements	28
4.4.11	On-Line Revocation/Status Checking Availability	28
4.4.12	On-Line Revocation Checking Requirements	28
4.4.13	Other Forms of Revocation Advertisements Available.....	28
4.4.14	Checking Requirements for Other Forms of Revocation Advertisements	28
4.4.15	Special Requirements Regarding Key Compromise	29
4.5	Security Audit Procedures (DL1-2)	29
4.5.1	Types of Events Recorded.....	29
4.5.2	Frequency of Processing Log	29
4.5.3	Retention Period for Audit Log.....	30
4.5.4	Protection of Audit Log.....	30
4.5.5	Audit Log Backup Procedures	30
4.5.6	Audit Collection System	30
4.5.7	Notification to Event-Causing Subject.....	30
4.5.8	Vulnerability Assessments	30
4.6	Records Archival (DL1-2).....	30
4.6.1	Types of Events Recorded.....	30
4.6.2	Retention Period for Archive	31
4.6.3	Protection of Archive.....	31
4.6.4	Archive Backup Procedures.....	31
4.6.5	Requirements for Time-Stamping of Records	31
4.6.6	Archive Collection System	31
4.6.7	Procedures to Obtain and Verify Archive Information	31
4.7	Key Changeover (Renewal) (DL1-2).....	31
4.8	Compromise and Disaster Recovery (DL1-2)	32
4.8.1	Computing Resources, Software, and/or Data Are Corrupted	32
4.8.2	Entity Public Key is Revoked	32
4.8.3	Entity Key is Compromised.....	32
4.8.4	Secure Facility After a Natural or Other Type of Disaster	32
4.9	CA Termination (DL1-2).....	33
5. Physical, Procedural, and Personnel Security Controls		
(DL1-2)		33
5.1	Physical Controls	34
5.1.1	Site Location and Construction	34
5.1.2	Physical Access.....	35
5.1.3	Power and Air Conditioning	35
5.1.4	Water Exposures	35
5.1.5	Fire Prevention and Protection	35
5.1.6	Media Storage	35
5.1.7	Waste Disposal.....	35
5.1.8	Off-Site Backup.....	35
5.2	Procedural Controls	36
5.2.1	Trusted Roles	36
5.2.2	Number of Persons Required Per Task	36

5.2.3	Identification and Authentication for Each Role	37
5.3	Personnel Controls	37
5.3.1	Background, Qualifications, Experience, and Clearance Requirements..	38
5.3.2	Background Check Procedures	38
5.3.3	Training Requirements.....	38
5.3.4	Retraining Frequency and Requirements	38
5.3.5	Job Rotation Frequency and Sequence.....	38
5.3.6	Sanctions for Unauthorized Actions.....	39
5.3.7	Contracting Personnel Requirements	39
5.3.8	Documentation Supplied to Personnel.....	39
6.	Technical Security Controls	39
6.1	Key Pair Generation and Installation.....	39
6.1.1	Key Pair Generation (DL1-2)	39
6.1.2	Private Key Delivery to Entity.....	40
6.1.2.1	Private Key Delivery to Entity – DL1.....	40
6.1.2.2	Private Key and SSCD Delivery to Entity – DL2.....	40
6.1.3	Public Key Delivery to Certificate Issuer (DL1-2)	41
6.1.4	CA Public Key Delivery to Users (DL1-2).....	41
6.1.5	Key Sizes (DL1-2).....	41
6.1.6	Public Key Parameters Generation (DL1-2).....	41
6.1.7	Parameter Quality Checking (DL1-2).....	42
6.1.8	Hardware/Software Key Generation (DL1-2)	42
6.1.9	Key Usage Purposes (As per X.509 v3 Key Usage Field) (DL1-2)	42
6.2	Private Key Protection	42
6.2.1	Standards for Cryptographic Modules (DL1-2)	43
6.2.2	Private Key (n out of m) Multi-Person Control (DL1-2).....	43
6.2.3	Private Key Escrow (DL1-2).....	43
6.2.4	Private Key Backup (DL1-2)	43
6.2.5	Private Key Archival (DL1-2).....	44
6.2.6	Private Key Entry into Cryptographic Module (DL1-2)	44
6.2.7	Method of Activating Private Key	44
6.2.7.1	DL1 Certificates.....	44
6.2.7.2	DL2 Certificates.....	44
6.2.8	Method of Deactivating Private Key (DL1-2).....	44
6.2.9	Method of Destroying Private Key (DL1-2)	44
6.3	Other Aspects of Key Pair Management (DL1-2).....	44
6.3.1	Public Key Archival	44
6.3.2	Usage Periods for the Public and Private Keys	45
6.4	Activation Data (DL1-2).....	45
6.4.1	Activation Data Generation and Installation	45
6.4.2	Activation Data Protection.....	45
6.4.3	Other Aspects of Activation Data	45
6.5	Computer Security Controls (DL1-2).....	45
6.5.1	Specific Computer Security Technical Requirements	45
6.5.2	Computer Security Rating.....	46
6.6	Life Cycle Technical Controls (DL1-2)	47

6.6.1	System Development Controls	47
6.6.2	Security Management Controls.....	47
6.6.3	Life Cycle Security Ratings.....	48
6.7	Network Security Controls (DL1-2)	48
6.8	Cryptographic Module Engineering Controls (DL1-2)	48
7.	Certificate and CRL Profile (DL1-2)	48
7.1	Certificate Profile.....	49
7.1.1	Version Number(s).....	49
7.1.2	Certificate Extensions	49
7.1.3	Algorithm Object Identifiers.....	50
7.1.4	Name Forms	50
7.1.5	Name Constraints	50
7.1.6	Certificate Policy Object Identifier	50
7.1.7	Usage of Policy Constraints Extension	51
7.1.8	Policy Qualifiers Syntax and Semantics.....	51
7.1.9	Processing Semantics for the Critical Certificate Policy Extension	51
7.2	CRL Profile.....	51
8.	Specification Administration (Class 1-3)	51
8.1	Specification Change Procedures.....	51
8.1.1	Items that Can Change Without Notification	51
8.1.2	Items that Can Change with Notification	52
8.1.2.1	List of Items.....	52
8.1.2.2	Notification Mechanism	52
8.1.2.3	Comment Period	52
8.1.2.4	Mechanism to Handle Comments	52
8.1.3	Changes Requiring Changes in the Certificate Policy OID or CPS Pointer 53	
8.2	Publication and Notification Policies	53
8.2.1	Items Not Published in the EDP or CPS	53
8.2.2	Distribution of the EDP and CPSs	53
8.3	CPS Approval Procedures	53
	Acronyms and Definitions	54
	Table of Acronyms.....	54
	Definitions.....	55
	Cross-Reference of ETSI Definitions to CP Definitions	58

1. Introduction

The VeriSign Trust Network European Directive Policies (referred to in this document as the singular acronym “EDP”) supplements the VeriSign Trust Network Certificate Policies (“CP”) with additional information as to how the VTN meets specific ETSI policy requirements. The purpose of the EDP is to facilitate compliance with the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for Electronic Signatures (the “Directive”).¹ The Directive is intended to facilitate the use of Electronic Signatures and establishes requirements for “Qualified Certificates” that support certain types of Electronic Signatures.

Please Note: The capitalized terms in this EDP are defined terms with specific meanings. Please see the Acronyms and Definitions section for a list of certain definitions specific to this EDP. Any other defined terms shall have the meanings given to them by the CP.

The EDP also describes the two certificate policies set forth in the European Telecommunications Standards Institute (“ETSI”) Technical Specification 101 456 (the “ETSI Policy Document Policy Document”).² The EDP defines two policies that supplement the CP, referred to here as “Directive Level 1” (“DL1”) and “Directive Level 2” (“DL2”).³ DL1 and DL2 correspond, respectively, to the “QCP public” certificate policy and “QCP public + SSCD” certificate policy defined in the ETSI Policy Document.⁴ Finally, the EDP supplements the certificate profile developed by ETSI (the “Qualified Certificate Profile”),⁵ which defines a technical format for Certificates that meet the requirements of the directive (“Qualified Certificates”). Certification Authorities issuing Qualified Certificates can use the Qualified Certificate Profile to assist them in issuing certificates that comply with annex I and II of the Directive.⁶

VeriSign, Inc. (“VeriSign”) is the leading provider of trusted infrastructure services to web sites, enterprises, electronic commerce service providers, and individuals. The company’s domain name, digital certificate, and payment services provide the critical web identity, authentication, and transaction infrastructure that online businesses require to conduct secure e-commerce and communications. The VeriSign Trust NetworkSM (“VTN”) is a global public key infrastructure (“PKI”) established to support the use of digital certificates (“Certificates”) in both wired and wireless applications. VeriSign offers VTN services together with a global network of affiliates (“Affiliates”)

¹ Council Directive 1999/93/EC, 2000 O.J. (L 0093) 12 [hereinafter referred to as the “Directive”].

² ETSI TS 101 456 V1.3.1 (2005-05) Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates. [hereinafter referred to as the “ETSI Policy Document”].

³ Although designations DL1 and DL2 do not appear in the Directive itself, the EDP uses these shorthand terms solely for the purpose of brevity. No official European Community imprimatur for the use of these terms should be inferred from their presence in the EDP.

⁴ ETSI Policy Document § 5.2.

⁵ European Telecommunications Standards Institute, Qualified certificate profile § 1 (ETSI TS 101 862 V1.2.1 June 2001) [hereinafter referred to as the “Qualified Certificate Profile”].

⁶ See Qualified Certificate Profile § 1.

throughout the world, many of whom are located within jurisdictions in the European Community (“EC”).

The CP is the principal statement of policy governing the VTN. It sets forth the business, legal, and technical requirements (“VTN Standards”) for approving, issuing, managing, using, revoking, and renewing, digital Certificates within the VTN and providing associated trust services. The EDP supplements the CP provisions by setting forth requirements that VTN Participants (including Affiliates, Customers, Subscribers, Subjects and Relying Parties) must meet in order to issue, manage, use, revoke, and renew “Qualified Certificates” within the meaning of the Directive and the ETSI Policy Document. The requirements for Qualified Certificates correspond to the DL1 supplemental policy. The EDP also sets forth the additional requirements for the use of Qualified Certificates in conjunction with a “secure-signature-creation device” (“SSCD”). The requirements for Qualified Certificates used in conjunction with an SSCD correspond to the DL2 supplemental policy.

This document, however, is not specific to the laws of any member nation of the EC. The Electronic Signature laws of EU member countries (“Member Countries”) vary. Therefore, practices specifically addressing the laws of individual member states may appear in the Affiliates’ Certification Practice Statements and other applicable documents. Moreover, the EDP is an evolving document and may change as new or modified requirements emerge.

Most of the footnotes to this EDP cite to the relevant portions of the Directive, the ETSI Policy Document, and the Qualified Certificate Profile that form the basis for specific requirements in the EDP. In other words, when a sentence in the EDP contains a footnote citing to a particular section of the Directive, ETSI Policy Document, or Qualified Certificate Profile, the sentence is creating a VTN-level requirement to implement the obligations imposed by the cited section. Footnotes containing such citations, however, do not add substantive requirements to the EDP.

As a supplement to the CP, the EDP does not attempt to address all topics relating to the VTN. In some instances, the EDP may not address a topic covered in the CP or may not address a topic at all. In these cases, the relevant section contains an entry stating, “No stipulation.” The lack of a stipulation in a particular section shall not be construed as the absence of any stipulation within any document in the VTN document architecture. Rather, the statement “No stipulation” means that the EDP has added no additional stipulation beyond what may appear in other documents within the VTN document architecture, including (but not limited to) the CP.

The authors of this EDP comprise the members of the VeriSign Trust Network Policy Management Authority (“PMA”). The PMA is responsible for proposing changes to the CP, supplemental policies to the CP, and other policy documents; updating these documents, and soliciting comments on them. The PMA also oversees compliance with the requirements of these documents.

1.1 Overview

The Directive identifies a special form of Electronic Signature based on a Qualified Certificate. Annexes I and II to the Directive set forth requirements respectively for Qualified Certificates and “certification-service-providers” (called “Certification Authorities” or “CAs” here and in the CP) that issue Qualified Certificates. Annex III of the Directive relates to the use of an SSCD in conjunction with a Qualified Certificate.

Under Article 5(2) of the Directive, Electronic Signatures shall not be:

“denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:

- in electronic form, or
- not based upon a qualified certificate, or
- not based upon a qualified certificate issued by an accredited certification-service-provider, or
- not created by a secure signature creation-device.”⁷

“‘Electronic signature’ means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.”⁸

Digital signatures, as described in the CP, verifiable by reference to Certificates (including Qualified Certificates), constitute “Advanced Electronic Signatures” within the meaning of the Directive.

“‘Advanced electronic signature’ means an electronic signature which meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using means that the signatory can maintain under his sole control; and (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.”⁹

Nonetheless, the use of a key pair and Certificates alone does not under the Directive invoke more favorable treatment of digital signatures produced or verifiable using the key pair than ordinary Electronic Signatures. The party seeking to use such digital signatures would still have the burden of satisfying the legal requirements of a signature in a litigation or other proceeding that normally would apply to handwritten signatures. The use of Certificates to make digital signatures pursuant to the CP, in other words, gives the Subscriber only the baseline legal validity under Article 5(2) in that these signatures must not be denied legal effectiveness simply because they are in electronic form. They do not automatically satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data .

Article 6 of the Directive, however, creates special liability rules for CA’s issuing Qualified Certificates relating to the lifecycle management of Qualified Certificates. CAs may wish to utilize the legal regime created by Article 6. If so, they must meet the

⁷ Directive art. 5(2).

⁸ Directive art. 2(1); ETSI Policy Document §3.1.

⁹ Directive art. 2(2); ETSI Policy Document §3.1.

requirements for issuing Qualified Certificates, and not simply any Certificates. Article 6 also imposes responsibilities on Subscribers and Subjects of Qualified Certificates.

The requirements relating to the approval, issuance, management, use, revocation, and renewal of Qualified Certificates are set forth in the QCP public certificate policy set forth in the ETSI Policy Document.¹⁰ The DL1 supplemental policy set forth in this EDP is intended for VTN Participants wishing to approve, issue, manage, use, revoke, and renew Certificates in order to:

- meet the requirements of the QCP public certificate policy in the ETSI Policy Document,
- conform to a standard code of practice that is recognized by most EU countries, as embodied in the ETSI Policy Document,
- have such certificates be considered “Qualified Certificates” within the meaning of the Directive,
- invoke the special liability rules of Article 6 of the Directive, and
- permit Subscribers to create digital signatures by the use of such Certificates, as one type of Electronic Signature, which shall not be denied legal effectiveness pursuant to Article 5(2) of the Directive.

More specifically, the combination of adhering to the CP and the DL1 supplemental policy is intended to permit VTN Participants to meet these objectives.

While Advanced Electronic Signatures used in conjunction with Qualified Certificates have a baseline of legal validity under Article 5(2) of the directive, if Subscribers of a Qualified Certificate use an SSCD to make Advanced Electronic Signatures, then the digital signatures created by these subscribers do satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data.

“Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device: (a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and (b) are admissible as evidence in legal proceedings.”¹¹

The use of Qualified Certificates and an SSCD to make digital signatures pursuant to the CP, in other words, gives the Subscriber the ability to create digital signatures that, under the Directive, are considered to the same extent as handwritten digital signatures.

The requirements relating to the approval, issuance, management, use, revocation, and renewal of Qualified Certificates in conjunction with an SSCD are set forth in the QCP public + SSCD certificate policy set forth in the ETSI Policy Document.¹² The DL2 supplemental policy set forth in this EDP is intended for VTN Participants wishing to approve, issue, manage, use, revoke, and renew Certificates in order to:

¹⁰ See ETSI Policy Document § 5.1.

¹¹ Directive art. 5(1).

¹² See ETSI Policy Document § 5.1.

- meet the requirements of the QCP public + SSCD certificate policy in the ETSI Policy Document,
- conform to a standard code of practice that is recognized by most EU countries, as embodied in the ETSI Policy Document,
- have such certificates be considered “Qualified Certificates” within the meaning of the Directive,
- have the private key protection token and reader used by Subscribers under DL2 be considered a “secure-signature-creation device” within the meaning of Annex III of the Directive, and
- invoke the special liability rules of Article 6 of the Directive, and
- permit Subscribers to create digital signatures, by the use of such Certificates and private key protection token, that have the benefit of the treatment of Advanced Electronic Signatures created in conjunction with an SSCD under Article 5(1) of the Directive.

More specifically, the combination of adhering to the CP and the DL2 supplemental policy is intended to permit VTN Participants to meet these objectives.

(a) Role of the EDP with Respect to Other Practices Documents

The CP describes at a general level the VTN Standards acting as requirements for the overall business, legal, and technical infrastructure of the VTN. The CP is published in electronic form within the VeriSign Repository at <https://www.verisign.com/CP>. The CP is available in the VeriSign Repository in Word format, Adobe Acrobat pdf, and HTML. VeriSign also makes the CP available in Adobe Acrobat pdf or Word format upon request sent to CP-requests@verisign.com. The CP is available in paper form from the PMA upon requests sent to: VeriSign, Inc., 487 East Middlefield Road, Mountain View, CA 94043 USA, Attn: Practices Development – CP.

As mentioned in the CP, VTN documentation includes ancillary security and operational documents that supplement the CP by providing more detailed requirements. Examples include the VeriSign Security Policy, the Security and Audit Requirements Guide, the Enterprise Security Guide, the Affiliate Practices Legal Requirements Guidebook, and the Key Ceremony Reference Guide. These documents are above the Certification Practice Statements and Ancillary agreements used by VeriSign or an Affiliate within the VTN documentation architecture. Figure 1 shows the relationship between the CP and other practices documents.

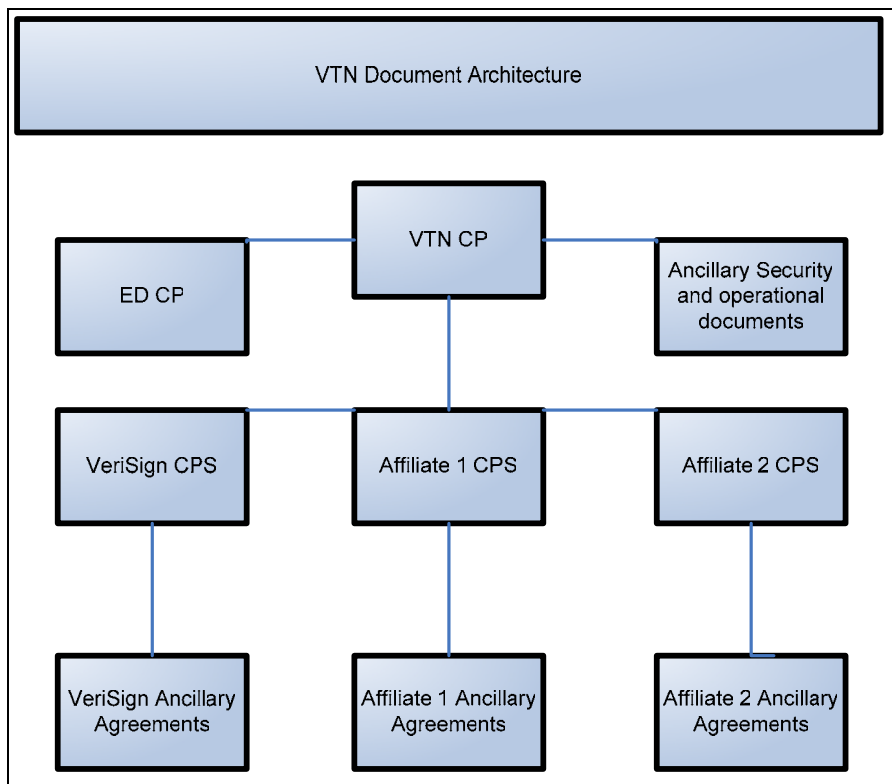


Figure 1 - VTN Document Architecture

The EDP within the VTN document architecture stands above CPSs and the ancillary agreements used by VeriSign and Affiliates. As with the CP and other ancillary security and operational documents, VeriSign and the PMA maintains this EDP.

EDPEDP

(b) Knowledge Assumed by the EDP

This EDP assumes that the reader is generally familiar with Digital Signatures, PKIs, VeriSign’s VTN, the Directive, the ETSI Policy Document, and the Qualified Certificate Profile. In addition, the EDP assumes that the reader is familiar with the CP. If not, VeriSign advises that the reader review the CP and obtain training in the use of public key cryptography and public key infrastructure as implemented in the VTN. The CP contains references to such information and a brief summary of the roles of the VTN participants. See CP § 1.1(b).

(c) Compliance with Applicable Standards

The structure of this EDP generally corresponds to the *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, known as RFC 2527 of the Internet Engineering Task Force, an Internet standards body. This document serves to define two supplemental policies, which can be considered

“certificate policies” within the meaning of RFC 2527. The RFC 2527 framework has become a standard in the PKI industry. This EDP conforms to the RFC 2527 framework in order to make policy mapping and comparisons, assessment, and interoperability easier for persons using or considering using VTN services that comply with the Directive.

While VeriSign has attempted to conform the EDP to the RFC 2527 structure where possible, slight variances in title and detail are necessary because of the breadth of VTN business models. VeriSign reserves the right to vary from the RFC 2527 structure as needed, for example to enhance the quality of the EDP or its suitability to the VTN. Moreover, the EDP’s structure may not correspond to future versions of RFC 2527.

(d) Policy Overview

The EDP defines two policies, DL1 and DL2. The DL1 policy corresponds to the QCP public certificate policy in the ETSI Policy Document. The Qualified Certificates issued under DL1 are appropriate for digital signatures for applications in which the level of validity provided by Article 5(2) of the Directive is appropriate and adequate. That is, Qualified Certificates issued under DL1 support the use of digital signatures that shall not be denied legal effectiveness simply because they are in electronic form.

The DL2 policy corresponds to the QCP public + SSCD certificate policy in the ETSI Policy Document. The Qualified Certificates issued under DL2 are appropriate for digital signatures for applications in which the level of validity provided by Article 5(1) of the Directive is necessary or desired. That is, Qualified Certificates issued under DL2 support the use of digital signatures that are equivalent in legal effectiveness to handwritten signatures.

The DL1 and DL2 policies are distinct from the VTN’s Classes 1, 2, and 3 within the meaning of the CP. DL1 and DL2 levels do not correspond to any particular VTN Class. Nonetheless, DL1 and DL2 both provide assurances of the identity of the Subscriber based on the direct or indirect personal (physical) presence of the Subscriber before a person that checks the Subscriber’s identity documentation. Only Class 3 individual Certificates require personal presence and the checking of identity credentials as the mechanism for authentication. Certificate Applicants for Class 2 Certificates are not required to appear personally before a CA or RA. Moreover, Class 1 Certificates do not provide assurances of identity at all. Therefore, if CAs and RAs perform only the minimum required procedures for the authentication of identity, Class 1 and Class 2 Certificates cannot be Qualified Certificates.

Section 1.1.1 of the CP, however, permits CAs and RAs to perform stronger authentication procedures than the minimum required procedures for Classes 1-3.

[B]y contract or within specific environments (such as an intra-company environment or within a community of interest), VTN Participants are permitted to use validation procedures stronger than the ones set forth within the CP, or use Certificates for higher security applications than the ones described in CP §§ 1.1.1, 1.3.4.1. Any such usage, however, shall be limited to such entities and subject to CP §§ 2.2.1.2, 2.2.2.2, and these entities shall be solely responsible for any harm or liability caused by such usage.¹³

Class 1 and Class 2 Certificates that are issued based on authentication procedures requiring personal presence pursuant to this clause of the CP may constitute Qualified Certificates if they meet all other requirements of DL1 or DL2.

Qualified Certificates may also provide assurances that a person is associated with a legal person or other organizational entity. These assurances are the equivalent of assurances that a Subscriber is an Affiliated Individual with respect to an organization within the meaning of the CP. Affiliated Individuals are natural persons that are related to a Client Managed PKI Customer or Client Managed PKI Lite 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 (e.g., a customer).

DL1 and DL2 Certificates are issued only to individuals. DL1 and DL2 Certificates may be Retail or Managed PKI Certificates or Certificates issued by a Gateway Customer, as long as all they meet all the requirements of the applicable supplemental policy.

1.2 Identification

VeriSign, acting as a policy-defining authority, has assigned the supplemental certificate policy within this EDP for each of DL1 and DL2 an object identifier value extension set forth below. The object identifier values used for DL1 and DL2 are:

- Directive Level 1: VeriSign/pki/policies/EDP/dl1 (2.16.840.1.113733.1.7.44.1).
- Directive Level 2: VeriSign/pki/policies/EDP/dl2 (2.16.840.1.113733.1.7.44.2).

1.3 Community and Applicability

The community governed by this EDP is that portion of the VeriSign Trust Network that desires or is required to approve, issue, manage, use, revoke, and renew of Qualified Certificates that meet the requirements of the Directive, ETSI Policy Document, and Qualified Certificate Profile.

1.3.1 Certification Authorities

Certification Authorities governed by the EDP are those CAs wishing to approve, issue, manage, revoke, and renew Qualified Certificates meeting the requirements of the

¹³ CP § 1.1.1.

Directive, ETSI Policy Document, and Qualified Certificate Profile. These CAs may fit within any of the five categories of CAs identified in the CP: (1) Processing Centers, (2) Client Service Centers, (3) Client Managed PKI Customers, (4) Gateway Customers, and (5) ASB Customers. CAs wishing to issue Qualified Certificates must notify their Superior Entities of their intention to do so, and their issuance of Qualified Certificates is subject to a special agreement or agreement addendum relating to Qualified Certificates and this EDP.

1.3.2 Registration Authorities

Registration Authorities governed by the EDP are those RAs wishing to approve and request the issuance, revocation, and renewal of Qualified Certificates meeting the requirements of the Directive, ETSI Policy Document, and Qualified Certificate Profile. These RAs may fit within any of the five categories of RAs identified in the CP: (1) Server Service Centers, (2) Client Managed PKI Lite Customers, (3) Server Managed PKI Customers, (4) Global Server Managed PKI Customers, and (5) ASB Providers. RAs wishing to issue Qualified Certificates must notify their Superior Entities of their intention to do so, and their issuance of Qualified Certificates is subject to a special agreement or agreement addendum relating to Qualified Certificates and this EDP.

1.3.3 End Entities

DL1 and DL2 Certificates are client Certificates issued only to individual end-user Subscribers and/or Subjects. Subscribers and Subjects may or may not be Affiliated Individuals in relation to a legal person or other organizational entity. 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 EDCP to distinguish between these two roles: "Subscriber", is the entity which contracts with the CA 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.¹⁴

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 EDP will invoke the correct understanding

¹⁴ See ETSI Policy Document § 4.4

1.3.4 Applicability

1.3.4.1 Suitable Applications

DL1 Certificates may be used to support digital signatures, where the applications making use of the digital signatures require Electronic Signatures that “are not [to be] denied legal effectiveness and admissibility as evidence in legal proceedings” in accordance with article 5(2) of the Directive. The uses for DL1 Certificates correspond to the uses for certificates identified in the QCP public certificate policy in the ETSI Policy Document.¹⁵

DL2 Certificates may be used to support digital signatures where the applications making use of the digital signatures require Advanced Electronic Signatures that “satisfy the requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper based data” in accordance with article 5(1) of the Directive. The uses for DL2 Certificates correspond to the uses for certificates identified in the QCP public + SSCD certificate policy in the ETSI Policy Document.¹⁶

In addition, DL1 and DL2 Certificates may be used for the other applications identified in the CP.

1.3.4.2 Restricted Applications

In addition to the restrictions in CP § 1.3.4.2, Subscribers and/or Subjects of DL2 Certificates shall use an SSCD to create digital signatures only in connection with the use of an SSCD.¹⁷

1.3.4.3 Prohibited Applications

See CP § 1.3.4.3.

1.4 Contact Details

1.4.1 Specification Administration Organization

The organization administering this EDP is the VTN Policy Management Authority. The address for the PMA is:

¹⁵ See ETSI Policy Document § 5.3.2.

¹⁶ See ETSI Policy Document § 5.3.1.

¹⁷ See ETSI Policy Document § 6.2(e).

VeriSign Trust Network Policy Management Authority
c/o VeriSign, Inc.
487 East Middlefield Road
Mountain View, CA 94043 USA
+1 (650) 961-7500 (voice)
+1 (650) 429-5113 (fax)
practices@verisign.com

1.4.2 Contact Person

Address inquiries about the EDP to practices@verisign.com or to the following address:

VeriSign, Inc.
487 East Middlefield Road
Mountain View, CA 94043 USA
Attn: Practices Development – EDP
+1 (650) 961-7500 (voice)
+1 (650) 429-5113 (fax)

1.4.3 Person Determining CPS Suitability for the Policy

The persons determining whether the CPS of an Affiliate is suitable for this EDP are the members of the VeriSign PMA. See CP § 1.4.2.

2. General Provisions

2.1 Obligations (DL1-2)

2.1.1 CA Obligations

CAs (see EDP § 1.3.1) shall perform the obligations applicable to CAs that appear elsewhere within the EDP. By performing CA obligations that appear in the CP and EDP, a CA thereby meets the general CA obligations set forth in the ETSI Policy Document.¹⁸ Also, a CA's obligation to take commercially reasonable efforts to bind Subscribers, Subjects and Relying Parties to Terms and Conditions is satisfied by using Subscriber Agreements and Relying Party Agreements under the VTN CP.¹⁹ Certain required terms of such Subscriber Agreements and Relying Party Agreements, however, are set forth below in this section.

In addition, CAs remain responsible for the performance of obligations set forth in the EDP, notwithstanding any delegation of front-end functions or back-end functions to

¹⁸ See ETSI Policy Document § 6.1.

¹⁹ See ETSI Policy Document §§ 6.3, 7.1(e).

another entity.²⁰ CAs shall also perform any obligations set forth in certificate content or incorporated by reference in the Certificate. Such obligations include, but are not limited to, obligations appearing in the Relying Party Agreement referred to in the Certificate.²¹ Finally, CAs shall perform their services in accordance with the applicable Affiliate's CPS.²²

Affiliates' policies and procedures shall be non-discriminatory and shall require that CAs make their services accessible to all applicants whose activities fall within their declared fields of operation.²³

Subscriber Agreements shall be in writing and in readily understandable language.²⁴ Furthermore, Subscriber Agreements shall contain the following terms required by the Directive and the ETSI Policy Document as well as any other terms required by law:²⁵

- The applicable policy, whether DL1 or DL2, including a clear statement as to whether the use of an SSCD is required or not,
- An acknowledgement that the information contained in the Certificate is correct unless the Subscriber informs the applicable CA or RA otherwise,
- Applicable limitations on use, which at a minimum shall include the limitations in CP § 1.3.4 and EDP § 1.3.4,
- The obligations of Subscribers set forth in CP § 2.1.1 and this section and assent to perform such obligations,
- Information on how to validate a Certificate, including a requirement to check the status of a Certificate, and the conditions upon which reliance on a certificate is deemed "reasonable," which apply to situations where Subscribers also act as Relying Parties,²⁶
- Applicable limitations of liability,
- Consent to the publication of the Certificate issued to the Subscriber and its availability for retrieval by Relying Parties,
- Consent to the retention of records used in enrollment, the provision of an SSCD to the Subscriber, revocation information, and the transition of such information to third parties in the event of CA termination (see EDP § 4.9) under the same conditions required by this EDP,
- The records retention period for Certificate Application information,
- The records retention period for CA event logs,
- Applicable dispute resolution procedures,
- Governing law, and

²⁰ See ETSI Policy Document § 4.1, 6.1, 7.4.1(b); CP § 1.3.1.

²¹ See ETSI Policy Document § 6.3?.

²² The specific obligations within this paragraph correspond to § 6.1 of the ETSI Policy Document.

²³ See ETSI Policy Document § 7.5.1(a)-(b).

²⁴ See Directive annex II(k); ETSI Policy Document §§ 7.3.1(b), 7.3.4(b).

²⁵ See Directive annex II(k); ETSI Policy Document §§ 7.3.1(hi), 7.3.4(a), 7.3.5(b)

²⁶ See CP § 2.2.1.1.

- Whether the CA has been certified to be conformant with the DL1 and QCP public certificate policies (in the case of DL1 Certificates) or with the DL2 and QCP public + SSCD certificate policies (in the case of DL2 Certificates).
- An acknowledgement that in the case of being informed that the CA which issued the subject's certificate has been compromised, the subscriber will ensure that the certificate is not used by the subject.

Subscriber Agreements shall be communicated to and accepted by Certificate Applicants before they submit enrollment information and with means that preserve the integrity of the Subscriber Agreements.²⁷ If the subject and subscriber are separate entities, the subscriber shall make the subject aware of those obligations applicable to the subject.

Prior to the issuance of a new Certificate upon renewal or rekeying, any changes to Subscriber Agreements implemented since the time of the last enrollment or re-enrollment shall be communicated to the Subscriber with means that preserve the integrity of the Subscriber Agreements.²⁸

Relying Party Agreements shall be in writing and in readily understandable language.²⁹

Furthermore, Relying Party Agreements shall contain the following terms required by the ETSI Policy Document:³⁰

- The applicable policy, whether DL1 or DL2, including a clear statement as to whether Subscribers are required to use an SSCD or not,
- Applicable limitations on use, which at a minimum shall include the limitations in CP § 1.3.4 and EDP § 1.3.4,
- Information on how to validate a Certificate, including a requirement to check the status of a Certificate, and the conditions upon which reliance on a certificate is deemed "reasonable,"
- Applicable limitations of liability,
- The records retention period for Certificate Application information,
- The records retention period for CA event logs,
- Applicable dispute resolution procedures,
- Governing law, and
- Whether the CA has been certified to be conformant with the DL1 and QCP public certificate policies (in the case of DL1 Certificates) or with the DL2 and QCP public + SSCD certificate policies (in the case of DL2 Certificates).

2.1.2 RA Obligations

RAs (see EDP § 1.3.2) shall perform the obligations applicable to RAs that appear elsewhere within the EDP. RAs shall also perform any obligations set forth in certificate

²⁷ See ETSI Policy Document § 7.3.1(a)-(b).

²⁸ See ETSI Policy Document § 7.3.2(b).

²⁹ See ETSI Policy Document § 7.3.4(b).

³⁰ See ETSI Policy Document § 7.3.4(a).

content or incorporated by reference in the Certificate. Such obligations include, but are not limited to, obligations appearing in the Relying Party Agreement referred to in the Certificate. Finally, RAs shall perform their services in accordance with the applicable Affiliate's CPS. To the extent RAs use Subscriber Agreements, they shall meet the requirements of EDP § 2.1.1. Server Service Centers and ASB Providers shall use Relying Party Agreements meeting the requirements set forth in EDP § 2.1.1.

Affiliates' CPSs shall require that RAs make their services accessible to all applicants whose activities fall within their declared fields of operation.³¹

2.1.3 Subscriber Obligations

Subscribers meeting the requirements of CP § 2.1.3 and other provisions of the CP thereby meet most of the obligations imposed on Subscribers by the ETSI Policy Document.³² In addition, though, a Subject shall use the private key corresponding to the public key within a DL2 Certificate (with which an SSCD must be used) to make a digital signature only if the private key was generated in the Subscriber's SSCD and the digital signature is made in connection with the use of the SSCD.³³

If the subject and subscriber are separate entities, the subscriber shall make the subject aware of the obligations applicable to the subject (as listed below):

- a) Submit accurate and complete information to the CA in accordance with the requirements of this policy, particularly with regards to registration;
- b) Only use the key pair for electronic signatures and in accordance with any other limitations notified to the subscriber;
- c) Exercise reasonable care to avoid unauthorized use of the subject's private key;
- d) If the subscriber or subject generates the subject's keys:
 - i) generate subject's keys using an algorithm recognized as being fit for the purposes of qualified electronic signatures;
 - ii) use a key length and algorithm which is recognized as being fit for the purposes of qualified electronic signatures during the validity time of the certificate;
 - iii) the subject's private key can be maintained under the subject's sole control.
- e) If the certificate policy requires use of an SSCD, only use the certificate with electronic signatures created using such a device;
- f) if the certificate is issued by the CA under certificate policy DL2 and the subject's keys are generated under control of the subscriber or subject, generate the subject's keys within the SSCD to be used for signing;
- g) Notify the CA without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:
 - i) The subject's private key has been lost (e.g. by forgetting the PIN number needed to use the key), stolen, potentially compromised; or

³¹ See ETSI Policy Document § 7.5.1(a)-(b).

³² See ETSI Policy Document § 6.2(a)-(d), (g).

³³ See ETSI Policy Document § 6.2(e)-(f).

- ii) Control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons; and/or
 - iii) Inaccuracy or changes to the certificate content, as notified to the subscriber or to the subject.
- h) Following compromise, the use of the subject's private key is immediately and permanently discontinued;
- i) In the case of being informed that the CA which issued the subject's certificate has been compromised, ensure that the certificate is not used by the subject.

2.1.4 Relying Party Obligations

Relying Parties meeting the requirements of CP § 2.1.4 and other provisions of the CP meet the obligations imposed on Relying Parties by the ETSI Policy Document.³⁴

2.1.5 Repository Obligations

No stipulation.

2.2 Liability (DL1-2)

2.2.1 Certification Authority Liability

The liability of Certification Authorities is governed by article 6 of the Directive.³⁵ The provisions of this EDP § 2.2.1 relate only to the use of private keys and Qualified Certificates with respect to the creation and verification of digital signatures.

2.2.1.1 Certification Authority Warranties to Subscribers and Relying Parties

In addition to the warranties set forth in CP § 2.2.1.1, Relying Party Agreements shall contain a warranty to Relying Parties who reasonably rely on a Qualified Certificate to verify a digital signature that:

- The Qualified Certificate contains all the details prescribed for a Qualified Certificate under the Directive,³⁶
- The Subscriber of such Qualified Certificate held the private key corresponding to the public key within such Qualified Certificate at the time the Qualified Certificate was issued,³⁷
- Where an Managed PKI Customer uses Managed PKI Key Manager to generate an end-user Subscriber key pair, or a CA pregenerates a key pair on an end-user Subscriber hardware token, the public key of such key pair can be used to verify digital signatures created with the corresponding private key,³⁸ and

³⁴ See ETSI Policy Document §§ 6.3, 6.3(a)-(c).

³⁵ See ETSI Policy Document § 6.4.

³⁶ See Directive art. 6(1)(a).

³⁷ See Directive art. 6(1)(b).

³⁸ See Directive art. 6(1)(c).

The CA and/or RA exercises reasonable care to provide notice of the revocation of Qualified Certificates in accordance with CP §§ 4.4.9, 4.4.11.³⁹

Subscriber Agreements shall also contain the foregoing warranties and apply to the extent Subscribers also act as Relying Parties. The required warranty of accuracy of the information contained in a Certificate⁴⁰ is satisfied by compliance with CP § 2.2.1.1.

2.2.1.2 Certification Authority Disclaimers of Warranties

See CP § 2.2.1.2.

2.2.1.3 Certification Authority Limitations of Liability

CAs are entitled to place within a Qualified Certificate a limitation of liability and a limit on the value of the transactions for which the Qualified Certificate can be used.⁴¹ The amount of such a limitation of liability and limit on the value of transactions shall not exceed the limitation of liability applicable either within or outside the context of any warranty plan, whichever is greater, pursuant to CP § 2.2.1.3. The Directive provides that a CA shall not be liable for damages arising from the use of a Qualified Certificate in amounts exceeding the limitation of liability or limit on the value of transactions indicated in the Qualified Certificate.⁴²

2.2.1.4 Force Majeure

No stipulation.

2.2.2 Registration Authority Liability

Server Service Centers and ASB Providers, on behalf of their ASB Customer CAs, shall include within Subscriber Agreements and Relying Party Agreements the warranties required by EDP § 2.2.1.1.⁴³

2.2.3 Subscriber Liability

The liability (and/or limitation thereof) of Subjects and Subscribers complies with ETSI Policy⁴⁴

2.2.4 Relying Party Liability

No stipulation.

³⁹ See Directive art. 6(2).

⁴⁰ See Directive art. 6(1)(a).

⁴¹ See Directive art. 6(3)-(4); ETSI Policy Document § 7.3.3(a).

⁴² See Directive art. 6(3)-(4); ETSI Policy Document § 7.3.3(a), Annex A.

⁴³ :ETSI Policy Document Annex A

⁴⁴ :ETSI Policy Document Annex A

2.3 Financial Responsibility (DL1-2)

2.3.1 Indemnification by Subscribers and Relying Parties

No stipulation.

2.3.2 Fiduciary Relationships

No stipulation⁴⁵

2.3.3 Administrative Processes

The requirement of financial responsibility and adequate errors and omissions insurance as described in CP Sections 9.2.1 and 9.2.2 satisfy the Directive's requirements for financial resources sufficient to meet the Directive's requirements and bear the risk of liability for damages.⁴⁶

2.4 Interpretation and Enforcement (DL1-2)

2.4.1 Governing Law

Pursuant to EDP §§ 2.1.1-2.1.2, and subject to CP § 2.4.1, Subscriber Agreements and Relying Party Agreements shall include a governing law clause specifying the jurisdiction whose law governs the enforceability, construction, interpretation, and validity of such agreements.

Subject to any limits appearing in applicable law⁴⁷, the following laws shall govern the enforceability, construction, interpretation, and validity of this EDP, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in a member state of the European Community, in the following order of precedence:

- a) The legislative acts of the European Council and the European Commission, including but not limited to the Directive, and
- b) Where the foregoing law is silent concerning, or not applicable to, a particular matter relating to a particular Certificate issued within a certain Affiliate's Subdomain, the laws of the jurisdiction in which such Affiliate has established its operations.

This governing law provision applies only to this EDP. Agreements incorporating the EDP by reference may have their own governing law provisions, provided that:

⁴⁵ ETSI Policy Document Annex A (1) C

⁴⁶ See Directive annex II(h); ETSI Policy Document § 7.5(e).

⁴⁷ :See ETSI Policy Document Section 7.3.1. note 11 for factors that are taken into account in identifying "applicable law" are:

- this EDP § 2.4.1 governs the enforceability, construction, interpretation, and validity of the terms of the EDP, and

CP § 2.4.1 governs the enforceability, construction, interpretation, and validity of the terms of the CP separate and apart from the remaining provisions of any such agreements, subject to any limitations appearing in applicable law.

This EDP 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. In specific, the provision of services by a given Affiliate or Customer of an Affiliate is subject to the laws of EU Member Countries interpreting and implementing the Directive, which the EU Member Countries may modify from time to time. Requirements specific to a given EU Member Country shall appear in an Affiliate's CPS.

2.4.2 Severability, Survival, Merger, Notice

No stipulation.

2.4.3 Dispute Resolution Procedures

Affiliates' CPSs and/or agreements shall have policies and procedures for the resolution of complaints and disputes received from Subscribers, Relying Parties, other customers, or other parties about the provisioning of electronic trust services or any other related matters. Affiliates shall ensure that Customers within their Subdomains wishing to approve Certificate Applications for DL1 and DL2 Certificates agree to abide by such dispute resolution procedures.⁴⁸

Pursuant to EDP §§ 2.1.1-2.1.2, Subscriber Agreements and Relying Party Agreements shall include a dispute resolution clause specifying procedures to handle complaints and disputes arising out of such agreements. The dispute resolution clause shall be consistent with CP § 2.4.3.

2.5 Fees (DL1-2)

No stipulation.

2.6 Publication and Repository (DL1-2)

2.6.1 Publication of CA Information

The requirement that VeriSign and Affiliates maintain a publicly-available repository making Certificates available satisfies the requirement for making Certificates available as necessary to Subscribers and Relying Parties.⁴⁹ The requirement that repositories includes revocation information concerning VTN Certificates and the applicable Relying

⁴⁸ See ETSI Policy Document § 7.3.4(a), 7.5(f).

⁴⁹ See Directive annex II(b), (l); ETSI Policy Document § 7.3.5.

Party Agreement in CP § 2.6.1 satisfies the requirement for the availability of publicly and internationally available revocation information (at least until the certificate expires) and relying party terms and conditions.⁵⁰ Revocation services, revocation status information, and Relying Party Agreements shall be available twenty-four (24) hours per day, seven (7) days per week.⁵¹ The Relying Party Agreement shall be readily identifiable within the repository of a VeriSign or an Affiliate.⁵² Upon system failure, or repository service unavailability, or other factors that are not under the control of VeriSign or an Affiliate, VeriSign or an Affiliate shall ensure that repository services are restored within the time limits set forth in CP § 4.8.4, EDP § 4.8.4, and the applicable CPS.

2.6.2 Frequency of Publication

See CP §§ 4.4.9, 4.4.11; EDP §§ 4.4.9, 4.4.11.

2.6.3 Access Controls

The controls imposed by VeriSign and Affiliates to prevent unauthorized persons from adding, deleting, or modifying repository entries under CP § 2.6.3 are intended to protect the integrity and authenticity of Certificate status information pursuant to the ETSI Policy Document.⁵³ More specifically, VeriSign and Affiliates shall use Trustworthy Systems for their repositories holding Qualified Certificates to store them in a verifiable form so that:

- Only authorized persons can make entries or changes,
- Information can be checked for authenticity,
- Qualified Certificates are publicly available for retrieval in only those cases for which the Subscriber's consent has been obtained, and
- Any technical changes resulting in a Compromise of these security requirements are apparent to the operator.⁵⁴

2.6.4 Repositories

No stipulation.

2.7 Compliance Audit (DL1-2)

If a CA or RA wishes to issue or approve the issuance of Qualified Certificates, the Compliance Audit that the CA or RA must undergo annually or whenever a change is made to the CA operations that is deemed a major change to the CA, by an independent qualified auditor under CP § 2.7 shall include a module to determine the CA's or RA's compliance with the applicable portion of the EDP, the QCP public and QCP public + SSCD certificate policies in the ETSI Policy Document, and the

⁵⁰ See Directive annex II(b), (l); ETSI Policy Document §§ 7.3.5(c), (f), 7.3.6, 7.3.6(k).

⁵¹ See ETSI Policy Document §§ 7.3.5(e), 7.3.6(h)-(i).

⁵² See ETSI Policy Document § 7.3.5(d).

⁵³ See ETSI Policy Document § 7.3.6(j); see also Directive annex II(b).

⁵⁴ See Directive annex II(l).

Directive.⁵⁵ In the case of CAs performing self-audits attesting to compliance with the ETSI Policy Document and DL1 or DL2, Customers shall make available to Subscribers and Relying Parties, evidence from the self-audit supporting the claim of compliance. The internal auditor shall be an independent department separate from the department operating the CA. An audit by an independent third party indicating compliance with the ETSI Policy Document and DL1 or DL2 satisfies the requirements of this EDP § 2.7.

If an audit shows significant non-conformance of the CA of the requirements for Qualified certificates, The CA shall remedy the non-conformance within a commercially reasonable time, failing which it shall cease issuing Public Qualified Certificates until such time it can demonstrate or has been assessed as being conformant. The means required to demonstrate conformance may depend on the specific legal requirements of the country where the CA is established.

2.8 Confidentiality and Privacy (DL1-2)

CAs shall comply with the European data protection Directive [4], as implemented through applicable legislation.⁵⁶ In addition, they shall, in accordance with the Directive and ETSI Policy Document,⁵⁷ comply with the requirements of the Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.⁵⁸ They shall also comply with the applicable EU Member Country's information retention legislation and may comply with its legislation to implement accreditation of CAs. VeriSign, Affiliates, and Customers shall collect personal data only directly from the Certificate Applicant, or after the explicit consent of the Certificate Applicant, and only insofar as it is necessary for the purposes of issuing and maintaining the Certificate. The data may not be collected or processed for any other purposes without the explicit consent of the Certificate Applicant.⁵⁹ Information considered confidential and private under applicable privacy policies shall be protected from loss, destruction, damage, falsification, and unauthorized or unlawful processing.⁶⁰

2.8.1 Types of Information to be Kept Confidential and Private

CP § 2.8.1 requires that Certificate Application records shall be kept confidential and private subject to CP §§ 2.8.2, 2.8.4, 2.8.5. This requirement satisfies the requirement that users be assured that the information they provide to CAs shall be protected from disclosure, unless with their agreement, a court order or other legal requirement for disclosure.⁶¹ This requirement shall appear in the privacy policies of Affiliates.

⁵⁵ See ETSI Policy Document § 5.4.1(b).

⁵⁶ See ETSI Policy Document § 7.4.10).

⁵⁷ See Directive art. 8(1); ETSI Policy Document § 7.4.10(b).

⁵⁸ Council Directive 1995/46/EC, 1995 O.J. (L 281) 31.

⁵⁹ See Directive art. 8(2).

⁶⁰ See ETSI Policy Document § 7.4.10(a), (c).

⁶¹ See ETSI Policy Document § 7.4.10(d).

The CA shall also comply with the following data protection issues addressed in the ETSI policy:

- _ Registration⁶²
- _ Confidentiality of records⁶³
- _ Protecting access to personal information⁶⁴
- _ User consent⁶⁵

2.8.2 Types of Information Not Considered Confidential or Private

No stipulation.

2.8.3 Disclosure of Certificate Revocation/Suspension Information

No stipulation.

2.8.4 Release to Law Enforcement Officials

No stipulation.

2.8.5 Release as Part of Civil Discovery

Records concerning Qualified Certificates shall be made available if required for the purposes of providing evidence of certification for the purpose of legal proceedings, subject to applicable privacy and other laws⁶⁶. The subject of the Qualified Certificate, and within the constraints of data protection requirements the subscriber, shall have access to registration and other information relating to the subject.

2.8.6 Disclosure Upon Owner's Request

Subscribers shall have access to registration and other information relating to him or herself.⁶⁷

2.8.7 Other Information Release Circumstances

No stipulation.

2.9 Intellectual Property Rights (DL1-2)

2.9.1 Property Rights in Certificates and Revocation Information

No stipulation.

⁶² See ETSI Policy Document § 7.3.1.

⁶³ See ETSI clauses 7.4.11(a) and 7.3.3(f)

⁶⁴ See ETSI clauses 7.4.6

⁶⁵ See ETSI Policy Document § 7.3.1(i)

⁶⁶ See ETSI Policy Document § 7.4.11(c).

⁶⁷ See ETSI Policy Document § 7.4.11(c).

2.9.2 Property Rights in the CP

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

2.9.3 Property Rights in Names

No stipulation.

2.9.4 Property Rights in Keys and Key Material

No stipulation.

3. Identification and Authentication

3.1 Initial Registration

3.1.1 Types of Names (DL1-2)

No stipulation.

3.1.2 Need for Names to be Meaningful (DL1-2)

Under the Directive, Member Countries shall not *prohibit* CAs from using pseudonyms (names other than a Subscriber's true personal or organizational name) within certificates.⁶⁸ Nonetheless, CAs are not *required* to accept pseudonyms within certificate applications. Pseudonyms are not permitted within Certificates issued under the CP, pursuant to CP § 3.1.2.

3.1.3 Rules for Interpreting Various Name Forms (DL1-2)

No stipulation.

3.1.4 Uniqueness of Names (DL1-2)

The requirement in CP § 3.1.4 that names within a CA's domain are unique satisfies the requirement of the ETSI Policy Document.⁶⁹

3.1.5 Name Claim Dispute Resolution Procedure (DL1-2)

No stipulation.

⁶⁸ Directive art. 8(3).

⁶⁹ See ETSI Policy Document § 7.3.3(e).

3.1.6 Recognition, Authentication, and Role of Trademarks (DL1-2)

No stipulation.

3.1.7 Method to Prove Possession of Private Key (DL1-2)

CP § 3.1.7 requires Certificate Applicants to prove possession of a private key using PKCS #10, another cryptographically-equivalent demonstration, or another VeriSign-approved method, except where a key pair is generated by a CA on behalf of a Subscriber. This CP provision meets the requirement for a CA to ensure that the Subject has possession of the private key corresponding to the public key to be certified, except where a key pair is generated by the CA.⁷⁰

3.1.8 Authentication of Organization Identity (DL1-2)

Where the subject is a person who is identified in association with an organizational entity,

evidence shall be provided of:

- full name and legal status of the associated organizational entity;
- any relevant existing registration information (e.g. company registration) of the organizational entity;
- evidence that the subject is associated with the organizational entity.⁷¹

3.1.9 Authentication of Individual Identity (DL1-2)

The identification and authentication of applicants for DL1 and DL2 Qualified Certificates is based on the direct or indirect personal (physical) presence of the Certificate Applicant before an agent of the CA or Managed PKI Customer, or before a notary public, authorized entity, or other official with comparable authority within the Certificate Applicant's jurisdiction.⁷² During the direct or indirect physical presence of the Certificate Applicant, the agent, notary, authorized entity, or other official shall check the identity of the Certificate Applicant who shall provide evidence of:

full name (including surname and given names consistent with the applicable law and national identification practices);

- date and place of birth, a nationally recognized identity number, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name.⁷³

The agent, notary, authorized entity, or other official shall also validate any other specific attributes of the person indicated in the Qualified Certificate. The validation procedures that CAs and RAs adopt under this EDP § 3.1.8 shall be consistent with applicable national law.⁷⁴

⁷⁰ See ETSI Policy Document § 7.3.1(k).

⁷¹ See ETSI Policy Document 7.3.1 (e)

⁷² See ETSI Policy Document § 7.3.1(c).

⁷³ See ETSI Policy Document § 7.3.1(d).

⁷⁴ See ETSI Policy Document § 7.3.1(c).

The personal physical appearance of the Certificate Applicant before an agent, notary, authorized entity, or other official may be at the time of enrollment for the Qualified Certificate. The ETSI Policy Document refers to this process as checking identity “directly” using means providing assurance of physical presence. Alternatively, the personal physical appearance of the Certificate Applicant may be at a point in time before enrollment. This is the process of checking identity “indirectly” using means providing assurance of physical presence. If validation procedures make use of “indirect” personal presence, during the session involving personal physical presence of the Certificate Applicant, the agent, notary, authorized entity, or other official shall, upon successful authentication, provide the Certificate Applicant with documentation, either paper or electronic, that the Certificate Applicant can later submit in connection with the Certificate Application as evidence of identity.⁷⁵

3.2 Routine Rekey (Renewal) (DL1-2)

As a condition of approving the renewal of a Qualified Certificate, the applicable CA or RA shall check that the information used to verify the identity of the Subject is still valid.⁷⁶ This procedure is for the purpose of ensuring that the person seeking to renew a Qualified Certificate is in fact the Subject of the Certificate, as required by CP § 3.2.1.⁷⁷ If any certified names or attributes have changed, or the previous certificate has been revoked, the registration information must be verified, recorded and agreed to by the subscriber in accordance with ETSI Policy Document clause 7.3.1 c) to g). The CA shall issue a new certificate using the subject's previously certified public key, only if its cryptographic security is still sufficient for the new certificate's validity period and no indications exist that the subject's private key has been compromised.

3.3 Rekey After Revocation (DL1-2)

As a condition of approving the rekeying a Qualified Certificate after revocation, the applicable CA or RA shall check that the information used to verify the identity of the Subject is still valid.⁷⁸ This procedure is for the purpose of ensuring that the person seeking to rekey is in fact the Subject of the Certificate, as required by CP § 3.3.⁷⁹

3.4 Revocation Request (DL1-2)

The requirement that revocation requests be authorized and validated is satisfied by compliance with CP § 3.4.⁸⁰

⁷⁵ See ETSI Policy Document § 7.3.1(c).

⁷⁶ See ETSI Policy Document § 7.3.2(a).

⁷⁷ See Directive annex II(d), (g); ETSI Policy Document § 7.3.2.

⁷⁸ See ETSI Policy Document § 7.3.2(a).

⁷⁹ See Directive annex II(d); ETSI Policy Document § 7.3.2.

⁸⁰ See ETSI Policy Document §§ 7.3.6, 7.3.6(c).

4. Operational Requirements

4.1 Certificate Application (DL1-2)

4.1.1 Certificate Applications for End-User Subscriber Certificates

The enrollment process for Qualified Certificate is in accordance with CP § 4.1.1, subject to the following clarifications:

- The Subscriber Agreement, to which Certificate Applicants manifest assent, shall be communicated in accordance with EDP §§ 2.1.1, 2.1.2,⁸¹
- The Certificate Applicant shall present evidence of identity consistent with EDP § 3.1.9,⁸² and
- The enrollment information provided in the Certificate Application shall include a physical address, or other attributes, that enable the CA or RA to contact the Certificate Applicant.⁸³

Records retained in accordance with EDP § 4.6 shall include the information used to authenticate the Subject's identity (including any reference number on the documentation used for authentication and any limitations on its validity)⁸⁴ and a record of the signed subscriber agreement, whether in paper or electronic form, wherein the Subscriber inter alia consents to the keeping of a record by the CA of information used in registration and include all other consents required in ETSI Policy Document Section 7.3.1.⁸⁵

In the case of an application for renewal or rekeying:

- Any changes in the terms of the Subscriber Agreement following the previous enrollment or re-enrollment shall be communicated in accordance with EDP §§ 2.1.1, 2.1.2, and
- Records retained under EDP § 4.6 shall also include the Subscriber's assent to any such changes.⁸⁶

4.1.2 Certificate Applications for CA or RA Certificates

No stipulation.

⁸¹ See ETSI Policy Document § 7.3.1(a)-(b).

⁸² See ETSI Policy Document § 7.3.1(d).

⁸³ See ETSI Policy Document § 7.3.1(h).

⁸⁴ See ETSI Policy Document § 7.3.1(f).

⁸⁵ See ETSI Policy Document § 7.3.1(i); see also ETSI Policy Document § 7.3.1(j).

⁸⁶ See ETSI Policy Document § 7.3.2(b)-(c).

4.2 Certificate Issuance (DL1-2)

4.2.1 Issuance of Qualified Certificates

The requirement of issuing Certificates following approval of Certificate Applications under CP § 4.2.1 meets the requirement in the ETSI Policy Document of making Certificates available following issuance.⁸⁷ The Certificates generated and issued in accordance with CP § 4.2.1 shall be issued by systems utilizing safeguards against forgery detailed in CP § 6 and EDP § 6 and that ensure that the Certificate is issued to the Certificate Applicant, or applicant for renewal or rekeying, holding the private key corresponding to the public key in the Certificate to be issued.⁸⁸

The issuance of Certificates under EDP § 3.2 is, as a technical matter, rekeying rather than a recertification of a previously-certified public key.⁸⁹

4.2.2 Issuance of CA and RA Certificates

Before enabling a potential Affiliate or Customer to begin operations, its potential Superior Entity shall ensure that the organization of the potential Affiliate or Customer is reliable.⁹⁰ More particularly, the Superior Entity shall not permit a potential Affiliate or Customer to begin operations until the Superior Entity has confirmed that the potential Affiliate or Customer:

- Can satisfy the personnel controls of CP § 5.3 and EDP § 5.3, including their non-discrimination requirement and training requirements,⁹¹
- Is obligated to make its services available to all applicants whose activities fall within its declared field of operation,⁹²
- Is a legal entity,⁹³ which shall be confirmed as part of the authentication of the potential CA or RA organization,⁹⁴
- Has a system or systems for quality and information security management appropriate for the certification services it is providing,⁹⁵ which, in the case of potential Affiliates, shall be confirmed as part of a Security and Practices Review performed under the CP,⁹⁶
- Can meet the financial responsibility obligations of CP § 2.3 and EDP § 2.3,⁹⁷
- Can meet the dispute resolution requirements of EDP § 2.4.3,⁹⁸

⁸⁷ See ETSI Policy Document § 7.3.5(a).

⁸⁸ See Directive annex II(g); ETSI Policy Document §§ 7.3.3, 7.3.3(b)-(c).

⁹⁰ See Directive annex II(a); ETSI Policy Document § 7.5.

⁹¹ See ETSI Policy Document § 7.5(a), 7.4.3(a)

⁹² See ETSI Policy Document § 7.5(b).

⁹³ See ETSI Policy Document § 7.5(c).

⁹⁴ See CP § 3.1.8.2.

⁹⁵ See ETSI Policy Document § 7.4.1(d).

⁹⁶ See CP § 2.7.

⁹⁷ See ETSI Policy Document § 7.5(d)-(e).

⁹⁸ See ETSI Policy Document § 7.5(f).

- In the case of Affiliates, has a properly documented agreement and contractual relationship in place with its Superior Entity,⁹⁹ and
- Is not known to have been convicted of criminal wrongdoing or adjudged to be liable in a civil case, where such conviction or adjudication casts serious doubts on the trustworthiness of the potential Affiliate or Customer.

4.3 Certificate Acceptance (DL1-2)

No stipulation.

4.4 Certificate Suspension and Revocation (DL1-2)

Subscribers are required to notify the CA and request revocation of a Qualified Certificate whenever there has been a compromise, or suspected compromise of the private key, or whenever the certificate content is no longer accurate. The ETSI Policy Document does not set more specific requirements relating to circumstances for revocation, who may request revocation, procedures for revocation requests and processing, and the choice of mechanism for distributing Certificate status information. Rather, it simply requires that CAs document these practices in a CPS,¹⁰⁰ which Affiliates do in accordance with CP § 8.3.

4.4.1 Circumstances for Revocation

No stipulation.

4.4.2 Who Can Request Revocation

No stipulation.

4.4.3 Procedure for Revocation Request

CAs and RAs shall process requests and reports relating to revocation upon receipt.¹⁰¹ When a Subscriber or Subject uses a Challenge Phrase to request revocation, this requirement is met because the Certificate is automatically revoked upon validation of the revocation request. The subject (and where applicable the subscriber) whose Certificate was revoked shall be informed of the revocation.¹⁰² Certificates that are revoked shall not be reinstated as valid Certificates.¹⁰³

4.4.4 Revocation Request Grace Period

No stipulation.

⁹⁹ See ETSI Policy Document § 7.5(g).

¹⁰⁰ See ETSI Policy Document § 7.3.6(a).

¹⁰¹ See ETSI Policy Document § 7.3.6(b).

¹⁰² See ETSI Policy Document § 7.3.6(e).

¹⁰³ See ETSI Policy Document § 7.3.6(f).

4.4.5 Circumstances for Suspension

Not applicable.

4.4.6 Who Can Request Suspension

Not applicable.

4.4.7 Procedure for Suspension Request

Not applicable.

4.4.8 Limits on Suspension Period

Not applicable.

4.4.9 CRL Issuance Frequency (If Applicable)

The requirement in CP § 4.4.9 that CRLs for end-user Subscriber Certificates shall be issued at least once per day meets the daily CRL-issuing requirement of the ETSI Policy Document.¹⁰⁴ CRLs shall be signed either by the CA that issued the Certificate or by another authority of the CA meeting the requirements of CP § 6 and EDP § 6.¹⁰⁵ A new CRL may be published before the stated time of the next CRL to be issued.¹⁰⁶

4.4.10 Certificate Revocation List Checking Requirements

No stipulation.

4.4.11 On-Line Revocation/Status Checking Availability

No stipulation.

4.4.12 On-Line Revocation Checking Requirements

No stipulation.

4.4.13 Other Forms of Revocation Advertisements Available

No stipulation.

4.4.14 Checking Requirements for Other Forms of Revocation Advertisements

No stipulation.

¹⁰⁴ See ETSI Policy Document § 7.3.6(g).

¹⁰⁵ See ETSI Policy Document § 7.3.6(g).

¹⁰⁶ See ETSI Policy Document § 7.3.6(g).

4.4.15 Special Requirements Regarding Key Compromise

No stipulation.

4.5 Security Audit Procedures (DL1-2)

Security audit procedures are invoked at system startup, and cease only at system shutdown. The requirement that audit logs contain the date and time of events meets the time recordation requirement of the Directive and the ETSI Policy Document.¹⁰⁷

4.5.1 Types of Events Recorded

When Processing Centers, Service Center, Managed PKI Customers, and Gateway Customers meet the requirements placed on them by subsections within CP § 4.5.1 to maintain logs of auditable events, they satisfy the requirements of the ETSI Policy Document for the logging of:

- All events relating to the lifecycle of Qualified Certificates, including those relating to initial registration, rekeying, or renewal and those relating to requests and reports relating to revocation and responses thereto,¹⁰⁸ and
- All events relating to the lifecycle of CA keys.¹⁰⁹
- In addition, Processing Centers generating RA or end-user Subscriber key pairs for placement on tokens and Managed PKI Customers using Managed PKI Key Manager shall log all events relating to the lifecycle of keys managed by such CAs.¹¹⁰ If applicable, CAs issuing DL2 Certificates shall log all events relating to the preparation of SSCDs.¹¹¹

The events and data logged shall be documented.¹¹² The retention of event logs as provided in CP § 4.5 and EDP § 4.5 facilitates holding personnel accountable for their activities.¹¹³

4.5.2 Frequency of Processing Log

The requirement of monitoring facilities in CP § 5.4.2 meets the requirement for such facilities to detect, register, and react in a timely manner upon any unauthorized and/or irregular attempts to access CA/RA system resources.¹¹⁴

¹⁰⁷ See Directive annex II(c); ETSI Policy Document § 7.4.11(d).

¹⁰⁸ See Directive annex II(i); ETSI Policy Document §§ 7.4.11, 7.4.11(h), (l), (o).

¹⁰⁹ See ETSI Policy Document § 7.4.11(k).

¹¹⁰ See ETSI Policy Document § 7.4.11(m).

¹¹¹ See ETSI Policy Document § 7.4.11(n).

¹¹² See ETSI Policy Document § 7.4.11(g).

¹¹³ See ETSI Policy Document § 7.4.6(f).

¹¹⁴ See ETSI Policy Document § 7.4.6(i), (k).

4.5.3 Retention Period for Audit Log

Unless the laws of a CAs jurisdiction require otherwise, the retention for the audit log shall be in accordance with the VTN CP Section 5.5.2¹¹⁵.

4.5.4 Protection of Audit Log

The retention of audit logs in offsite storage under CP § 4.6.4 and the implementation of mechanisms to protect the log files from unauthorized viewing, modification, deletion, or other tampering under CP § 4.5.4 meets the integrity requirements of the ETSI Policy Document.¹¹⁶

4.5.5 Audit Log Backup Procedures

No stipulation.

4.5.6 Audit Collection System

No stipulation.

4.5.7 Notification to Event-Causing Subject

No stipulation.

4.5.8 Vulnerability Assessments

No stipulation.

4.6 Records Archival (DL1-2)

4.6.1 Types of Events Recorded

The requirement for Affiliates performing front-end functions, Managed PKI Customers, Gateway Customers, and ASB Providers to retain evidence relating to the identity of Subscribers in CP § 4.6.1 includes a requirement to retain the following information in connection with Certificate Applications for Qualified Certificates:

- all the information used to verify the subjects' identity and, if applicable, any specific attributes of the subject, including any reference number on the documentation used for verification, and any limitations on its validity;
- The identity of the Affiliate, Managed PKI Customer, Gateway Customer, or ASB Provider that receives and accepts Certificate Applications; and
- A validation plan showing the methods used to validate identification documents.¹¹⁷

¹¹⁵ See ETSI Policy Document § 7.4.11

¹¹⁶ See ETSI Policy Document § 7.4.11(f).

¹¹⁷ See ETSI Policy Document § 7.4.11(i).

In addition, Affiliates, Managed PKI Customers, Gateway Customers, and ASB Providers approving Certificate Applications for Qualified Certificates shall retain records of the following information:

- The storage location of Certificate Applications and identification documents, including any signed Subscriber Agreements, and
- Any specific choices indicated on Subscriber Agreements, such as consent to publish the Certificate, if it is not already indicated in the text of such Subscriber Agreements.¹¹⁸

4.6.2 Retention Period for Archive

The Directive and ETSI Policy Document do not set a specific record retention period requirement, although the retention period requirement of CP § 5.5.2 is likely sufficient to meet the appropriateness requirement of the ETSI Policy Document.¹¹⁹ This section is subject to any applicable Member Country-specific record retention requirements.

4.6.3 Protection of Archive

The protections of archived records against unauthorized viewing, modification, deletion, or other tampering by storage within a Trustworthy System meets the confidentiality and integrity requirements of the ETSI Policy Document.¹²⁰ The records retention requirements of section 4.6 shall be subject to the privacy and confidentiality requirements of CP § 2.8 and EDP § 2.8 and the data protection legislation within the different member states of the EU.¹²¹

4.6.4 Archive Backup Procedures

No stipulation.

4.6.5 Requirements for Time-Stamping of Records

See EDP § 4.5.

4.6.6 Archive Collection System

No stipulation.

4.6.7 Procedures to Obtain and Verify Archive Information

No stipulation.

4.7 Key Changeover (Renewal) (DL1-2)

No stipulation.

¹¹⁸ See ETSI Policy Document § 7.4.11(i).

¹¹⁹ See Directive annex II(i); ETSI Policy Document §§ 7.3.1(i), 7.4.11(e).

¹²⁰ See ETSI Policy Document § 7.4.11(a)-(b); see also ETSI Policy Document § 7.4.10(a), (c), see also 7.4.6

¹²¹ See ETSI Policy Document § 7.4.11(a)-(b), (j).

4.8 Compromise and Disaster Recovery (DL1-2)

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

The incident and Compromise reporting and handling requirements of VTN CP § 5.7.1 meet the corresponding requirements of the ETSI Policy Document.¹²²

4.8.2 Entity Public Key is Revoked

The notice requirements under CP § 4.8.2 following a compromise of the CA's private key and subsequent revocation of the CA's Certificate meet the notice requirements of the ETSI Policy Document.¹²³ In the case of compromise, the CA shall at a minimum provide the following undertakings:

- That it will take commercially reasonable steps to inform all subscribers and other entities with which the CA has agreements or other form of established relations. In addition, this information shall be made available to other relying parties.
- That it will take commercially reasonable steps to indicate that certificates and revocation status information issued using this CA key may no longer be valid.

4.8.3 Entity Key is Compromised

The requirement of revoking a CA Certificate following a Compromise of the CA's private key under CP § 4.8.4 satisfies the revocation requirement of the ETSI Policy Document.¹²⁴

Should the encryption algorithm used by the CA or its Subscribers be proved to be compromised to such an extent to make it insufficient for its intended remaining usage then the CA shall inform subscribers and relying parties and shall migrate away from using that CA to sign certificates. In appropriate circumstances the CA will be revoked.

CA systems data necessary to resume CA operations shall be backed up and stored in safe places suitable to allow the CA to timely resume operations in case of incident/disasters. Back-up and restore functions shall be performed by the relevant trusted roles and procedures

4.8.4 Secure Facility After a Natural or Other Type of Disaster

Disaster recovery plans required by CP § 4.8.4 shall address the Compromise or suspected Compromise of the authoring entity's private key as a disaster.¹²⁵ The requirement that Processing Centers must restore certain operations within twenty-four (24) hours following a disaster and that Processing Centers and Service Centers restore

¹²² See ETSI Policy Document § 7.4.5(b), (h),(i),(j)

¹²³ See ETSI Policy Document § 7.4.8(d).

¹²⁴ See ETSI Policy Document § 7.4.8(d)

¹²⁵ See ETSI Policy Document § 7.4.8(d); *see also* Directive annex II(a).

all functions within one week satisfies the requirement in the ETSI Policy Document to restore operations “as soon as possible” after a disaster.¹²⁶ Such operations include:

- Certificate issuance (including publication for purposes of dissemination),
- Certificate revocation, and
- Publication of revocation information.

4.9 CA Termination (DL1-2)

When a CA is going to be terminated, such CA shall ensure that potential disruptions to Subscribers and Relying Parties resulting from the cessation of the CA’s services are minimized.¹²⁷ Such CA shall implement a termination plan required under CP § 4.9, which shall include:

- Providing notice to all parties affected by the termination, such as (other) CA’s, Subscribers, Relying Parties, and Subjects,
- The termination of the CA’s authorization to RAs and CMAs acting on behalf of the CA,
- The revocation of the Certificate issued to the CA by the Superior Entity,
- The transfer of the CA’s archives (including revocation status information) and records to a successor entity and the retention of such archives and records for the time periods required in CP § 4.6, and
- The destruction of the CA private keys under CP § 6.2.9.2.¹²⁸
- Termination of the authorization of administrators to act on behalf of the CA in the performance of any functions related to the process of issuing certificates

Such CAs shall have an arrangement to cover the costs of complying with this section in the event the CA becomes bankrupt or for other reasons is unable to cover the costs by itself.¹²⁹ Affiliates’ CPS shall implement the foregoing requirements and shall state whether unexpired unrevoked certificates will be revoked in connection with the termination.¹³⁰

5. Physical, Procedural, and Personnel Security Controls (DL1-2)

The requirement in CP § 5 that all entities performing CA and RA functions draft, implement, and enforce a security policy satisfies the ETSI Policy Document’s requirement for writing and publishing an information security policy.¹³¹ Such security policies shall include administrative and management procedures, appropriate for the certification services it is providing, that correspond to recognized standards, as more particularly set forth in CP § 5 and this EDP § 5.¹³² Also, the security infrastructure needed to implement the security policy and manage security shall be maintained at all

¹²⁶ See ETSI Policy Document § 7.4.8; see also ETSI Policy Document §§ 7.3.5(e), 7.3.6(h), (i).

¹²⁷ See ETSI Policy Document § 7.4.9; see also Directive annex II(a).

¹²⁸ See ETSI Policy Document § 7.4.9(a); see also Directive annex II(i).

¹²⁹ See ETSI Policy Document § 7.4.9(b).

¹³⁰ See ETSI Policy Document § 7.4.9(c).

¹³¹ See ETSI Policy Document §§ 7.4.1(f),

¹³² See Directive annex II(e); ETSI Policy Document § 7.4.1.

times. Any changes to the security policy or infrastructure implementing it that will impact the level of security provided shall be approved by a management forum of the CA or RA in charge of security.¹³³

CA and RA security personnel shall be responsible for implementing their respective security policies. Such personnel shall be organizationally separate from personnel performing normal operations. In addition, security personnel shall be responsible for security oversight over the performance of:

- Operational procedures and responsibilities;
- Secure systems planning and acceptance;
- Protection from malicious software;
- Housekeeping;
- Network management;
- Active monitoring of audit journals, event analysis, and followup;
- Media handling and security; and
- Data and software exchange.¹³⁴

Some of these functions may be delegated to non-specialist operational personnel under the oversight of security personnel in accordance with the applicable security policy.¹³⁵ Ultimately, however, senior management of the CA or RA has the responsibility for ensuring that its practices, including security practices, are properly implemented.¹³⁶

5.1 Physical Controls

5.1.1 Site Location and Construction

The site location and construction requirements of CP § 5.1.1, which implement the requirements of the Security and Audit Requirements Guide and the Enterprise Security Guide, meet the ETSI Policy Document's requirements of physical protection within clearly defined security perimeters around the Certificate generation, Subscriber device provision, and revocation management services.¹³⁷ These site location parameters, coupled with access controls under CP § 5.1.2, are controls implemented to avoid loss, damage, theft, or Compromise of information, information processing facilities, or other assets, and to avoid interruption of business activities.¹³⁸ These controls also protect against equipment, information, media, and software relating to CA services being taken offsite without authorization.¹³⁹

¹³³ See ETSI Policy Document § 7.4.1(e).

¹³⁴ See ETSI Policy Document § 7.4.5(k).

¹³⁵ See ETSI Policy Document § 7.4.5(k).

¹³⁶ See ETSI Policy Document § 7.1(f).

¹³⁷ See ETSI Policy Document § 7.4.4(f).

¹³⁸ See ETSI Policy Document § 7.4.4(b)-(c); see also ETSI Policy Document § 7.4.4(g).

¹³⁹ See ETSI Policy Document § 7.4.4(h).

The placement of Information Services systems needed to support CA/RA functions in at least Tier 3 space under CP § 5.1.1 is consistent with the requirement to keep local network components in a physically secure environment.¹⁴⁰

5.1.2 Physical Access

The physical access control measures required by CP § 5.1.2 meet the access control requirement in the ETSI Policy Document.¹⁴¹ CAs pregenerating keys on SSCDs shall generate such keys within Tier 4 space and shall, prior to distributing such tokens, store them in Tier 5 space.

5.1.3 Power and Air Conditioning

Environmental controls for power and air conditioning, water exposures, and fire prevention and detection meet some of the requirements of the ETSI Policy Document. In addition, Affiliates and Customers performing CA and RA functions shall provide environmental controls addressing telecommunications failures, structural collapse, and natural disasters.¹⁴²

5.1.4 Water Exposures

See EDP § 5.1.3.

5.1.5 Fire Prevention and Protection

See EDP § 5.1.3.

5.1.6 Media Storage

The media handling controls of CP § 5.1.6 satisfy the ETSI Policy Document's media security requirements.¹⁴³ As far as commercially reasonable, media management procedures shall protect against obsolescence and deterioration of media within the period of time that records are required to be retained.

5.1.7 Waste Disposal

The waste disposal controls of CP § 5.1.7 satisfy the ETSI Policy Document's media disposal security requirement.¹⁴⁴

5.1.8 Off-Site Backup

No stipulation.

¹⁴⁰ See ETSI Policy Document § 7.4.6(h).

¹⁴¹ See ETSI Policy Document § 7.4.4(a), (d).

¹⁴² See ETSI Policy Document § 7.4.4(g).

¹⁴³ See ETSI Policy Document § 7.4.5(c), (f).

¹⁴⁴ See ETSI Policy Document § 7.4.5(c), (f).

5.2 Procedural Controls

VeriSign, Affiliates, and Customers shall assess business and security risks and ensure that their systems are secure and correctly operated, with minimal risk of failure.¹⁴⁵

VeriSign, Affiliate, and Customer personnel shall perform administrative and management procedures and processes in accordance with their respective security policies.¹⁴⁶

5.2.1 Trusted Roles

The security policies of VeriSign, Affiliates, and Customers shall clearly identify trusted roles.¹⁴⁷ The CA shall employ a sufficient number of trusted personnel which possess the expert knowledge, experience and qualifications necessary for the offered services and as appropriate to the job function. CA/RA personnel hired to become Trusted Persons filling Trusted Positions shall have job descriptions defined (including where possible skills and experience requirements) and be formally appointed pursuant to personnel security practices approved by senior management responsible for security.¹⁴⁸

Trusted Positions shall include:

- Security personnel who administer the implementation of security practices;
- Administrators who approve Certificate Applications or the revocation of Certificates;
- System administrators, who install, configure, and maintain CA or RA Trustworthy Systems for enrollment, Certificate issuance, SSCD provision, and revocation management;
- System operators, who are responsible for operating CA or RA Trustworthy Systems on a day-to-day basis and who are authorized to perform system backups and recoveries; and
- System auditors, who are authorized to view and maintain archives and audit logs of the CA or RA trustworthy systems.¹⁴⁹

VeriSign, Affiliates, and Customers shall establish and implement procedures for all Trusted Positions and administrative roles that have an impact on the provision of their services.¹⁵⁰

5.2.2 Number of Persons Required Per Task

Security roles and responsibilities, as specified in VeriSign's, Affiliates', and Customers' security policies, shall be documented in job descriptions.¹⁵¹ Such job descriptions

¹⁴⁵ See Directive annex II(e); ETSI Policy Document § 7.4.5.

¹⁴⁶ See ETSI Policy Document § 7.4.3(e).

¹⁴⁷ See ETSI Policy Document § 7.4.3(c).

¹⁴⁸ See ETSI Policy Document § 7.4.3(i).

¹⁴⁹ See ETSI Policy Document § 7.4.3(h).

¹⁵⁰ See ETSI Policy Document § 7.4.5(e).

¹⁵¹ See ETSI Policy Document § 7.4.3(c).

support the requirement of the segregation of duties based on job responsibilities of CP § 5.2.2. Such descriptions shall also be drafted to support the security concept of “least privilege,” or ensuring that personnel shall be given the lowest level of privileges needed to perform their job functions.¹⁵²

5.2.3 Identification and Authentication for Each Role

The identification and authentication requirement in CP § 5.2.3 satisfies the corresponding requirement in the ETSI Policy Document.¹⁵³

5.3 Personnel Controls

VeriSign, Affiliates, and Customers shall ensure that their personnel and hiring practices enhance and support the trustworthiness of their services.¹⁵⁴ VeriSign, Affiliates, and Customers shall employ a sufficient number of personnel necessary to provide their services in the context of the type, range, and volume of work performed.¹⁵⁵

VeriSign, Affiliate, and Customer personnel holding Trusted Positions, senior executives, and senior staff members shall be free from conflicting interests, such as commercial, financial, or other pressures, that might prejudice the impartiality of their operations or adversely influence trust in the services they provide.¹⁵⁶ The organization within VeriSign, Affiliates, and Customers into which Administrators or other personnel performing Certificate generation and revocation management are hired shall be independent of other organizations in connection with the decisions of such Administrators or other personnel relating to establishing, provisioning, revoking, and maintaining services.¹⁵⁷ The parts of the organization of VeriSign, Affiliates, and Customers concerned with Certificate generation and revocation management shall have a documented structure that safeguards the impartiality of operations.¹⁵⁸

VeriSign, Affiliates, and Customers shall develop and utilize in their hiring practices job descriptions developed to support the separation of duties, least privilege concept, determining position sensitivity based on duties and access levels, background screening, and employee training and awareness. Where appropriate, such job descriptions shall differentiate between general functions and CA/RA-specific functions and shall include skill and experience requirements.¹⁵⁹

To the extent that it is commercially reasonable, managerial personnel shall be employed who possess experience or training in electronic signature technology and familiarity with security procedures for personnel with security responsibilities and

¹⁵² See ETSI Policy Document § 7.4.3(d).

¹⁵³ See ETSI Policy Document § 7.4.6(e).

¹⁵⁴ See Directive annex II(e); ETSI Policy Document § 7.4.3.

¹⁵⁵ See ETSI Policy Document § 7.4.3(a)

¹⁵⁶ See ETSI Policy Document §§ 7.4.3(g), 7.5(h)

¹⁵⁷ See ETSI Policy Document 7.5(h)

¹⁵⁸ See ETSI Policy Document 7.5(i)

¹⁵⁹ See ETSI Policy Document § 7.4.3(d).

experience with information security and risk assessment sufficient to carry out management functions. Managerial personnel not possessing such experience or training will be trained by the CA to the extent necessary to perform their managerial duties.

5.3.1 Background, Qualifications, Experience, and Clearance Requirements

The background, qualifications, and experience requirements of CP § 5.3.1 satisfy the ETSI Policy Document's corresponding requirements.¹⁶⁰ In addition, managerial personnel hired by VeriSign, Affiliates, and Customers shall possess expertise or receive on-the-job training in Electronic Signature technology and familiarity with security procedures for personnel with security responsibilities.¹⁶¹

5.3.2 Background Check Procedures

Subject to limitations imposed by local law, the background check procedures required by CP § 5.3.2 will uncover criminal convictions. VeriSign, Affiliates, and Customers shall not appoint to Trusted Positions any person who is known to have a conviction for a serious crime or other offence that affects his or her suitability for the position for which he or she is a candidate. Any person shall not have access to the responsibilities or privileges granted to a Trusted Position until all background checks are completed.¹⁶² Where local law precludes VeriSign, Affiliates, or Customers from obtaining information on criminal convictions, they are (subject to applicable law) entitled to ask candidates for Trusted Positions or management roles to provide such information, and candidates' refusal to provide such information shall be grounds for cancellation of offers of employment or the termination of existing personnel undergoing a periodic post-hiring background check.¹⁶³

5.3.3 Training Requirements

The requirement in CP § 5.3.3 for on-the-job training facilitates the fulfillment of the personnel knowledge, experience, and qualifications requirements of the ETSI Policy Document.¹⁶⁴

5.3.4 Retraining Frequency and Requirements

No stipulation.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

¹⁶⁰ See ETSI Policy Document §§ 7.4.3(a),

¹⁶¹ See ETSI Policy Document § 7.4.3(f).

¹⁶² See ETSI Policy Document § 7.4.3(j).

¹⁶³ See ETSI Policy Document § 7.4.3(i) note 4.

¹⁶⁴ See ETSI Policy Document § 7.4.3(a).

5.3.6 Sanctions for Unauthorized Actions

Appropriate disciplinary sanctions shall be applied to personnel violating CA policies or procedure.

5.3.7 Contracting Personnel Requirements

VeriSign, Affiliates, or Customers may use independent contractors to fill Trusted Positions pursuant to CP § 5.3.7. Nonetheless, they shall remain responsible for conformance with the procedures prescribed by this EDP.¹⁶⁵

5.3.8 Documentation Supplied to Personnel

The documentation that VeriSign, an Affiliate, or a Customer provides to its personnel pursuant to CP § 5.3.8 shall include its information security policy.¹⁶⁶

6. Technical Security Controls

VeriSign, Affiliates, and Customers shall use Trustworthy Systems and products that are protected against modification and ensure the technical and cryptographic security of the processes supported by them.¹⁶⁷ In so far as reasonably possible, the security controls listed below form part of the audit requirements in Section 2.7

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation (DL1-2)

Processing Centers shall generate CA keys in Tier 4 or greater space consistent with CP § 5.1.1 by Trusted Persons in accordance with multi-person control required by CP § 6.2.2. The personnel authorized to generate CA keys shall be limited to those who are required to do so consistent with their security and key generation policies.¹⁶⁸ Processing Centers shall generate CA keys in devices meeting the requirements of EDP § 6.2.1.¹⁶⁹ Affiliates requiring Common Criteria rated hardware use EAL 4+ rated version devices. The devices used by VeriSign meet the requirements of FIPS 140 Level 3.

For DL2 Certificates, if the Subject's keys are generated under control of the subscriber or subject, it shall be generated within the SSCD to be used for signing;¹⁷⁰

Where Processing Centers pregenerate end-user Subscriber keys on tokens, including SSCDs, or Client Managed PKI Customers using Managed PKI Key Manager use the

¹⁶⁵ See ETSI Policy Document § 6.1.

¹⁶⁶ See ETSI Policy Document § 7.4.1(c).

¹⁶⁷ See Directive annex II(f), (l); ETSI Policy Document § 7.4.7.

¹⁶⁸ See ETSI Policy Document § 7.2.1(a).

¹⁶⁹ See ETSI Policy Document § 7.2.1(b).

¹⁷⁰ See ETSI Policy Document § 6.2(f).

Managed PKI Key Manager Software to generate keys on behalf of end-user Subscribers, the Processing Center or Client Managed PKI Customer shall ensure that such keys are generated securely and the privacy of the Subject's private key is assured.¹⁷¹ One way in which this requirement may be met is using a suitable protection profile, defined in accordance with ISO 15408 or its equivalent.¹⁷²

Article 9 of the Directive establishes an "Electronic-Signature Committee" to assist the European Commission.¹⁷³ A proposal exists currently for the establishment of a cryptographic advisory panel to assist the Committee.¹⁷⁴ Under that proposal, the panel would determine appropriate algorithms for generating CA signing keys, for CA signing operations using CA keys, and end-user Subscriber signing operations using Subscriber keys.¹⁷⁵ The determination of appropriate algorithms will inform requirements in the ETSI Policy Documents that CA signing keys and end-user Subscriber signing keys be generated using, and shall be used with, algorithms that are "recognized as being fit for the purposes of qualified electronic signatures."¹⁷⁶ Until the panel determines which algorithms are appropriate for the purposes of Qualified Electronic Signatures, the Directive and ETSI Policy Document have no specific requirement for the use of certain algorithms for CA or end-user Subscriber signing keys.

6.1.2 Private Key Delivery to Entity

6.1.2.1 Private Key Delivery to Entity – DL1

This section applies where Client Managed PKI Customers using Managed PKI Key Manager use the Managed PKI Key Manager Software and Trustworthy Systems to deliver private keys to Subscribers or where private keys are pre-generated on hardware tokens that do not meet the requirements placed on SSCDs, making the Qualified Certificates certifying the public keys corresponding to such private keys ineligible to be DL2 Certificates. The requirements of CP § 6.1.2 to protect such private keys meet the requirements placed on CA-generated Subscriber keys in the ETSI Policy Document.¹⁷⁷ The subject's private key shall be delivered to the subject, if required via the subscriber, in a manner such that the secrecy and the integrity of the key is not compromised and, once delivered to the subject, the private key can be maintained under the subject's sole control.

6.1.2.2 Private Key and SSCD Delivery to Entity – DL2

This section applies where private keys are pre-generated on SSCDs in connection with the issuance of DL2 Certificates. The requirements of CP § 6.1.2 to protect such

¹⁷¹ See ETSI Policy Document § 7.2.9; see also Directive annex II(f), (g), (j).

¹⁷² See ETSI Policy Document § 7.2.9 note 3.

¹⁷³ See Directive art. 9(1)

¹⁷⁴ See ETSI Policy Document §§ 6.2(d) note 1, , 7.2.8(b) note 1.

¹⁷⁵ See ETSI Policy Document §§ 6.2(d) note 1, 7.2.1(c), (d) note 2, 7.2.8(b) note

¹⁷⁶ ETSI Policy Document §§ 6.2(d), 7.2.1(c)-(d), 7.2.8(a)-(b); see also ETSI Policy Document § 7.2.1. See generally Directive annex II(f).

¹⁷⁷ See ETSI Policy Document § 7.2.8(c)-(d).

private keys meet the requirements placed on CA-generated Subscriber keys in the ETSI Policy Document.¹⁷⁸

In addition, however, regardless of whether the Subscriber or the CA generates the keys on the SSCD:

- SSCD preparation shall be securely controlled by the CA,
- SSCDs shall be securely stored and distributed,
- SSCD deactivation and reactivation shall be securely controlled, and
- Where the SSCD has associated activation data (e.g., a PIN), the activation data shall be securely prepared and distributed separately from the SSCD, for example by using different delivery times or routes.¹⁷⁹

When delivered by the Subscriber, the subject's SSCD shall be delivered to the subject in a manner such that the secrecy and the integrity of the private key is not compromised and, once delivered to the subject, the private key can be maintained under the subject's sole control.

6.1.3 Public Key Delivery to Certificate Issuer (DL1-2)

No stipulation.

6.1.4 CA Public Key Delivery to Users (DL1-2)

The CA public key delivery requirements of CP § 6.1.4 meet the requirements of the ETSI Policy Document.¹⁸⁰

6.1.5 Key Sizes (DL1-2)

The cryptographic advisory panel to assist the Electronic-Signature Committee referred to in EDP § 6.1.1 may, under the proposal to create the panel, determine appropriate key lengths for CA signing keys and end-user Subscriber signing keys.¹⁸¹ The determination of appropriate key lengths will inform requirements in the ETSI Policy Documents that CA signing keys and end-user Subscriber signing keys have lengths that are “recognized as being fit for the purposes of qualified electronic signatures.”¹⁸² Until the panel determines which key lengths are appropriate for the purposes of Qualified Electronic Signatures, the Directive and ETSI Policy Document have no specific requirement for the lengths of CA or end-user Subscriber signing keys.

6.1.6 Public Key Parameters Generation (DL1-2)

No stipulation.

¹⁷⁸ See ETSI Policy Document § 7.2.8(c)-(d).

¹⁷⁹ See ETSI Policy Document § 7.2.9 & note 2.

¹⁸⁰ See ETSI Policy Document § 7.2.3; see also Directive annex II(g), (l).

¹⁸¹ See ETSI Policy Document §§ 6.2(d) note 1, 7.2.1(d) note 1, 7.2.8(b) note 1.

¹⁸² ETSI Policy Document §§ 6.2(d), 7.2.1(d), 7.2.8(b).

6.1.7 Parameter Quality Checking (DL1-2)

No stipulation.

6.1.8 Hardware/Software Key Generation (DL1-2)

CA key pairs shall be generated in hardware meeting the requirements of EDP § 6.2.1.¹⁸³ For Subjects of DL2 Certificates generating their own keys, such generation shall take place on the SSCD hardware device to be used for signing.¹⁸⁴ Otherwise, the Subject's keys may be generated in software, although CAs generating keys on behalf of Subscribers of DL2 Certificates in software must place such keys within the Subscriber's SSCD hardware device and distribute the SSCDs in accordance with the controls of EDP § 6.1.2.2.

6.1.9 Key Usage Purposes (As per X.509 v3 Key Usage Field) (DL1-2)

The content of the key usage extension of DL1 and DL2 Certificates shall be subject to any applicable laws of EU Member Countries interpreting and implementing the Directive.

6.2 Private Key Protection

The private key protection provisions of CP § 6.2 meet the general confidentiality and integrity requirements of the ETSI Policy Document.¹⁸⁵ Processing Centers shall protect CA keys in devices meeting the requirements of EDP § 6.2.1.¹⁸⁶ Processing Centers shall ensure that CA signing keys are used only for the purpose of signing Certificates and/or signing revocation status information within premises secured in accordance with CP § 5.1.1 and shall not be used for other purposes.¹⁸⁷

Where Client Managed PKI Customers using Managed PKI Key Manager use the Key Manager Software and Trustworthy Systems to deliver private keys to Subjects in a manner such that the secrecy and the integrity of the key is not compromised and, once delivered to the subject, the private key can be maintained under the subject's sole

¹⁸³ See ETSI Policy Document § 7.2.1(b).

¹⁸⁴ See ETSI Policy Document § 6.2(f).

¹⁸⁵ See ETSI Policy Document §§ 6.2(c), 7.2.2; see also Directive annex II(f), (g).

¹⁸⁶ See ETSI Policy Document § 7.2.2(a).

¹⁸⁷ See ETSI Policy Document § 7.2.5.

control. Where private keys are pre-generated on hardware tokens, including SSCDs, the measures to protect such private keys shall conform to EDP § 6.1.2.¹⁸⁸

6.2.1 Standards for Cryptographic Modules (DL1-2)

Processing Centers shall perform all CA cryptographic operations with their own private keys and the private keys of the Client Service Centers, Client Managed PKI Customers, and ASB Customers within their Subdomains, on cryptographic modules that either:

- meet the requirements identified in FIPS 140-1 level 3 or utilize a set of controls that, as a whole, provide the level of security required by FIPS 140-1 level 3, or
- that are part of a Trustworthy System assured to EAL 4 or higher in accordance with ISO 15408 or equivalent security criteria, which assurance shall be in relation to a security target or protection profile that meets the requirements of the ETSI Policy Document, based on a risk analysis and taking into account physical and other non-technical security measures¹⁸⁹

6.2.2 Private Key (n out of m) Multi-Person Control (DL1-2)

The multi-person control requirements of CP § 6.2.2 meet the dual control requirements for CA private keys in the ETSI Policy Document.¹⁹⁰ The installation, activation, back-up and recovery of the CA's signing keys in cryptographic hardware shall require simultaneous control of at least of two trusted employees.

6.2.3 Private Key Escrow (DL1-2)

CA private keys and Subject signature private keys shall not be escrowed.¹⁹¹

6.2.4 Private Key Backup (DL1-2)

The process of backing up CA private keys in accordance with the physical controls required by CP § 6.2.4 and multi-person control required by CP § 6.2.2 meet the CA private key backup, storage, and recovery requirements of the ETSI Policy Document. The personnel that back up, store, and recover CA keys shall be limited to those who are required to do so consistent with their security and key generation policies.¹⁹²

The backup of end-user Subscriber private keys subject to the Managed PKI Key Manager service, is governed by EDP § 6.2.3.

¹⁸⁸ See ETSI Policy Document § 7.2.8(c)-(d).

¹⁸⁹ See ETSI Policy Document §§ 7.2.1(b), 7.2.2(a).

EDP

¹⁹⁰ See ETSI Policy Document §§ 7.2.1(a), 7.2.2(c), 7.2.7(c).

¹⁹¹ See Directive annex II(j); ETSI Policy Document § 7.2.4.

¹⁹² See ETSI Policy Document § 7.2.2(c)-(d).

6.2.5 Private Key Archival (DL1-2)

CA private keys shall not be archived.

6.2.6 Private Key Entry into Cryptographic Module (DL1-2)

The encryption of CA private keys during the transfer from one cryptographic module to another as part of the backup process under CP § 6.2.6, and limiting exposure of CA private keys outside the cryptographic module to such backup procedures, meets the requirements in the ETSI Policy Document to prevent Compromises to CA private keys outside a cryptographic module.¹⁹³

6.2.7 Method of Activating Private Key

6.2.7.1 DL1 Certificates

Subjects of DL1 Certificates have no requirement to use an SSCD in connection with the use and activation of their private keys, subject to CP § 6.2.7.1.

6.2.7.2 DL2 Certificates

In addition to the requirements of CP § 6.2.7.1, Subjects of DL2 Certificates shall use an SSCD in connection with the use and activation of their private keys.¹⁹⁴

6.2.8 Method of Deactivating Private Key (DL1-2)

No stipulation.

6.2.9 Method of Destroying Private Key (DL1-2)

The CA private key destruction requirements of CP § 6.2.9 meet the ETSI Policy Document's requirements for CA private key destruction or secure archival.¹⁹⁵

6.3 Other Aspects of Key Pair Management (DL1-2)

6.3.1 Public Key Archival

No stipulation.

¹⁹³ See ETSI Policy Document § 7.2.2(b), (e).

¹⁹⁴ See ETSI Policy Document § 6.2(e)-(f).

¹⁹⁵ See ETSI Policy Document § 7.2.6(a).

6.3.2 Usage Periods for the Public and Private Keys

The requirement in CP § 6.3.2 that CAs shall, upon the expiration of the usage period for their key pairs, cease all use of such key pair is consistent with the corresponding requirement of the ETSI Policy Document.¹⁹⁶

6.4 Activation Data (DL1-2)

6.4.1 Activation Data Generation and Installation

The use of and controls over activation data as required by CP § 6.2.7.1 are part of the process by which Subjects take steps to avoid use of their private keys.¹⁹⁷ See also EDP § 6.1.2.2 (controls over the delivery of activation data used with SSCDs).

6.4.2 Activation Data Protection

See EDP § 6.4.1.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls (DL1-2)

6.5.1 Specific Computer Security Technical Requirements

The requirement in CP § 6.5 that CA and RA functions take place on Trustworthy System consistent with the Security and Audit Requirements Guide (in the case of VeriSign and Affiliates) or the Enterprise Security Guide (in the case of Managed PKI Customers) by implication includes the more specific requirement that the integrity of CA and RA systems and information shall be protected against viruses and malicious and unauthorized software.¹⁹⁸

CP § 6.5.1 requires that Processing Centers, Service Centers, and Managed PKI Customers use 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. This requirement meets, in part, the requirement in the ETSI Policy Document to protect CA internal network domains from external network domains accessible by third parties.¹⁹⁹ In addition, however, the foregoing requirement shall apply to all Customers approving Certificate Applications for Qualified Certificates.

¹⁹⁶ See ETSI Policy Document § 7.2.6.

¹⁹⁷ See ETSI Policy Document § 6.2(c).

¹⁹⁸ See ETSI Policy Document § 7.4.5(a).

¹⁹⁹ See Directive annex II(f); ETSI Policy Document § 7.4.6(a).

Moreover, firewalls shall be configured to prevent protocols and accesses not required for the operation of the CA/RA.²⁰⁰

VeriSign, Affiliates, and Customers shall ensure effective administration of user access to maintain system security, including user account management, auditing, and timely modification or removal of access. Users include operators, Administrators, system administrators, and any users given direct access to the system.²⁰¹ Moreover, CA and RA personnel shall be successfully identified and authenticated before using critical applications related to certificate management.²⁰² VeriSign, Affiliates, and Customers shall also ensure that access to information and application system functions is restricted in accordance with the entity's access control policy and that the CA/RA system provides sufficient computer security controls for the separation of Trusted Positions identified in a CA's CPS or security documentation. Such controls shall include the separation of the system administrator and operation functions. Use of system utility programs shall be restricted and tightly controlled.²⁰³ Access shall be restricted allowing access only to resources as necessary for carrying out the role(s) allocated to a user

Sensitive data, such as Subscriber enrollment information, shall be protected against disclosure through re-used stored objects (e.g., deleted files) being accessible to unauthorized users.²⁰⁴

CA system software for the issuance of Certificates shall enforce access control on attempts to add or delete Certificates or modify other associated information.²⁰⁵ CA system software for the generation of Certificate status information shall enforce access control on attempts to modify Certificate status information.²⁰⁶

CA systems shall, through continuous monitoring and alarm facilities, detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources providing certificate lifecycle services, including, but not limited to, certificate generation and revocation.²⁰⁷

6.5.2 Computer Security Rating

The requirement that VeriSign, Affiliates, and Customers use Trustworthy Systems and products protected against modification may be ensured using, for example, systems conforming to a suitable protection profile (or profiles), defined using, for example, systems conforming to CWA 14167-1 [9] or to a suitable protection profile (or profiles),

²⁰⁰ See ETSI Policy Document § 7.4.6(a) note 1.

²⁰¹ See ETSI Policy Document §§ 7.4.5(c), 7.4.6.

²⁰² See ETSI Policy Document § 7.4.6(e).

²⁰³ See ETSI Policy Document § 7.4.6(d).

²⁰⁴ See ETSI Policy Document § 7.4.6(g) & note 3; see also ETSI Policy Document § 7.4.6.

²⁰⁵ See ETSI Policy Document § 7.4.6(j); see also Directive annex II(l).

²⁰⁶ See ETSI Policy Document § 7.4.6(l); see also Directive annex II(l).

²⁰⁷ See ETSI Policy Document § 7.4.6(i), (k).

defined in accordance with ISO/IEC 15408 [8] or equivalent standard.²⁰⁸ The risk analysis carried out on their services should identify critical services requiring Trustworthy Systems and the levels of assurance required.²⁰⁹ See also EDP § 6.2.1 (relating to the rating of CA systems that including cryptographic modules).

6.6 Life Cycle Technical Controls (DL1-2)

6.6.1 System Development Controls

An analysis of security requirements shall be carried out at the design and requirements specification stage of any systems development project undertaken with respect to the CA/RA software used by VeriSign, Affiliates, or Customers to ensure that security is built into IT systems.²¹⁰ Change control procedures shall be utilized for releases, modifications, and emergency software fixes for such software.²¹¹

6.6.2 Security Management Controls

VeriSign, Affiliates, and Customers shall maintain an inventory of all information assets and shall assign a classification of their protection requirements consistent with the risk analysis.²¹² Local network components are kept in a physically secure environment. The configuration of Information Services systems supporting CA and RA functions shall be audited periodically, including under CP § 2.7 and EDP § 2.7.²¹³ Capacity demands shall be monitored and requirements for projections of future capacity shall be developed to ensure that adequate processing power and storage are available for information assets.²¹⁴

Further, Processing Centers shall ensure the security of CA and RA cryptographic modules throughout their lifecycle (including certificate and revocation status information signing cryptographic hardware).²¹⁵ More specifically, Processing Centers shall ensure that such cryptographic modules:

- Are not tampered with during shipment,²¹⁶
- Are not tampered with while being stored,²¹⁷
- Are functioning correctly,²¹⁸
- When retired, are processed so that the CA or RA private keys stored within them are destroyed in accordance with CP § 6.2.9 and EDP § 6.2.9.²¹⁹

²⁰⁸ See ETSI Policy Document § 7.4.7 note 1.

²⁰⁹ See ETSI Policy Document § 7.4.7 note 2.

²¹⁰ See ETSI Policy Document § 7.4.7(a).

²¹¹ See ETSI Policy Document § 7.4.7(b).

²¹² See ETSI Policy Document § 7.4.2(a).

²¹³ See ETSI Policy Document § 7.4.6(h).

²¹⁴ See ETSI Policy Document § 7.4.5(g).

²¹⁵ See ETSI Policy Document § 7.2.7.

²¹⁶ See ETSI Policy Document § 7.2.7(a).

²¹⁷ See ETSI Policy Document § 7.2.7(b).

²¹⁸ See ETSI Policy Document § 7.2.7(d).

²¹⁹ See ETSI Policy Document § 7.2.7(e).

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls (DL1-2)

The requirement that VeriSign, Affiliates, and Customers protect communications using encryption and digital certificates satisfies the requirement that sensitive data be protected against unauthorized access or modification when exchanged over insecure networks.²²⁰ Also, the confidentiality and integrity of registration data shall be protected, especially when being exchanged with the Subscriber, Subject or between distributed CA system components.²²¹ When registration data is exchanged with Processing Centers, or between Managed PKI Customers and their Superior Entities, the communicating parties shall authenticate themselves to each other.

²²² Communications between Customers and Affiliates or between Affiliates and VeriSign shall, in general, be secured so that the security of information among parties having distributed PKI responsibilities is maintained.²²³

6.8 Cryptographic Module Engineering Controls (DL1-2)

See CP § 6.2.1, EDP § 6.2.1. In addition, CAs shall distribute SSCDs to DL2 end-user Subscribers that meet the following requirements. First, SSCDs must, by appropriate technical and procedural means, ensure that at least:

- The private key within the SSCD can practically occur only once, and that its secrecy is reasonably assured,
- Such private key cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently-available technology, and
- Such private key can be reliably be protected by the Subscriber against use by others.²²⁴

Second, SSCDs must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.²²⁵ Third, CAs shall ensure that the SSCDs have been determined to meet the requirements of Annex III of the Directive by the applicable national body designated pursuant to Article 3(4) the Directive (if any).²²⁶

7. Certificate and CRL Profile (DL1-2)

The content of DL1 and DL2 Certificates shall be subject to any applicable laws of EU Member Countries interpreting and implementing the Directive.

²²⁰ See ETSI Policy Document § 7.4.6(b).

²²¹ See ETSI Policy Document § 7.3.3(f).

²²² See ETSI Policy Document § 7.3.3(g).

²²³ See ETSI Policy Document § 7.4.1(e).

²²⁴ See Directive annex III(1).

²²⁵ See Directive annex III(2).

²²⁶ Directive art. 3(4).

7.1 Certificate Profile

DL1 and DL2 Certificates shall, in content, adhere to the Qualified Certificate Profile,²²⁷ as further specified in this EDP § 7.1. Pursuant to the Qualified Certificate Profile, DL1 and DL2 Certificates shall also comply with RFC 3039 where it does not conflict with the Qualified Certificate Profile.²²⁸ Also, the basic fields within Certificates required under CP § 7.1 adhere to the requirements of the Directive to include within Certificates:

- An indication that the certificate is issued as a qualified certificate
- The identification of the CA [Certification-Service-Provider] and the State in which it is established
- The name of the signatory
- Provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended
- Signature-verification data (subject public key),²²⁹
- The beginning and end of their validity periods (valid from and valid to dates),²³⁰
- The identity code of the Certificate (serial number).²³¹
- The Advanced Electronic Signature of the issuing certification-service-provider (digital signature of the CA).²³²
- Limitations on the scope of use of the certificate, if applicable; and
- Limits on the value of transactions for which the certificate can be used, if applicable

Processing Centers and Gateway Customers issuing DL1 and DL2 Certificates shall ensure that they have the profile set forth in this EDP § 7.1. In addition, Processing Centers shall issue DL1 and DL2 Certificates having such profile for their own CAs and the CAs of Client Service Centers, Client Managed PKI Customers, and ASB Customers within their Subdomains.

7.1.1 Version Number(s)

No stipulation.

7.1.2 Certificate Extensions

DL1 and DL2 Certificates shall contain a private extension containing an OID identifying the statement stating that the Certificate is issued in accordance with the Directive, as implemented in the country under which the applicable Affiliate is operating, in whose Subdomain the Certificate was issued. Such extension shall conform to the definition in

²²⁷ See Qualified Certificate Profile § 1.

²²⁸ See Qualified Certificate Profile § 4 (citing RFC 3039 Internet X.509 Public Key Infrastructure Qualified Certificates Profile [hereinafter “RFC 3039”).

²²⁹ See Directive annex I(e).

²³⁰ See Directive annex I(f).

²³¹ See Directive annex I(g).

²³² See Directive annex I(h).

section 4.2.1(2) of the Qualified Certificate Profile.²³³ This extension may be marked as critical or not critical at the option of the CA.

At the option of the CA, the following additional private extensions may be used:

- An extension containing a statement expressing the limit on the value of transactions for which the Certificate can be used in accordance with section 4.2.2 of the Qualified Certificate Profile,²³⁴ and
- An extension containing a statement indicating the record retention period applicable to the Certificate under CP § 4.6.1 and EDP 4.6.1, in accordance with section 4.2.3 of the Qualified Certificate Profile.²³⁵

7.1.3 Algorithm Object Identifiers

No stipulation.

7.1.4 Name Forms

The name of the CA in the issuer field of DL1 and DL2 Certificates shall contain a country name stored in the country name attribute. The specified country shall be the country in which the CA is established and located.²³⁶ The name of the Subscriber shall appear in the Subject field in accordance with CP § 7.1.4.²³⁷

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

The object identifier for the Certificate policy corresponding to DL1 and DL2 is set forth in EDP § 1.2. Processing Centers and Gateway Customers shall populate the CertificatePolicies extension in each Qualified Certificate with the object identifier of the Certificate policy corresponding to either DL1 or DL2, as applicable, consistent with EDP § 1.2. Note that the DL1 and DL2 policies, whose OIDs appear within the Certificate Policies extension Certificates issued under this EDP, are for the purpose of clearly expressing that CAs have issued such Certificates as Qualified Certificates and that they claim compliance with annex I and annex II of the Directive.²³⁸ Moreover, by virtue of including the DL1 OID or DL2 OID, which refer to the policies of this EDP containing limitations on the scope of the use of the Certificate, DL1 and DL2 Certificates contain such limitations.²³⁹

²³³ See Directive annex I(a); Qualified Certificate Profile § 4.2.1(2).

²³⁴ See Directive annex I(j); Qualified Certificate Profile § 4.2.2.

²³⁵ See Qualified Certificate Profile § 4.2.3.

²³⁶ See Directive annex I(b); Qualified Certificate Profile § 4.1.

²³⁷ See Directive annex I(c).

²³⁸ See Qualified Certificate Profile § 4.2.1(1); see also Directive annex I(a).

²³⁹ See Directive annex I (i).

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

No stipulation.

7.2 CRL Profile

No stipulation.

8. Specification Administration (Class 1-3)

8.1 Specification Change Procedures

Amendments to this EDP shall be made by the VeriSign Trust Network Policy Management Authority. Amendments shall either be in the form of a document containing an amended form of the EDP 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 EDP. The PMA shall determine whether changes to the EDP require a change in the Certificate policy object identifiers of the Certificate policies corresponding to either DL1 or DL2.

Affiliates wishing to offer or support DL1 or DL2 Certificates within their Subdomains shall define a review process for their CPSs and other practice documents including responsibilities for maintaining their CPSs.²⁴⁰ Such Affiliates shall give due notice of changes it intended to make in their CPSs and shall, following approval by the Affiliate's management body under EDP § 8.3, publish the revised CPS as required under EDP § 8.2.²⁴¹

8.1.1 Items that Can Change Without Notification

VeriSign and the PMA reserve the right to amend the EDP 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.

²⁴⁰ See ETSI Policy Document § 7.1(g).

²⁴¹ See ETSI Policy Document § 7.1(h).

8.1.2 Items that Can Change with Notification

The PMA shall make material amendments to the EDP in accordance with this Section 8.1.2.

8.1.2.1 List of Items

Material amendments are those changes that the PMA, under EDP § 8.1.1, considers to be substantive.

8.1.2.2 Notification Mechanism

The PMA shall send Affiliates notice of material amendments to the EDP proposed by the PMA. The notice shall state the text of the proposed amendments and the comment period under Section 8.1.2.3. Proposed amendments to the EDP shall also appear in the Practices Updates and Notices section of the VeriSign Repository, which is located at: <https://www.verisign.com/repository/updates>. Affiliates, in whose Subdomains DL1 or DL2 Certificates are issued, shall publish or provide a link to the proposed amendments on their own web-based repositories within a reasonable time after receiving notice of such amendments.

The PMA solicits proposed amendments to the EDP from other VTN 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 EDP to the contrary, if the PMA believes that material amendments to the EDP 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 and identify them as material 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.

8.1.2.3 Comment Period

Except as noted under EDP § 8.1.2.2, the comment period for any material amendments to the EDP shall be fifteen (15) days, starting on the date on which the amendments are posted on the VeriSign Repository. Any VTN Participant shall be entitled to file comments with the PMA up until the end of the comment period.

8.1.2.4 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 under EDP § 8.1.2.2, 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 under Section 8.1.2.3.

8.1.3 Changes Requiring Changes in the Certificate Policy OID or CPS Pointer

If the PMA determines that a change is necessary in the object identifier corresponding to either DL1 or DL2, the amendment shall contain new object identifiers for the Certificate policies corresponding to each type of Certificate. Otherwise, amendments shall not require a change in Certificate policy object identifier.

8.2 Publication and Notification Policies

8.2.1 Items Not Published in the EDP or CPS

Security documents and information in them considered confidential by VeriSign and the Affiliates are not disclosed to the public.²⁴²

8.2.2 Distribution of the EDP and CPSs

This EDP is published in electronic form within the VeriSign Repository at <https://www.verisign.com/CP>. The EDP is available in the VeriSign Repository in Word format, Adobe Acrobat pdf, and HTML. VeriSign also makes the EDP available in Adobe Acrobat pdf or Word format upon request sent to practices@verisign.com. The EDP is available in paper form from the PMA upon requests sent to: VeriSign, Inc., 487 East Middlefield Road, Mountain View, CA 94043 USA, Attn: Practices and External Affairs – EDP.

Affiliates wishing to offer or support DL1 or DL2 Certificates within their Subdomains shall make available to Subscribers and Relying Parties its CPS and other relevant documentation, as necessary to assess conformance to the EDP and ultimately the Directive.²⁴³

8.3 CPS Approval Procedures

Affiliates wishing to offer or support DL1 or DL2 Certificates within their Subdomains shall develop a CPS which shall be written and approved pursuant to CP § 8.3 and as follows:

- Such Affiliates shall carry out a risk assessment to evaluate business risks and determine the necessary security requirements and operational procedures of CAs within their Subdomains. The risk analysis shall be regularly reviewed and revised if necessary.²⁴⁴

²⁴² See ETSI Policy Document § 7.1(c) note 2.

²⁴³ See ETSI Policy Document § 7.1(c).

²⁴⁴ See ETSI Policy Document § 7.4.1(a).

- Such Affiliates shall write a CPS to address all the requirements addressed in this EDP (which ultimately apply the requirements of the Directive, ETSI Policy Document, and Qualified Certificate Policy),²⁴⁵ which CPS may be the same CPS written pursuant to the CP,
- Such CPS shall identify the requirements of VeriSign and their Customers, including their applicable procedures and practices,²⁴⁶
- Such Affiliates shall establish a high level management body with final authority and responsibility for approving the CPS,²⁴⁷ and
- The Affiliate shall submit this CPS to VeriSign for approval under CP § 8.3.

These requirement may already be satisfied by Affiliates whose CPSs have been approved by VeriSign, subject to whatever amendments are necessary to indicate that such CPSs support the DL1 and DL2 policies.

Such CPSs demonstrate reliability of CAs within Affiliates' respective Subdomains necessary for providing Certification services.²⁴⁸ In addition, Affiliates' CPSs shall identify all obligations of its Customers performing RA functions in support of Qualified Certificates within their respective Subdomains, including the applicable policies and practices that apply to them.²⁴⁹

Acronyms and Definitions

Table of Acronyms

Acronym	Term
ANSI	The American National Standards Institute.
ASB	Authentication Service Bureau.
B2B	Business-to-business.
BXA	The United States Bureau of Export Administration of the United States Department of Commerce.
CA	Certification Authority.
CP	Certificate Policy.
CPS	Certification Practice Statement.
CRL	Certificate Revocation List.
EAL	Evaluation assurance level (pursuant to the Common Criteria).
EDI	Electronic Data Interchange.
EDIFACT	EDI for Administration, Commerce, and Transport (standards established by the United Nations Economic Commission for Europe).
EDP	European Directive Policies
ETSI	European Telecommunications Standards Institute
FIPS	United State Federal Information Processing Standards.

²⁴⁵ See ETSI Policy Document § 7.1(a).

²⁴⁶ See ETSI Policy Document § 7.1(b).

²⁴⁷ See ETSI Policy Document § 7.1(f).

²⁴⁸ See ETSI Policy Document § 7.1 (citing Directive annex II(a)).

²⁴⁹ See ETSI Policy Document § 7.1(b).

Acronym	Term
ICC	International Chamber of Commerce.
ISO	International Organization for Standardization
KRB	Key Recovery Block.
LSVA	Logical security vulnerability assessment.
OCSP	Online Certificate Status Protocol.
OFX	Open Financial Exchange.
PCA	Primary Certification Authority.
PIN	Personal identification number.
PKCS	Public-Key Cryptography Standard.
PKI	Public Key Infrastructure.
PMA	Policy Management Authority.
QCP	Qualified Certificate Policy
RA	Registration Authority.
RFC	Request for comment.
SAS	Statement on Auditing Standards (promulgated by the American Institute of Certified Public Accountants).
S/MIME	Secure multipurpose Internet mail extensions.
SSCD	Secure-Signature-Creation Device
SSL	Secure Sockets Layer.
VTN	VeriSign Trust Network.
WAP	Wireless Application Protocol.
WTLS	Wireless Transport Layer Security.

Definitions

Only definitions that are not included in the VTN CP or have been amended are included in the list of definitions.

Term	Definition
Advanced Electronic Signature	An Electronic Signature which meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using means that the signatory can maintain under his sole control; and (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.
Attribute	Information bound to an entity that specifies a characteristic of an entity, such as a group membership or a role, or other information associated with that entity
Certificate	A message that, at least, states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key together with some other information secured with the private key of the certification authority which issued it, identifies the Certificate's Operational Period, contains a Certificate serial number, and is digitally signed by the CA.

Term	Definition
Certificate Policies (CP)	The document, which is entitled “VeriSign Trust Network Certificate Policies” and is the principal statement of policy governing the VTN. This policy includes a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements
Certificate Revocation List (CRL)	A periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates and are no longer considered valid by the certificate issuer. 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.
Certification Authority (CA)	An entity authorized and trusted by trusted by one or more users to issue, manage, revoke, and renew Certificates in the VTN.
Certification-Service-Provider (CSP)	An entity or a legal or natural person who issues certificates or provides other services related to electronic signatures
Certification Practice Statement (CPS)	A statement of the practices that VeriSign or an Affiliate employs in and issuing, managing, and revoking and renewing or re-keying Certificates, and requires its Managed PKI Customers and Gateway Customers to employ.
Electronic Signature	Data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication of that data.
Key Ceremony Reference Guide	A document describing Key Generation Ceremony requirements and practices.
Qualified Certificate	A Certificate which meets the requirements laid down in annex I (of the Directive) and is provided by a certification-service-provider who fulfils the requirements laid down in annex II (of the Directive).
Qualified Electronic Signature	An Advanced Electronic Signature which is based on a Qualified Certificate and which is created by an Secure-Signature-Creation Device, as defined in article 5.1 of the Directive.
Qualified Certificate Policy (QCP)	The certificate policy contained in this EDP which incorporates the requirements laid down in annex I and annex II of the Directive 1999/93/EC EDP
Relying Party	Recipient of a certificate which acts in reliance on that certificate and/or digital signatures verified using that certificate

Term	Definition
Secure-Signature-Creation Device (SSCD)	A device, comprised of configured software or hardware used to implement a private key used to create a digital signature, which meets the requirements laid down in annex III (of the Directive).
Server Gated Cryptography	A technology that permits web servers that have been issued a Global Server ID to create an SSL session with a browser that is encrypted using strong cryptographic protection.
Server Service Center	A Service Center that is an Affiliate providing Secure Server IDs and Global Server IDs either in the Web Site or Enterprise line of business.
Signature-creation Data	Unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature Where qualified certificates are based on public key cryptography, as covered by the present document, then the signature-creation data includes private keys. Hence, within the present document the term private key is used for the signature-creation data.
Signature-creation Device	Configured software or hardware used to implement the signature-creation data
Secure-signature-creation device	Signature-creation device which meets the requirements laid down in annex III of Directive 1999/93/EC
Signature-verification Data	Data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature In qualified certificates based on public key cryptography, as covered by the present document, the signature-verification data include public keys. Hence within the present document the term public key is used for the signature-verification data.
Subject	The entity identified in a certificate as the holder of a private key corresponding to a public key included in the certificate. The term "Subject" can, in the case of an organizational Certificate, refer to the equipment or device that holds a private key. A Subject is assigned an unambiguous name, which is bound to the public key contained in the Subject's Certificate.
Subscriber	An entity subscribing with a Certification Authority on behalf of either itself or one or more subjects
Time-Stamping Authority	The VeriSign entity that signs Digital Receipts as part of the VeriSign Digital Notarization Service.
Time-Stamping Authority CA	The VeriSign CA that issued a special Class 3 organizational Certificate to the Time-Stamping Authority used to verify the digital signatures on Digital Receipts.

Cross-Reference of ETSI Definitions to CP Definitions

Term as Defined in the ETSI Policy Document § 3.1	Corresponding Term in the CP
<i>advanced electronic signature</i>	The term “digital signature” used in the CP is one form of Advanced Electronic Signature.
<i>certificate</i>	certificate
<i>certificate policy</i>	A certificate policy, but not necessarily the CP
<i>certification authority</i>	certification authority
<i>certification practice statement</i>	certification practice statement
<i>certification-service-provider</i>	In the context of the CP, certification authority
<i>electronic signature</i>	electronic signature
<i>qualified certificate</i>	This term has no analog within the CP.
<i>qualified certificate policy</i>	This term has no analog within the CP.
<i>qualified electronic signature</i>	This term has no analog within the CP.
<i>relying party</i>	relying party
<i>signature-creation data</i>	signature private key
<i>signature-creation device</i>	hardware token used by a Subscriber
<i>secure-signature-creation device</i>	This term has no analog within the CP.
<i>signature-verification data</i>	public key
<i>subscriber</i>	Subscriber

VeriSign Certification Practice Statement

Version 3.8.1

Effective Date: February 01, 2009



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

VeriSign Certificate Practices Statement

© 2009 VeriSign, Inc. All rights reserved.
Printed in the United States of America.

Published date: February 1, 2009

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**.

Table of Contents

1.	INTRODUCTION	8
1.1	Overview	8
1.2	Document name and Identification	9
1.3	PKI Participants	9
1.3.1	Certification Authorities	9
1.3.2	Registration Authorities	10
1.3.3	Subscribers	10
1.3.4	Relying Parties	11
1.3.5	Other Participants	11
1.4	Certificate Usage	11
1.4.1	Appropriate Certificate Usages	11
1.4.2	Prohibited Certificate Uses	12
1.5	Policy Administration	13
1.5.1	Organization Administering the Document	13
1.5.2	Contact Person	13
1.5.3	Person Determining CP Suitability for the Policy	13
1.5.4	CPS Approval Procedure	13
1.6	Definitions and Acronyms	14
2.	Publication and Repository Responsibilities	14
2.1	Repositories	14
2.2	Publication of Certificate Information	14
2.3	Time or Frequency of Publication	15
2.4	Access Controls on Repositories	15
3.	Identification and Authentication	15
3.1	Naming	16
3.1.1	Type of Names	16
3.1.2	Need for Names to be Meaningful	16
3.1.3	Anonymity or pseudonymity of Subscribers	17
3.1.4	Rules for Interpreting Various Name Forms	18
3.1.5	Uniqueness of Names	18
3.1.6	Recognition, Authentication, and Role of Trademarks	18
3.2	Initial Identity Validation	18
3.2.1	Method to Prove Possession of Private Key	18
3.2.2	Authentication of Organization identity	18
3.2.3	Authentication of Individual Identity	19
3.2.4	Non-Verified Subscriber information	21
3.2.5	Validation of Authority	21
3.2.6	Criteria for Interoperation	21
3.3	Identification and Authentication for Re-key Requests	21
3.3.1	Identification and Authentication for Routine Re-key	22
3.3.2	Identification and Authentication for Re-key After Revocation	22
3.4	Identification and Authentication for Revocation Request	23
4.	Certificate Life-Cycle Operational Requirements	23
4.1	Certificate Application	23
4.1.1	Who Can Submit a Certificate Application?	23
4.1.2	Enrollment Process and Responsibilities	24
4.2	Certificate Application Processing	24
4.2.1	Performing Identification and Authentication Functions	24
4.2.2	Approval or Rejection of Certificate Applications	24
4.2.3	Time to Process Certificate Applications	24
4.3	Certificate Issuance	25
4.3.1	CA Actions during Certificate Issuance	25
4.3.2	Notifications to Subscriber by the CA of Issuance of Certificate	25
4.4	Certificate Acceptance	25
4.4.1	Conduct Constituting Certificate Acceptance	25
4.4.2	Publication of the Certificate by the CA	25
4.4.3	Notification of Certificate Issuance by the CA to Other Entities	25
4.5	Key Pair and Certificate Usage	25
4.5.1	Subscriber Private Key and Certificate Usage	25
4.5.2	Relying Party Public Key and Certificate Usage	25
4.6	Certificate Renewal	26

4.6.1	Circumstances for Certificate Renewal	26
4.6.2	Who May Request Renewal	26
4.6.3	Processing Certificate Renewal Requests	26
4.6.4	Notification of New Certificate Issuance to Subscriber	27
4.6.5	Conduct Constituting Acceptance of a Renewal Certificate	27
4.6.6	Publication of the Renewal Certificate by the CA	27
4.6.7	Notification of Certificate Issuance by the CA to Other Entities	27
4.7	Certificate Re-Key	27
4.7.1	Circumstances for Certificate Re-Key	28
4.7.2	Who May Request Certification of a New Public Key	28
4.7.3	Processing Certificate Re-Keying Requests	28
4.7.4	Notification of New Certificate Issuance to Subscriber	28
4.7.5	Conduct Constituting Acceptance of a Re-Keyed Certificate	28
4.7.6	Publication of the Re-Keyed Certificate by the CA	28
4.7.7	Notification of Certificate Issuance by the CA to Other Entities	28
4.8	Certificate Modification	29
4.8.1	Circumstances for Certificate Modification	29
4.8.2	Who May Request Certificate Modification	29
4.8.3	Processing Certificate Modification Requests	29
4.8.4	Notification of New Certificate Issuance to Subscriber	29
4.8.5	Conduct Constituting Acceptance of Modified Certificate	29
4.8.6	Publication of the Modified Certificate by the CA	29
4.8.7	Notification of Certificate Issuance by the CA to Other Entities	29
4.9	Certificate Revocation and Suspension	29
4.9.1	Circumstances for Revocation	29
4.9.2	Who Can Request Revocation	30
4.9.3	Procedure for Revocation Request	31
4.9.4	Revocation Request Grace Period	31
4.9.5	Time within Which CA Must Process the Revocation Request	31
4.9.6	Revocation Checking Requirements for Relying Parties	31
4.9.7	CRL Issuance Frequency	31
4.9.8	Maximum Latency for CRLs	32
4.9.9	On-Line Revocation/Status Checking Availability	32
4.9.10	On-Line Revocation Checking Requirements	32
4.9.11	Other Forms of Revocation Advertisements Available	32
4.9.12	Special Requirements regarding Key Compromise	32
4.9.13	Circumstances for Suspension	32
4.9.14	Who Can Request Suspension	32
4.9.15	Procedure for Suspension Request	32
4.9.16	Limits on Suspension Period	33
4.10	Certificate Status Services	33
4.10.1	Operational Characteristics	33
4.10.2	Service Availability	33
4.10.3	Optional Features	33
4.11	End of Subscription	33
4.12	Key Escrow and Recovery	33
4.12.1	Key Escrow and Recovery Policy and Practices	33
4.12.2	Session Key Encapsulation and Recovery Policy and Practices	34
5.	Facility, Management, and Operational Controls	34
5.1	Physical Controls	34
5.1.1	Site Location and Construction	35
5.1.2	Physical Access	35
5.1.3	Power and Air Conditioning	35
5.1.4	Water Exposures	35
5.1.5	Fire Prevention and Protection	35
5.1.6	Media Storage	35
5.1.7	Waste Disposal	35
5.1.8	Off-Site Backup	36
5.2	Procedural Controls	36
5.2.1	Trusted Roles	36
5.2.2	Number of Persons Required per Task	36
5.2.3	Identification and Authentication for Each Role	37

5.2.4	Roles Requiring Separation of Duties	37
5.3	Personnel Controls	37
5.3.1	Qualifications, Experience, and Clearance Requirements	37
5.3.2	Background Check Procedures	38
5.3.3	Training Requirements	38
5.3.4	Retraining Frequency and Requirements	39
5.3.5	Job Rotation Frequency and Sequence	39
5.3.6	Sanctions for Unauthorized Actions	39
5.3.7	Independent Contractor Requirements	39
5.3.8	Documentation Supplied to Personnel	39
5.4	Audit Logging Procedures	39
5.4.1	Types of Events Recorded	39
5.4.2	Frequency of Processing Log	40
5.4.3	Retention Period for Audit Log	40
5.4.4	Protection of Audit Log	40
5.4.5	Audit Log Backup Procedures	40
5.4.6	Audit Collection System (Internal vs. External)	40
5.4.7	Notification to Event-Causing Subject	40
5.4.8	Vulnerability Assessments	40
5.5	Records Archival	41
5.5.1	Types of Records Archived	41
5.5.2	Retention Period for Archive	41
5.5.3	Protection of Archive	41
5.5.4	Archive Backup Procedures	41
5.5.5	Requirements for Time-Stamping of Records	41
5.5.6	Archive Collection System (Internal or External)	41
5.5.7	Procedures to Obtain and Verify Archive Information	41
5.6	Key Changeover	42
5.7	Compromise and Disaster Recovery	42
5.7.1	Incident and Compromise Handling Procedures	42
5.7.2	Computing Resources, Software, and/or Data Are Corrupted	42
5.7.3	Entity Private Key Compromise Procedures	42
5.7.4	Business Continuity Capabilities After a Disaster	43
5.8	CA or RA Termination	43
6.	Technical Security Controls	44
6.1	Key Pair Generation and Installation	44
6.1.1	Key Pair Generation	44
6.1.2	Private Key Delivery to Subscriber	44
6.1.3	Public Key Delivery to Certificate Issuer	45
6.1.4	CA Public Key Delivery to Relying Parties	45
6.1.5	Key Sizes	45
6.1.6	Public Key Parameters Generation and Quality Checking	46
6.1.7	Key Usage Purposes (as per X.509 v3 Key Usage Field)	46
6.2	Private Key Protection and Cryptographic Module Engineering Controls	46
6.2.1	Cryptographic Module Standards and Controls	46
6.2.2	Private Key (n out of m) Multi-Person Control	46
6.2.3	Private Key Escrow	46
6.2.4	Private Key Backup	46
6.2.5	Private Key Archival	47
6.2.6	Private Key Transfer Into or From a Cryptographic Module	47
6.2.7	Private Key Storage on Cryptographic Module	47
6.2.8	Method of Activating Private Key	47
6.2.9	Method of Deactivating Private Key	49
6.2.10	Method of Destroying Private Key	49
6.2.11	Cryptographic Module Rating	49
6.3	Other Aspects of Key Pair Management	49
6.3.1	Public Key Archival	49
6.3.2	Certificate Operational Periods and Key Pair Usage Periods	49
6.4	Activation Data	51
6.4.1	Activation Data Generation and Installation	51
6.4.2	Activation Data Protection	51
6.4.3	Other Aspects of Activation Data	51

6.5	Computer Security Controls	52
6.5.1	Specific Computer Security Technical Requirements.....	52
6.5.2	Computer Security Rating	52
6.6	Life Cycle Technical Controls.....	52
6.6.1	System Development Controls	52
6.6.2	Security Management Controls	53
6.6.3	Life Cycle Security Controls	53
6.7	Network Security Controls	53
6.8	Time-Stamping.....	53
7.	Certificate, CRL, and OCSP Profiles	53
7.1	Certificate Profile.....	53
7.1.1	Version Number(s)	54
7.1.2	Certificate Extensions.....	54
7.1.3	Algorithm Object Identifiers	56
7.1.4	Name Forms.....	57
7.1.5	Name Constraints.....	57
7.1.6	Certificate Policy Object Identifier.....	57
7.1.7	Usage of Policy Constraints Extension.....	57
7.1.8	Policy Qualifiers Syntax and Semantics	57
7.1.9	Processing Semantics for the Critical Certificate Policies Extension.....	58
7.2	CRL Profile	58
7.2.1	Version Number(s)	58
7.2.2	CRL and CRL Entry Extensions	58
7.3	OCSP Profile.....	58
7.3.1	Version Number(s)	58
7.3.2	OCSP Extensions.....	58
8.	Compliance Audit and Other Assessments	59
8.1	Frequency and Circumstances of Assessment.....	59
8.2	Identity/Qualifications of Assessor	59
8.3	Assessor's Relationship to Assessed Entity.....	59
8.4	Topics Covered by Assessment.....	59
8.5	Actions Taken as a Result of Deficiency.....	60
8.6	Communications of Results	60
9.	Other Business and Legal Matters	60
9.1	Fees.....	60
9.1.1	Certificate Issuance or Renewal Fees.....	60
9.1.2	Certificate Access Fees.....	60
9.1.3	Revocation or Status Information Access Fees.....	60
9.1.4	Fees for Other Services.....	60
9.1.5	Refund Policy	61
9.2	Financial Responsibility	61
9.2.1	Insurance Coverage	61
9.2.2	Other Assets.....	61
9.2.3	Extended Warranty Coverage	61
9.3	Confidentiality of Business Information	61
9.3.1	Scope of Confidential Information	61
9.3.2	Information Not Within the Scope of Confidential Information	62
9.3.3	Responsibility to Protect Confidential Information	62
9.4	Privacy of Personal Information	62
9.4.1	Privacy Plan	62
9.4.2	Information Treated as Private	62
9.4.3	Information Not Deemed Private	62
9.4.4	Responsibility to Protect Private Information	62
9.4.5	Notice and Consent to Use Private Information.....	62
9.4.6	Disclosure Pursuant to Judicial or Administrative Process.....	62
9.4.7	Other Information Disclosure Circumstances	63
9.5	Intellectual Property rights	63
9.5.1	Property Rights in Certificates and Revocation Information	63
9.5.2	Property Rights in the CP.....	63
9.5.3	Property Rights in Names.....	63
9.5.4	Property Rights in Keys and Key Material	63
9.6	Representations and Warranties.....	64

9.6.1	CA Representations and Warranties	64
9.6.2	RA Representations and Warranties	64
9.6.3	Subscriber Representations and Warranties	64
9.6.4	Relying Party Representations and Warranties	65
9.6.5	Representations and Warranties of Other Participants	65
9.7	Disclaimers of Warranties	65
9.8	Limitations of Liability	65
9.9	Indemnities	66
9.9.1	Indemnification by Subscribers.....	66
9.9.2	Indemnification by Relying Parties	66
9.10	Term and Termination.....	66
9.10.1	Term.....	66
9.10.2	Termination	66
9.10.3	Effect of Termination and Survival.....	66
9.11	Individual Notices and Communications with Participants	66
9.12	Amendments.....	67
9.12.1	Procedure for Amendment	67
9.12.2	Notification Mechanism and Period	67
9.12.3	Circumstances Under Which OID Must be Changed	67
9.13	Dispute Resolution Provisions	68
9.13.1	Disputes Among VeriSign, Affiliates, and Customers.....	68
9.13.2	Disputes with End-User Subscribers or Relying Parties	68
9.14	Governing Law.....	68
9.15	Compliance with Applicable Law.....	68
9.16	Miscellaneous Provisions.....	68
9.16.1	Entire Agreement	68
9.16.2	Assignment.....	68
9.16.3	Severability.....	69
9.16.4	Enforcement (Attorney's Fees and Waiver of Rights).....	69
9.16.5	Force Majeure	69
9.17	Other Provisions	69
Appendix A.	Table of Acronyms and definitions.....	70
	Table of Acronyms	70
	Definitions	70
Appendix B1.	Supplemental Validation Procedures for Extended Validation SSL Certificates	80
Appendix B2 —	Minimum Cryptographic Algorithm and Key Sizes	112
Appendix B3 —	EV Certificates Required Certificate Extensions	113
Appendix B4 —	Country Specific Organization Name Guidelines	115
Appendix C —	History of Changes	

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.¹ 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.

¹ Authenticated Content Signing Certificates (ACS) are issued by a non-VTN CA. However, reference is made to these certificates in certain sections of this VeriSign CPS, for ACS customers to understand certain procedural differences used for these certificates.

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 documents² 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 domains³, 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.

² 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

³ Class 4 certificates are not currently issued by the VTN

VeriSign also operates the “VeriSign Universal Root Certification Authority”. The “VeriSign Universal Root Certification Authority” is not defined under a particular certificate Class, and may issue any class of Subordinate CA.

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.

A 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.⁴

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

⁴ An example of a third party RA is a customer of Managed PKI services customer.

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.

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 Usage⁵

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.

⁵ "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."

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

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

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

1.5 Policy Administration

1.5.1 Organization Administering the Document

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

1.5.2 Contact Person

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

1.5.3 Person Determining CP Suitability for the Policy

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

1.5.4 CPS Approval Procedure

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

1.6 Definitions and Acronyms

See Appendix A for a table of acronyms and definitions

2. Publication and Repository Responsibilities

2.1 Repositories

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

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

2.2 Publication of Certificate Information

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

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

VeriSign will at all times publish a current version of:

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

VeriSign is responsible for the repository function for:

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

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

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

VeriSign publishes Certificates in accordance with Table 3 below.

Certificate Type	Publication Requirements
VeriSign PCA and VeriSign Issuing Root CA Certificates	Available to Relying Parties through inclusion in current browser software and as part of a Certificate Chain that can be obtained with the end-user Subscriber Certificate through the query functions described below.
VeriSign Issuing CA Certificates	Available to Relying Parties as part of a Certificate Chain that can be obtained with the end-user Subscriber Certificate through the query functions described below.
Certificate of the VeriSign CA supporting Managed PKI Lite Certificates and CA Certificates of Managed PKI Customers	Available through query of the VeriSign LDAP directory server at directory.verisign.com .
VeriSign OCSP Responder Certificates	Available through query of the VeriSign LDAP directory server at directory.verisign.com .
End-User Subscriber Certificates	Available to relying parties through query functions in the VeriSign repository at: https://digitalid.verisign.com/services/client/index.html and https://digitalid.verisign.com/services/server/search.htm . Also available through query of the VeriSign LDAP directory server at directory.verisign.com .
End-User Subscriber Certificates issued through Managed PKI Customers	Made available through the query functions listed above, although at the discretion of the Managed PKI Customer, the Certificate may be accessible only via a search using the Certificate's serial number.
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.

Attribute	Value
Country (C) =	"US" or not used.
Organization (O) =	"VeriSign, Inc." ⁶
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"> • CA Name • VeriSign Trust Network • A statement referencing the applicable Relying Party Agreement governing terms of use of the Certificate and • A copyright notice. • Text to describe the type of Certificate.
State or Province (S) =	Not used.
Locality (L) =	Not used except for the VeriSign Commercial Software Publishers CA, which uses "Internet."
Common Name (CN) =	This attribute includes the CA Name (if the CA Name is not specified in an OU attribute) or is not used.

Table 4 – Distinguished Name Attributes in CA Certificates

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

Attribute	Value
Country (C) =	2 letter ISO country code or not used.
Organization (O) =	The Organization attribute is used as follows: <ul style="list-style-type: none"> • "VeriSign, Inc." for VeriSign OCSP Responder and optionally for individual Certificates that do not have an organization affiliation. • Subscriber organizational name for web server Certificates and individual Certificates that have an organization affiliation.
Organizational Unit (OU) =	VeriSign end-user Subscriber Certificates may contain multiple OU attributes. Such attributes may contain one or more of the following: <ul style="list-style-type: none"> • Subscriber organizational unit (for organizational Certificates and individual Certificates that have an organization affiliation) • VeriSign Trust Network • A statement referencing the applicable Relying Party

⁶ An exception to this is the Secure Server CA, which indicates "RSA Data Security, Inc.," but is now a VeriSign CA.

Attribute	Value
	Agreement governing terms of use of the Certificate <ul style="list-style-type: none"> • A copyright notice • “Authenticated by VeriSign” and “Member, VeriSign Trust Network” in Certificates whose applications were authenticated by VeriSign • “Persona Not Validated” for Class 1 Individual Certificates • Text to describe the type of Certificate.
State or Province (S) =	Indicates the Subscriber’s State or Province (State is not a required field in certificates issued to individuals).
Locality (L) =	Indicates the Subscriber’s Locality (Locality is not a required field in certificates issued to individuals).
Common Name (CN) =	This attribute includes: <ul style="list-style-type: none"> • The OCSP Responder Name (for OCSP Responder Certificates) • Domain name (for web server Certificates) • Organization name (for code/object signing Certificates) • Name (for individual Certificates).
E-Mail Address (E) =	E-mail address for Class 1 individual Certificates and generally for MPKI Subscriber Certificates

Table 5 – Distinguished Name Attributes in End User Subscriber Certificates

The Common Name (CN=) component of the Subject distinguished name of end-user Subscriber Certificates is authenticated in the case of Class 2-3 Certificates.

The authenticated common name value included in the Subject distinguished names of organizational Certificates is a domain name (in the case of Secure Server IDs and Global Server IDs) or the legal name of the organization or unit within the organization.

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

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.

Certificate Type	Additional Procedures
Extended Validation Certificates	VeriSign's procedures for issuing Extended Validation SSL Certificates are described in Appendix B1 to this CPS.
OFX Server IDs	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"> • 60xx Depository institutions • 61xx Nondepository credit institutions • 62xx Security, commodity brokers, and services • 63xx Insurance carriers • 64xx Insurance agents, brokers, and services • 67xx Holding and other investment offices • 7372 Prepackaged software • 7373 Computer integrated systems design • 7374 Data processing and preparation • 3661 Telephone and telegraph apparatus • 8721 Accounting, auditing, and bookkeeping.
Hardware Protected SSL Certificate	VeriSign verifies that the key pair was generated on FIPS 140 certified hardware
Managed PKI for Intranet SSL Certificate	VeriSign verifies that the host name or IP address assigned to a Device is not accessible from the Internet (publicly facing), and is owned by the Certificate Subscriber.
Authenticated Content Signing Certificate	Before VeriSign Digitally Signs any content using ACS it authenticates that the content is the original content signed by the Organization using its Code Signing Certificate.

Table 6 – Specific Authentication Procedures

3.2.3 Authentication of Individual Identity

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

Certificate Class	Authentication of Identity
Class 1	No identity authentication. There is a limited confirmation of the Subscriber's e-mail address by requiring the Subscriber to be able to answer an e-mail to that address.
Class 2	Authenticate identity by matching the identity provided by the Subscriber to:

	<ul style="list-style-type: none"> • information residing in the database of a VeriSign-approved identity proofing service, such as a major credit bureau or other reliable source of information providing, or • information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals
Class 3	<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.⁷</p>
Shared Service Provider Certificates for non federal entities	The identity of the Certificate Subscriber is verified substantially in compliance with the requirements of the X.509 Certificate Policy for the US Department of Homeland Security Public Key Infrastructure (PKI)

Table 7. Authentication of individual identity

⁷ 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.

3.2.4 Non-Verified Subscriber information

Non-verified subscriber information includes:

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

3.2.5 Validation of Authority

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

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

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 issue⁸
- 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

⁸ 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

is generated on the web server and most web server key generation tools permit the creation of a new Certificate Request for an existing key pair, there is a distinction between “rekey” and “renewal.”

3.3.1 Identification and Authentication for Routine Re-key

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

One acceptable procedure is through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. Subscribers choose and submit with their enrollment information a Challenge Phrase. Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber’s Challenge Phrase (or the equivalent thereof) with the Subscriber’s reenrollment information, and the enrollment information (including Corporate and Technical contact information) has not changed, a renewal Certificate is automatically issued. As an alternative to using a challenge phrase (or equivalent) VeriSign may send an e-mail message to the e-mail address associated with the verified corporate contact for the certificate being renewed, requesting confirmation of the Certificate renewal order and authorization to issue the Certificate. Upon receipt of confirmation authorizing issuance of the Certificate, VeriSign will issue the Certificate if the enrollment information (including Corporate and Technical contact information⁹) has not changed.

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.¹⁰

In particular, for subsequent re-key requests for retail Class 3 Organizational SSL 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, or a confirmatory response is obtained to an e-mail to the corporate contact 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

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

¹⁰ 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 entity approving the Subscriber's Certificate Application discovers or has reason to believe that a material fact in the Certificate Application is false. or
- For any other reason deemed necessary by VeriSign to protect the VTN

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

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

3.4 Identification and Authentication for Revocation Request

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

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

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

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

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

The requests to revoke a CA Certificate shall be authenticated by 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 and/or exclusive control 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 information¹¹) has not changed, a renewal Certificate is automatically issued. As an alternative to using a challenge phrase (or equivalent) VeriSign may send an e-mail message to the e-mail address associated with the verified corporate contact for the certificate being renewed, requesting confirmation of the Certificate renewal order and authorization to issue the Certificate. Upon receipt of confirmation authorizing issuance of the Certificate, VeriSign will issue the Certificate if the enrollment information (including Corporate and Technical contact information¹²) has not changed.

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 SSL 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, or a confirmatory response is obtained to an e-mail to the corporate contact, 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.

¹¹ If contact information has changed via an approved formal contact change procedure the certificate shall still qualify for automated renewal.

¹² If contact information has changed via an approved formal contact change procedure the certificate shall still qualify for automated renewal.

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 information¹³) 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.

¹³ If contact information has changed via an approved formal contact change procedure the certificate shall still qualify for automated renewal.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

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

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

4.8.2 Who May Request Certificate Modification

See Section 4.1.1

4.8.3 Processing Certificate Modification Requests

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

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See Section 4.4.1

4.8.6 Publication of the Modified Certificate by the CA

See Section 4.4.2

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Only in the circumstances listed below, will an end-user Subscriber certificate be revoked by VeriSign (or by the Subscriber) and published on a CRL. Upon request from a subscriber who can no longer use (or no longer wishes to use) a certificate for a reason other than one mentioned below, VeriSign will flag the certificate as inactive in its database but will not publish the certificate on a CRL.

An end-user Subscriber Certificate is revoked if:

- VeriSign, a Customer, or a Subscriber has reason to believe or strongly suspects that there has been a Compromise of a Subscriber's private key,
- VeriSign or a Customer has reason to believe that the Subscriber has materially breached a material obligation, representation, or warranty under the applicable Subscriber Agreement,
- The Subscriber Agreement with the Subscriber has been terminated,
- The affiliation between an Enterprise Customer with a Subscriber is terminated or has otherwise ended,

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

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

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

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

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

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

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

4.9.2 Who Can Request Revocation

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

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

4.9.3 Procedure for Revocation Request

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

An end-user Subscriber requesting revocation is required to communicate the request to 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 annually, but also whenever a CA Certificate is revoked.¹⁴

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.

¹⁴ CRLs for the "VeriSign Class 3 Organizational VIP Device CA" are only issued whenever a certificate issued by that CA is revoked.

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

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

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

4.9.10 On-Line Revocation Checking Requirements

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

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable

4.9.12 Special Requirements regarding Key Compromise

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

4.9.13 Circumstances for Suspension

Not applicable

4.9.14 Who Can Request Suspension

Not applicable

4.9.15 Procedure for Suspension Request

Not applicable

4.9.16 Limits on Suspension Period

Not applicable

4.10 Certificate Status Services

4.10.1 Operational Characteristics

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

4.10.2 Service Availability

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

4.10.3 Optional Features

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

4.11 End of Subscription

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

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

4.12 Key Escrow and Recovery

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

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

4.12.1 Key Escrow and Recovery Policy and Practices

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

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

- Enterprise customers using Managed PKI Key Manager shall confirm the identity of any person purporting to be the Subscriber to ensure that a purported Subscriber request for the Subscriber's private key is, in fact, from the Subscriber and not an imposter,
- Enterprise customers shall recover a Subscriber's private key without the Subscriber's authority only for their legitimate and lawful purposes, such as to comply with judicial or

- administrative process or a search warrant, and not for any illegal, fraudulent, or other wrongful purpose, and
- Such Enterprise customers shall have personnel controls in place to prevent Key Management Service Administrators and other persons from obtaining unauthorized access to private keys.

It is recommended that Enterprise Customers using KMS:

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

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Private keys are stored on the enterprise's premises in encrypted form¹⁵. 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.

¹⁵ In Limited circumstances, and only when expressly authorized through an Enterprise Service Agreement, VeriSign may host an Enterprise's Key Management Service and associated escrowed private keys.

5.1.1 Site Location and Construction

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

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

5.1.2 Physical Access

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

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

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

5.1.3 Power and Air Conditioning

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

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

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

All media containing production software and data, audit, archive, or backup information is stored within VeriSign facilities or in a secure off-site storage facility with appropriate physical and logical

access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic).

5.1.7 Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance with 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, at a minimum, meets the requirements of FIPS 140-1 level 3.

6.1.2 Private Key Delivery to Subscriber

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

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

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

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

6.1.3 Public Key Delivery to Certificate Issuer

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

6.1.4 CA Public Key Delivery to Relying Parties

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

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

6.1.5 Key Sizes

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

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

6.1.6 Public Key Parameters Generation and Quality Checking

Not applicable

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

Refer to Section 7.1.2.1.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

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

6.2.1 Cryptographic Module Standards and Controls

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

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

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

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

6.2.3 Private Key Escrow

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

6.2.4 Private Key Backup

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

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

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

6.2.5 Private Key Archival

Upon expiration of a VeriSign CA Certificate, the key pair associated with the certificate will be securely retained for a period of at least 5 years using hardware cryptographic modules that meet the requirements of this CPS. These CA key pairs shall not be used for any signing events after their expiration date, unless the CA Certificate has been renewed in terms of 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

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 below¹⁶. End user Subscriber Certificates that are renewals of existing subscriber certificates may have a longer validity period (up to 3 months).

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.

¹⁶ Certificate validity periods may be extended beyond the limits set in Section 6.3.2 for certificates using stronger encryption algorithms or key lengths are used, e.g. the use of SHA 2 or ECC algorithms and/or the use of 2048 bit or larger keys.

Certificate Issued By:	Validity Period
PCA self-signed (1024 bit)	Up to 30 years
PCA self-signed (2048 bit)	Up to 50 years
PCA to Offline intermediate CA	Generally 10 years but up to 15 years after renewal
PCA to online CA	Generally 5 years but up to 10 years after renewal ¹⁷
Offline intermediate CA to online CA	Generally 5 years but up to 10 years after renewal ¹⁸
Online CA to End-user Individual Subscriber	Normally up to 2 years, but under the conditions described below, up to 5 years ¹⁹
Online CA to End-Entity Organizational Subscriber	Normally up to 5 years ²⁰

Table 8 – Certificate Operational Periods

In terms of Section 6.3.2 of the VTN CP, the VeriSign PMA has approved an exception to extend a limited number CAs beyond the specified limits, in order to ensure uninterrupted PKI services during CA key pair migration. This exception may not be used to extend a CA's validity beyond a 13 year total validity, and shall not be made available after April 30, 2011.

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.

¹⁷ The VeriSign Onsite Administrator CA-Class 3 and Class 3 Secure Server Operational Administrator CA have a validity beyond 10 years to support legacy systems and shall be revoked when appropriate

¹⁸ 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.

¹⁹ 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.

²⁰ At a minimum, the Distinguished Name of four and five year validity SSL certificates is reverified after three years from date of certificate issuance. With the exception of the VeriSign Automated Administration certificate, 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.

VeriSign also operates the "VeriSign Class 3 International Server CA" and the "Class 3 Open Financial Exchange CA - G2" which are online CAs signed by a PCA. The validity of these CAs may exceed the validity periods described in Table 8 above to ensure continued interoperability of certificates offering SGC and OFX capability.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

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

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

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

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

6.4.2 Activation Data Protection

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

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

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

6.4.3 Other Aspects of Activation Data

6.4.3.1 Activation Data Transmission

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

6.4.3.2 Activation Data Destruction

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

6.5 Computer Security Controls

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

6.5.1 Specific Computer Security Technical Requirements

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

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

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

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

6.5.2 Computer Security Rating

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

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

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

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

6.6.2 Security Management Controls

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

6.6.3 Life Cycle Security Controls

No stipulation

6.7 Network Security Controls

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

6.8 Time-Stamping

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

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

VeriSign Certificates conform generally to (a) ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 and (b) RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 ("RFC 5280").

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

Field	Value or Value constraint
Serial Number	Unique value per Issuer DN
Signature Algorithm	Object identifier of the algorithm used to sign the certificate (See CP § 7.1.3)
Issuer DN	See Section 7.1.4
Valid From	Universal Coordinate Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 5280.
Valid To	Universal Coordinate Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 5280.
Subject DN	See CP § 7.1.4
Subject Public Key	Encoded in accordance with RFC 5280
Signature	Generated and encoded in accordance with RFC 5280

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 5280: 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 TRUE for CA certificates and may be set to either TRUE, or FALSE for end entity Subscriber certificates.

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

Table 10 – Settings for KeyUsage Extension

7.1.2.2 Note: The nonRepudiation bit²¹ is not required to be set in these Certificates because the PKI industry has not yet reached a consensus as to what the nonRepudiation bit means. Until such a consensus emerges, the nonRepudiation bit might not be meaningful for potential Relying Parties. Moreover, the most commonly used applications do not always respect the nonRepudiation bit. Therefore, setting the bit might not help Relying Parties make a trust decision. Consequently, this CPS does

²¹ The nonRepudiation bit may also be referred to as ContentCommitment in Digital Certificates in accordance with the X.509 standard.

not require that the nonRepudiation bit be set. It may be set in the case of dual key pair signature Certificates issued through Managed PKI Key Manager, or as otherwise requested. Any dispute relating to non-repudiation arising from the use of a digital certificate is a matter solely between the Subscriber and the Relying Party(s). VeriSign shall incur no liability in relation thereto.

7.1.2.3 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.

7.1.2.4 Subject Alternative Names

The subjectAltName extension of X.509 Version 3 Certificates are populated in accordance with RFC 5280. The criticality field of this extension shall be set to FALSE.

7.1.2.5 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.

7.1.2.6 Extended Key Usage

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

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

Table 11 – Certificates Using the Extended Key Usage Extension

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

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

7.1.2.7 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.

7.1.2.8 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.

7.1.2.9 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 5280. 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.

- sha256withRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
- ecdsa-with-Sha384 OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 3}
- 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 may include 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. This OU must appear if a pointer to the applicable Relying Party Agreement is not included in the policy extension of the certificate.

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 Version1 and Version 2 CRLs. Version 2 CRLs comply with the requirements of RFC 5280.

7.2.2 CRL and CRL Entry Extensions

No stipulation

7.3 OCSP Profile

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

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

OCSP responders conform to RFC 2560.

7.3.1 Version Number(s)

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

7.3.2 OCSP Extensions

VeriSign's TGV Service used to validate Class 3 Organizational certificates uses secure timestamp and validity period to establish the current freshness of each OCSP response. VeriSign does not use a nonce to establish the current freshness of each OCSP response and

clients should not expect a nonce in the response to a request that contains a nonce. Instead, clients should use the local clock to check for response freshness.

8. Compliance Audit and Other Assessments

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

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

- VeriSign shall be entitled, within its sole and exclusive discretion, to perform at any time an "Exigent Audit/Investigation" on a Customer in the event VeriSign has reason to believe that the audited entity has failed to meet VTN Standards, has experienced an incident or compromise, or has acted or failed to act, such that the audited entity's failure, the incident or compromise, or the act or failure to act poses an actual or potential threat to the security or integrity of the VTN.
- VeriSign shall be entitled to perform "Supplemental Risk Management Reviews" on a Customer following incomplete or exceptional findings in a Compliance Audit or as part of the overall risk management process in the ordinary course of business.

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

8.1 Frequency and Circumstances of Assessment

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

8.2 Identity/Qualifications of Assessor

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

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

8.3 Assessor's Relationship to Assessed Entity

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

8.4 Topics Covered by Assessment

The scope of VeriSign's annual WebTrust for Certification Authorities (or equivalent) audit includes CA environmental controls, key management operations and

Infrastructure/Administrative CA controls, certificate life cycle management and CA business practices disclosure.

8.5 Actions Taken as a Result of Deficiency

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

8.6 Communications of Results

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

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

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

9.1.2 Certificate Access Fees

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

9.1.3 Revocation or Status Information Access Fees

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

9.1.4 Fees for Other Services

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

9.1.5 Refund Policy

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

VeriSign adheres to, and stands behind, rigorous practices and policies in undertaking certification operations and in issuing certificates. Nevertheless, if for any reason a subscriber is not completely satisfied with the certificate issued to him, her, or it, the subscriber may request that VeriSign revoke the certificate within thirty (30) days of issuance and provide the subscriber with a refund. Following the initial thirty (30) day period, a subscriber may request that VeriSign revoke the certificate and provide a refund if VeriSign has breached a warranty or other material obligation under this CPS or the NetSure^(sm) Protection Plan relating to the subscriber or the subscriber's certificate. After VeriSign revokes the subscriber's certificate, VeriSign will promptly credit the subscriber's credit card account (if the certificate was paid for via credit card) or otherwise reimburse the subscriber via check, for the full amount of the applicable fees paid for the certificate. To request a refund, please call customer service at +1 650 426-3400. This refund policy is not an exclusive remedy and does not limit other remedies that may be available to subscribers.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

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

9.2.2 Other Assets

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

9.2.3 Extended Warranty Coverage

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

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

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

- CA application records, whether approved or disapproved,
- Certificate Application records,

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

9.3.2 Information Not Within the Scope of Confidential Information

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

9.3.3 Responsibility to Protect Confidential Information

VeriSign secures private information from compromise and disclosure to third parties.

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:

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

Table 14 – Liability Caps

The liability caps in Table 14 limit damages recoverable outside the context of the NetSure Protection Plan. Amounts paid under the NetSure Protection Plan are subject to their own liability caps. The liability caps under the NetSure Protection Plan for different kinds of Certificates range from \$50,000 US to \$250,000 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 Fairfax County, Virginia, 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 Commonwealth of Virginia, 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 Virginia, USA. This choice of law is made to ensure uniform procedures and interpretation for all VTN Participants, no matter where they are located.

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

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

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Not applicable

9.16.2 Assignment

Not applicable

9.16.3 Severability

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

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

Not applicable

9.16.5 Force Majeure

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

9.17 Other Provisions

Not applicable

Appendix A. Table of Acronyms and definitions

Table of Acronyms

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

Definitions

Term	Definition
Administrator	A Trusted Person within the organization of a Processing Center, Service Center, Managed PKI Customer, or Gateway Customer that performs validation and other CA or RA functions.
Administrator Certificate	A Certificate issued to an Administrator that may only be used to perform CA or RA functions.
Affiliate	A leading trusted third party, for example in the technology, telecommunications, or financial services industry, that has entered into an agreement with VeriSign to be a VTN distribution and services channel within a specific territory.
Affiliate Practices Legal Requirements Guidebook	A VeriSign document setting forth requirements for Affiliate CPSs, agreements, validation procedures, and privacy policies, as well as other requirements that Affiliates must meet.
Affiliated Individual	A natural person that is related to a Managed PKI Customer, Managed PKI Lite Customer, or Gateway Customer entity (i) as an officer, director, employee, partner, contractor, intern,

Term	Definition
	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.
Applicant	The Private Organization or Government Entity that applies for (or seeks renewal of) an EV Certificate naming it as the Subject.
Applicant Representative	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.
Application Software Vendor	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.
Automated Administration	A procedure whereby Certificate Applications are approved automatically if enrollment information matches information contained in a database.
Automated Administration Software Module	Software provided by VeriSign that performs Automated Administration.
Certificate	A message that, at least, states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key, identifies the Certificate's Operational Period, contains a Certificate serial number, and is digitally signed by the CA.
Certificate Applicant	An individual or organization that requests the issuance of a Certificate by a CA.
Certificate Application	A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.
Certificate 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 of an EV Certificate 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.
Certificate Chain	An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.
Certificate Management Control Objectives	Criteria that an entity must meet in order to satisfy a Compliance Audit.
Certificate Policies (CP)	This document, which is entitled "VeriSign Trust Network Certificate Policies" and is the principal statement of policy governing the VTN.
Certificate 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.
Certificate Revocation List (CRL)	A periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates in accordance with CP § 3.4. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation.
Certificate Signing Request	A message conveying a request to have a Certificate issued.
Certification Authority (CA)	An entity authorized to issue, manage, revoke, and renew Certificates in the VTN.
Certification Practice Statement (CPS)	A statement of the practices that VeriSign or an Affiliate employs in approving or rejecting Certificate Applications and issuing, managing, and revoking Certificates, and requires its Managed PKI Customers and Gateway Customers to employ.
Challenge Phrase	A secret phrase chosen by a Certificate Applicant during enrollment for a Certificate. When issued a Certificate, the Certificate Applicant becomes a Subscriber and a CA or RA can use the Challenge Phrase to authenticate the Subscriber when the Subscriber seeks to revoke or renew the Subscriber's Certificate.
Class	A specified level of assurances as defined within the CP. See CP § 1.1.1.
Client Service Center	A Service Center that is an Affiliate providing client Certificates either in the Consumer or Enterprise line of business.
Compliance Audit	A periodic audit that a Processing Center, Service Center, Managed PKI Customer, or Gateway Customer undergoes to determine its conformance with VTN Standards that apply to it.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
Confidential/Private Information	Information required to be kept confidential and private pursuant to CP § 2.8.1.
Contract Signer	A Contract Signer is a natural person who is employed by the Applicant, or an authorized

Term	Definition
	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 for an EV Certificate.
Country	A Country shall mean a Sovereign state as defined in the Guidelines.
CRL Usage Agreement	An agreement setting forth the terms and conditions under which a CRL or the information in it can be used.
Customer	An organization that is either a Managed PKI Customer, Gateway Customer, or ASB Customer.
Demand Deposit Account	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.
Enterprise, as in Enterprise Service Center	A line of business that an Affiliate enters to provide Managed PKI services to Managed PKI Customers.
Enterprise EV Certificate:	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.
Enterprise RA	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.
Enterprise Roaming Server	A server residing at the site of a Managed PKI Customer used in conjunction with the VeriSign Roaming Service to hold Roaming Subscribers' encrypted private keys and portions of symmetric keys used to encrypt and decrypt Roaming Subscribers' private keys.
EV Certificate:	A digital certificate that contains information specified in the EV Guidelines and that has been validated in accordance with the Guidelines.
EV OID	An identifying number, called an "object identifier," that is included in the certificate Policies 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.
Exigent Audit/Investigation	An audit or investigation by VeriSign where VeriSign has reason to believe that an entity's failure to meet VTN Standards, an incident or Compromise relating to the entity, or an actual or potential threat to the security of the VTN posed by the entity has occurred.
Extended Validation	Validation Procedures defined by the Guidelines for Extended Validation Certificates published by a forum consisting of major certification authorities and browser vendors.
Intellectual Property Rights	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.
Intermediate Certification Authority (Intermediate CA)	A Certification Authority whose Certificate is located within a Certificate Chain between the Certificate of the root CA and the Certificate of the Certification Authority that issued the end-user Subscriber's Certificate.
International Organization	An International Organization is an organization founded by a constituent document, e.g., charter, treaty, convention, or similar document, signed by, or on behalf of, a minimum of two or more Sovereign State governments.
Key Generation Ceremony	A procedure whereby a CA's or RA's key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.
Key Manager Administrator	An Administrator that performs key generation and recovery functions for a Managed PKI Customer using Managed PKI Key Manager.
Key Recovery Block (KRB)	A data structure containing a Subscriber's private key that is encrypted using an encryption key. KRBs are generated using Managed PKI Key Manager software.
Key Recovery Service	A VeriSign service that provides encryption keys needed to recover a Key Recovery Block as part of a Managed PKI Customer's use of Managed PKI Key Manager to recover a Subscriber's private key.
Managed PKI	VeriSign's fully integrated managed PKI service that allows enterprise Customers of VeriSign and its Affiliates to distribute Certificates to individuals, such as employees, partners, suppliers, and customers, as well as devices, such as servers, routers, and firewalls. Managed PKI permits enterprises to secure messaging, intranet, extranet, virtual private network, and e-commerce applications.
Managed PKI Administrator	An Administrator that performs validation or other RA functions for an Managed PKI Customer.

Term	Definition
Managed PKI Control Center	A web-based interface that permits Managed PKI Administrators to perform Manual Authentication of Certificate Applications
Managed PKI Key Manager	A key recovery solution for those Managed PKI Customers choosing to implement key recovery under a special Managed PKI Agreement.
Managed PKI Key Management Service Administrator's Guide	A document setting forth the operational requirements and practices for Managed PKI Customers using Managed PKI Key Manager.
Manual Authentication	A procedure whereby Certificate Applications are reviewed and approved manually one-by-one by an Administrator using a web-based interface.
NetSure Protection Plan	An extended warranty program, which is described in CP § 9.2.3.
Nonverified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.
Non-repudiation	An attribute of a communication that provides protection against a party to a communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the identity associated with the sender is unknown. Note: only an adjudication by a court, arbitration panel, or other tribunal can ultimately prevent repudiation. For example, a digital signature verified with reference to a VTN Certificate may provide proof in support of a determination of Non-repudiation by a tribunal, but does not by itself constitute Non-repudiation.
Offline CA	VeriSign PCAs, Issuing Root CAs and other designated intermediate CAs that are maintained offline for security reasons in order to protect them from possible attacks by intruders by way of the network. These CAs do not directly sign end user Subscriber Certificates.
Online CA	CAs that sign end user Subscriber Certificates are maintained online so as to provide continuous signing services.
Online Certificate Status Protocol (OCSP)	A protocol for providing Relying Parties with real-time Certificate status information.
Operational Period	The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.
Parent Company	Parent Company: A parent company is defined as a company that owns a majority of the Subsidiary Company and this can be verified by referencing a QIIS or from financial statement supplied by a registered Chartered Professional Accountant (CPA) or equivalent outside of the USA.
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKCS #12	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
Policy Management Authority (PMA)	The organization within VeriSign responsible for promulgating this policy throughout the VTN.
Primary Certification Authority (PCA)	A CA that acts as a root CA for a specific Class of Certificates, and issues Certificates to CAs subordinate to it.
Principal Individual(s)	Individuals of a Private Organization, Government Entity or Business Entity that are either owners, partners, managing members, directors or officers, as identified by their title of employment, or an employee, contractor or agent authorized by such entity or organization to conduct business related to the request, issuance and use of EV Certificates.
Processing Center	An organization (VeriSign or certain Affiliates) that creates a secure facility housing, among other things, the cryptographic modules used for the issuance of Certificates. In the Consumer and Web Site lines of business, Processing Centers act as CAs within the VTN and perform all Certificate lifecycle services of issuing, managing, revoking, and renewing Certificates. In the Enterprise line of business, Processing Centers provide lifecycle services on behalf of their Managed PKI Customers or the Managed PKI Customers of the Service Centers subordinate to them.
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system. The VTN PKI consists of systems that collaborate to provide and implement the VTN.
Registration Agency	A Governmental Agency that registers business information in connection with an entity's business formation or authorization to conduct business under a license, charter or other certification. A Registration Agency MAY include, but is not limited (i) a State Department of Corporations or a Secretary of State; (ii) a licensing agency, such as a State Department

Term	Definition
	of Insurance; or (iii) a chartering agency, such as a state office or department of financial regulation, banking or finance, or a federal agency such as the Comptroller of Currency (OCC) or Office of Thrift Supervision (OTC)
Registration Authority (RA)	An entity approved by a CA to assist Certificate Applicants in applying for Certificates, and to approve or reject Certificate Applications, revoke Certificates, or renew Certificates.
Regulated Financial Institution	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.
Relying Party	An individual or organization that acts in reliance on a certificate and/or a digital signature.
Relying Party Agreement	An agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a Relying Party.
Retail Certificate	A Certificate issued by VeriSign or an Affiliate, acting as CA, to individuals or organizations applying one by one to VeriSign or an Affiliate on its web site.
Roaming Subscriber	A Subscriber using the VeriSign Roaming Service whose private key is encrypted and decrypted with a symmetric key that is split between the VeriSign Roaming Server and an Enterprise Roaming Server.
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
RSA Secure Server Certification Authority (RSA Secure Server CA)	The Certification Authority that issues Secure Server IDs.
RSA Secure Server Hierarchy	The PKI hierarchy comprised of the RSA Secure Server Certification Authority.
Secret Share	A portion of a CA private key or a portion of the activation data needed to operate a CA private key under a Secret Sharing arrangement.
Secret Sharing	The practice of splitting a CA private key or the activation data to operate a CA private key in order to enforce multi-person control over CA private key operations under CP § 6.2.2.
Secure Server ID	A Class 3 organizational Certificate used to support SSL sessions between web browsers and web servers.
Secure Sockets Layer (SSL)	The industry-standard method for protecting Web communications developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a Transmission Control Protocol/Internet Protocol connection.
Security and Audit Requirements Guide	A VeriSign document that sets forth the security and audit requirements and practices for Processing Centers and Service Centers.
Security and Practices Review	A review of an Affiliate performed by VeriSign before an Affiliate is permitted to become operational.
Service Center	An Affiliate that does not house Certificate signing units for the issuance of Certificates for the purpose of issuing Certificates of a specific Class or type, but rather relies on a Processing Center to perform issuance, management, revocation, and renewal of such Certificates.
Sovereign State	A Sovereign state is a state, or country, that administers its own government, and is not dependent upon, or subject to, another power.
Subdomain	The portion of the VTN under control of an entity and all entities subordinate to it within the VTN hierarchy.
Subject	The holder of a private key corresponding to a public key. The term "Subject" can, in the case of an organizational Certificate, refer to the equipment or device that holds a private key. A Subject is assigned an unambiguous name, which is bound to the public key contained in the Subject's Certificate.
Subscriber	In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organizational Certificate, an organization that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. A Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate.
Subscriber Agreement	An agreement used by a CA or RA setting forth the terms and conditions under which an individual or organization acts as a Subscriber.
Subsidiary Company	A subsidiary company is defined as a company that is majority owned by Applicant as verified by referencing a QIIS or from financial statement supplied by a registered Chartered Professional Accountant (CPA) or equivalent outside of the USA.
Superior Entity	An entity above a certain entity within a VTN hierarchy (the Class 1, 2, or 3 hierarchy).
Supplemental Risk	A review of an entity by VeriSign following incomplete or exceptional findings in a

Term	Definition
Management Review	Compliance Audit of the entity or as part of the overall risk management process in the ordinary course of business.
Reseller	An entity marketing services on behalf of VeriSign or an Affiliate to specific markets.
Trusted Person	An employee, contractor, or consultant of an entity within the VTN responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices as further defined in CP § 5.2.1.
Trusted Position	The positions within a VTN entity that must be held by a Trusted Person.
Trustworthy System	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognized in classified government nomenclature.
VeriSign	Means, with respect to each pertinent portion of this CPS, VeriSign, Inc. and/or any wholly owned VeriSign subsidiary responsible for the specific operations at issue.
VeriSign Digital Notarization Service	A service offered to Managed PKI Customers that provides a digitally signed assertion (a Digital Receipt) that a particular document or set of data existed at a particular point in time.
VeriSign Repository	VeriSign's database of Certificates and other relevant VeriSign Trust Network information accessible on-line.
VeriSign Roaming Server	A server residing at VeriSign's Processing Center used in conjunction with the VeriSign Roaming Service to hold portions of symmetric keys used to encrypt and decrypt Roaming Subscribers' private keys.
VeriSign Roaming Service	The service offered by VeriSign that enables a Subscriber to download his or her private key and perform private key operations on different client terminals.
VeriSign Trust Network (VTN)	The Certificate-based Public Key Infrastructure governed by the VeriSign Trust Network Certificate Policies, which enables the worldwide deployment and use of Certificates by VeriSign and its Affiliates, and their respective Customers, Subscribers, and Relying Parties.
VTN Participant	An individual or organization that is one or more of the following within the VTN: VeriSign, an Affiliate, a Customer, a Universal Service Center, a Reseller, a Subscriber, or a Relying Party.
VTN Standards	The business, legal, and technical requirements for issuing, managing, revoking, renewing, and using Certificates within the VTN.

Appendix B1

Supplemental Validation Procedures for Extended Validation SSL Certificates

TABLE OF CONTENTS

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

	(d)	Qualified Independent Information Sources (QIIS)	
	(e)	Qualified Government Information Sources (QGIS)	
23.		Other Verification Requirements	
	(a)	High Risk Status	
	(b)	Denied Lists and Other Legal Black Lists	
24.		Final Cross-Correlation and Due Diligence	
25.		Certificate Renewal Verification Requirements	
G.		CERTIFICATE STATUS CHECKING AND REVOCATION ISSUES	
		EV Certificate Status Checking	
		EV Certificate Revocation	
		EV Certificate Problem Reporting and Response Capability	
H.		EMPLOYEE AND THIRD PARTY ISSUES.....	
		Trustworthiness and Competence	
		Delegation of Functions to Registration Authorities and Subcontractors	
I.		DATA AND RECORD ISSUES	
		Documentation and Audit Trail Requirements.....	
		Document Retention.....	
	(a)	Audit Log Retention	
	(b)	Retention of Documentation	
		Reuse and Updating Information and Documentation	
	(a)	Use of Documentation to Support Multiple EV Certificates.....	
	(b)	Use of Pre-Existing Information or Documentation.....	
		Data Security.....	
J.		COMPLIANCE.....	
		Audit Requirements	
	(a)	Pre-Issuance Readiness Audit.....	
	(b)	Regular Self Audits	
	(c)	Annual Independent Audit.....	
	(d)	Auditor Qualifications	
	(e)	Root Key Generation	
K.		OTHER CONTRACTUAL COMPLIANCE	
		Privacy Issues	
		Limitations on EV Certificate Liability	
	(a)	CA Liability	

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 or Registration Agency in the Subject’s Jurisdiction of Incorporation or Registration 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 or Registration;
- 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 or Registration Agency in the Subject’s Jurisdiction of Incorporation or Registration, 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(s) 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 the 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 a company 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, Business Entities 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 or Registration Agency, or Governing Body in its Jurisdiction of Incorporation or Registration (e.g., by issuance of a certificate of incorporation) or is an entity that is chartered by a state or federal regulatory agency;
- (2) The organization MUST have designated with the Incorporating or Registration Agency, or Governing Body either a Registered Agent, or a Registered Office (as required under the laws of the Jurisdiction of Incorporation Registration) or an equivalent facility;
- ;
- (3) The organization MUST not be designated on the records of the Incorporating or Registration Agency, or Governing Body by labels such as "inactive," "invalid," "not current," or the equivalent;
- (4) The Private organization MUST have a verifiable physical existence and business presence;
- (5) The organization's Jurisdiction of Incorporation, Registration, Charter, or License 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
- (6) 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 political subdivision in which such Government Entity operates.;
- (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) Business Entities. VeriSign MAY issue EV Certificates to Business Entities that satisfy the following requirements:

- (1) The Business Entity MUST be a legally recognized entity whose formation included the filing of certain forms with the Registration Agency in its Jurisdiction ,the issuance or approval by such Registration Agency of a charter, certificate, or license, and whose existence can be verified with that Registration Agency;
- (2) The Business Entity MUST have a verifiable physical existence and business presence;

- (3) At least one Principal Individual associated with the Business Entity MUST be identified and validated. ;
- (4) The identified Principal Individual MUST attest to the representations made in the Subscriber Agreement;
- (5) Where the Business Entity represents itself under an assumed name, VeriSign verifies the Business Entity's use of the assumed name pursuant to the requirements of Section 15 herein;

(d) Non-Commercial Entity Subjects

VeriSign MAY issue EV Certificates to Non-Commercial Entities who do not qualify under subsections (b), (c) and (d) but satisfy the following requirements:

(1) International Organization Entity Subjects

- (i) The International Organization Entity is created under a Charter, Treaty, Convention or equivalent instrument that was signed by, or on behalf of, more than one country's government. The CABForum may publish a listing of International Organizations that have been approved for EV eligibility, and
- (ii) The International Organization Entity MUST NOT be headquartered in any country where VeriSign is prohibited from doing business or issuing a certificate by the laws of the VeriSign's jurisdiction; and
- (iii) The International Organization Entity MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the VeriSign's jurisdiction. Subsidiary organizations or agencies of qualified international organizations may also qualify for EV certificates issued in accordance with these Guidelines.

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 or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified as provided herein. VeriSign MAY abbreviate the organization prefixes or suffixes in the Organization name, e.g., if the QGIS shows "**Company Name* Incorporated" VeriSign MAY include *Company Name*, inc. VeriSign uses common abbreviations that are generally accepted in the Jurisdiction of Incorporation or Registration.

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 characters as defined by RFC 5280, VeriSign will use only the full legal organization name in the certificate.

If the Organization name by itself exceeds 64 characters, VeriSign MAY abbreviate parts of organization name, and/or omit non-material words in the organization name in such a way that the name in the certificate does not exceed the 64 character limit, and a Relying Party will not be misled into thinking they are dealing with a different Organization.

(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 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) Business Category:

The Business Category is included in the subject:businessCategory (OID 2.5.4.15)

This field contains one of the following strings: ‘V1.0, Clause 5.(b)’, ‘V1.0, Clause 5.(c)’ or ‘V1.0, Clause 5.(d)’, depending whether the Subject qualifies under the terms of Section 5b, 5c, or 5d of the Guidelines, respectively.

Subject Type	Business Category string
Private Organization	V1.0, Clause 5.(b)
Government Entity	V1.0, Clause 5.(c)
Business Entity	V1.0, Clause 5.(d)
Non-Commercial Entities:	V1.0, Clause 5.(3)

Table 1 Business category field content

(4) Jurisdiction of Incorporation or Registration

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

Address Part	Required/Optional	Certificate Field
Locality	If required	jurisdictionOfIncorporationLocalityName (OID 1.3.6.1.4.1.311.60.2.1.1) ASN.1 - X520LocalityName as specified in RFC 5280
State or province (if any)	If required	jurisdictionOfIncorporationStateOrProvinceName (OID 1.3.6.1.4.1.311.60.2.1.2) ASN.1 - X520StateOrProvinceName as specified in RFC 5280
Country	Required	jurisdictionOfIncorporationCountryName (OID 1.3.6.1.4.1.311.60.2.1.3) ASN.1 - X520countryName as specified in RFC 5280

Table2. Jurisdiction of Incorporation Certificate Fields

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

(5) Registration Number

VeriSign EV Certificates include the unique Registration (or similar) Number assigned to the Subject by the Incorporating or Registration 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.

For Government Entities that do not have a Registration Number or readily verifiable date of creation, VeriSign enters appropriate language to indicate that the Subject is a Government Entity.

(6) 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 (OID 2.5.4.17)

Table 3. 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 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 – 13 months;
- Assumed name – 13 months;

- Address of Place of Business – 13 months, 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 – 13 months;
- Bank account verification – 13 months;
- Domain name – 13 months;
- Identity and authority of Certificate Approver – 13 months, 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
- 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

- **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.
- **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.

- **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 Organizational 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 or, having obtained it from a reliable source, confirm it with 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 or Registration (for Private Organizations), or as specified in the law of the political subdivision in which the Government Entity operates (for Government Entities), or as registered with the government business Registration Agency (for Business 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 or Registration: Applicant's Jurisdiction of Incorporation or Registration 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 or Registration Agency: The name of the Applicant's Incorporating or Registration Agency;
- Registration Number: The registration number assigned to Applicant by the Incorporating or Registration Agency in Applicant's Jurisdiction of Incorporation or

Registration 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

(A) private Organizations

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

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

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

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 or Registration.

(B) Government Agencies

VeriSign verifies that the Applicant is a legally recognized Government Entity, in existence in the political subdivision in which such Government Entity operates, and that Applicant's formal legal name matches Applicant's name in the EV Certificate Request. VeriSign will obtain Applicant's date of incorporation, registration, or formation, or the identifier for the legislative act that created the Government Entity. In circumstances where this information is not available, VeriSign MUST enter appropriate language to indicate that the Subject is a Government Entity

Government Entities are verified directly with, or obtained directly from, one of the following:

- a. a QGIS in the political subdivision in which such Government Entity operates; or
- b. A superior governing Government Entity in the same political subdivision as Applicant (e.g. a Secretary of State may verify the legal existence of a specific State Department), or
- c. From a judge that is an active member of the federal, state or local judiciary within that political subdivision, or
- d. An attorney representing the Government Entity.

Such verification MAY be by direct contact with the appropriate Government Entity in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained from a Qualified Independent Information Source.

Any communication from a judge SHALL be verified in the same manner as is used for verifying factual assertions that are asserted by an Attorney as set forth in Section 22(a) of the Guidelines.

(C) Business Entities

To verify a Business Entity's legal existence and identity VeriSign verifies that the Entity is engaged in business under the name submitted by Applicant in the Application. VeriSign verifies that the Applicant's formal legal name as recognized by the Registration Authority in Applicant's Jurisdiction of Registration matches Applicant's name in the EV Certificate Request. VeriSign records the specific unique Registration Number assigned to Applicant by the Registration Agency in Applicant's Jurisdiction of Registration. Where the Registration Agency does not assign a Registration Number, the Applicant's date of Registration will be recorded. In addition, the identity of a Principal Individual associated with the Business Entity is verified in accordance with Section 14(b)(4) of the EV Guidelines.

(D) Non-Commercial Entities

(1) International Organization Entities

VeriSign verifies that Applicant is a legally recognized International Organization Entity and that Applicant's formal legal name matches Applicant's name in the EV Certificate Request. Such verification . VeriSign will also obtain Applicant's date of formation, or the identifier for the legislative act that created the International Organization Entity. In circumstances where this information is not available, VeriSign MUST enter appropriate language to indicate that the Subject is an International Organization Entity.

The International Organization Entity is verified either:

- With reference to the constituent document under which the International Organization was formed; or
- Directly with a signatory country's government in which the VeriSign is permitted to do business. Such verification may be obtained from an appropriate government agency or from the laws of that country, or by verifying that the country's government has a mission to represent it at the International Organization; or
- Directly against any current list of qualified entities that the CABForum may maintain at www.cabforum.org.
- In cases where the International Organization applying for the EV certificate is an organ or agency - including a non-governmental organization (NGO) of a verified International Organization, then VeriSign may verify the International Organization applicant directly with the verified umbrella International Organization of which the applicant is an organ or agency.

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 or Registration Agency in Applicant's Jurisdiction of Incorporation or Registration, 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, VeriSign verifies that the physical address provided by Applicant is an address where Applicant or a Parent/Subsidiary Company conducts business operations (e.g., not a mail drop or P.O. Box), and is the address of Applicant's Place of Business.

For Government Entity Applicants, the address contained in the records of the QGIS in Applicant's Jurisdiction shall be regarded as the verified address.

For other entities, 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 or Registration:
- (1) For Applicants listed at the same Place of Business address in the current version of at least one (1) Qualified Independent Information Source, or a Qualified Governmental Tax Information Source (QGTIS), VeriSign confirms that the Applicant's address as listed in the EV Certificate Request is a valid business address for Applicant or a Parent/Subsidiary Company by reference to such Qualified Independent Information Sources, or a QGTIS, 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, or a QGTIS, VeriSign may confirm that the is in fact Applicant's or a Parent/Subsidiary Company'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 or Registration, VeriSign requires a Verified Legal Opinion that indicates the address of Applicant's or a Parent/Subsidiary Company 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. A listing in a Parent/Subsidiary Company's name at that address is acceptable.

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 a Qualified Governmental Tax Information Source; or
- (B) During a site visit, the person who is conducting the site visit MUST confirm the Applicant's or Parent/Subsidiary Company'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.

For Government Entity Applicants, VeriSign may rely on the telephone number contained in the records of the QGIS in Applicant's Jurisdiction.

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 or registration agency indicates that the Applicant has been in existence for less than three (3) years, , and the Applicant is not listed in either the current version of one (1) Qualified Independent Information Source or a Qualified

Governmental Tax Information Source, , VeriSign verifies that the Applicant has the ability to engage in business.

In the absence of a verified legal or accountant opinion confirming an active current Demand Deposit Account with a regulated financial institution, 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.

For Government Entity Applicants, the VeriSign MAY rely on the domain name listed for that entity in the records of the QGIS in Applicant's Jurisdiction to verify Domain Name.

- (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. Confirmation that the registered owner of the domain name is a Parent/Subsidiary Company of Applicant, or a registered trading name of Applicant is sufficient to establish that Applicant is the registered owner of the domain name.

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, that it controls the confirmed domain name.

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;

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.

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.

- (5) **Prior Equivalent Authority:** The signing authority of the Contract Signer, and/or the EV authority of the Certificate Approver, MAY be verified by relying on a demonstration of Prior Equivalent Authority.
Prior Equivalent Authority of a Contract Signer MAY be relied upon for confirmation or verification of the signing authority of the Contract Signer when the Contract Signer has executed a binding contract between the VeriSign and/or its parents or Subsidiaries and the Applicant with a legally valid and enforceable seal or handwritten signature and only when the contract was executed more than 90 days prior to the EV certificate application. VeriSign MUST record sufficient details of the previous agreement to correctly identify it and associate it with the EV application. Such details MAY include any of the following:

1. Agreement title Date of Contract Signer's signature

2. Contract reference number
3. Filing location

Prior Equivalent Authority of a Certificate Approver MAY be relied upon for confirmation or verification of the EV authority of the Certificate Approver when the Certificate Approver has performed one or more of the following:

- (1) Under contract to VeriSign and/or a Parent/Subsidiary, has served (or is serving) as an Enterprise RA for the Applicant
- (2) Has participated in the approval of one or more SSL certificates issued by the CA, which are currently in use on public servers operated by the Applicant. In this case VeriSign and/or a Parent/Subsidiary MUST have contacted the Certificate Approver by phone at a previously validated phone number or have accepted a signed and notarized letter approving the certificate request.

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 Registration 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 Registration 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. In circumstances where the opinion is digitally signed, in a manner that confirms the authenticity of the document and the identity of the signer, as verified by VeriSign in Section 22(b)(2)(A), no further verification of authenticity is required.

(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 Registration 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. In circumstances where the opinion is digitally signed, in a manner that confirms the authenticity of the document and the identity of the signer, as verified by VeriSign in Section 22(b)(2)(A), no further verification of authenticity is required.

(c) Face-to-face Validation of Principal Individual

Before relying on any face-to-face vetting documents VeriSign verifies that the Third-Party Validator meets the following requirements:

- (A) Qualification of Third-Party Validator. VeriSign independently verifies that the Third-Party Validator is a legally-qualified Latin Notary or Notary (or legal equivalent in Applicant's jurisdiction), Lawyer, or Accountant in the jurisdiction of the individual's residency, by directly contacting the authority responsible for registering or licensing such Third-Party Validators in the applicable jurisdiction.
- (B) Document chain of custody. VeriSign verifies that that the Third-Party Validator viewed the Vetting Documents in a face-to-face meeting with the individual being validated. The Third party validator must attest that they obtained the Vetting Documents submitted to the CA for the individual during a face-to-face meeting with the individual.

- (C) If the Third-Party Validator is not a Latin Notary, then VeriSign confirms the authenticity of the attestation and vetting documents, by making a telephone call to the Third-Party Validator and obtaining confirmation from them or their assistant that they performed the face-to-face validation. VeriSign may rely upon self-reported information obtained from the Third-Party Validator for the sole purpose of performing this verification process. In circumstances where the attestation is digitally signed, in a manner that confirms the authenticity of the documents, and the identity of the signer as verified by VeriSign in Section 22(c)(2)(A), no further verification of authenticity is required.

(d) 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 or Registration as listed in the official records of the Incorporating or Registration Agency, with instructions that it be forwarded to an appropriate Confirming Person.
- (iii) A named individual verified to be in the direct line of management above the Contract Signer or Certificate Approver by contacting Applicant’s Human Resources Department by phone or mail (at the verified phone number or address for Applicant’s Place of Business)

(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 Qualified Government Tax 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 or Registration.
- (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 Qualified Government Tax 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.
- (3) VeriSign MAY rely on a verified Confirming Person to confirm their own contact information: email address, telephone number, and facsimile number. VeriSign may rely on this verified contact information for future correspondence with the Confirming Person if:
1. The domain of the e-mail address is owned by the Applicant and is the Confirming Person's own e-mail address and not a group e-mail alias,
 2. The Confirming Person's telephone/fax number is verified by VeriSign to be a telephone number that is part of the organization's telephone system, and is not the personal phone number for the person.

(e) 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.

(f) 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. VeriSign may use third-party vendors to obtain the information from the Government Entity provided that the third party obtains the information directly from the Government Entity.

(g) Qualified Government Tax Information Source (QGTIS). A Qualified

Governmental Information Source that specifically contains tax information relating to Private Organizations, Business Entities or Individuals (e.g. the I.R.S. in the United States).

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 Registration 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 Registration 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.

EV Certificate Renewal is the process whereby an Applicant who has a valid unexpired and non-revoked EV certificate makes application, to the CA that issued the original certificate, for a newly issued EV certificate for the same organizational and domain name prior to the expiration of the applicant's existing EV Certificate.

(a) Validation for Renewal Requests. In conjunction with the EV Certificate Renewal process, VeriSign performs all authentication and verification tasks required by their CPS to ensure that the renewal request is properly authorized by Applicant and that the information in the EV Certificate is still accurate and valid.

(b) Exceptions. Notwithstanding the requirements set forth in Section 33(b) (Use of Pre-Existing Information or Documentation) and Section 8 (Maximum Validity Period), VeriSign, when performing the authentication and verification tasks for EV Certificate Renewal MAY:

(1) EV Certificate previously issued by VeriSign:

(i) Rely on its prior authentication and verification of:

(a) A Principal Individual of a Business Entity under Section 14(b)(4) if the Principal Individual is the same as the Principal Individual verified by the CA in connection with the previously issued EV Certificate,

(b) Applicant's Place of Business under Section 16(a),

(c) The verification of telephone number of Applicant's Place of Business required by Section 16(b), but still MUST perform the verification required by Section 16(b)(2)(a),

(d) Applicant's Operational Existence under Section 17,

(e) The name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester under Section 19, except where a contract is in place between VeriSign and Applicant that specifies a specific term for the authority of the Contract Signer, and/or the Certificate Approver, and/or Certificate Requester in which case, the term specified in such contract will control,

(f) The prior verification of the email address used by VeriSign for independent confirmation from applicant under Section 22(d)(1)(B)(ii).

(ii) Rely on prior Verified Legal/Accountant Opinion that established:

(a) Applicant's exclusive right to use the specified domain name under Section 18 (b)(2)(A)(1) & Section 18 (b)(2)(B)(1), provided that VeriSign verifies that either:

a. The WHOIS record still shows the same registrant as indicated when VeriSign received the prior Verified Legal Opinion, or

b. The Applicant establishes domain control via a practical demonstration as detailed in Section 18(b)(2)(B)(2).

(b) Verification that Applicant is aware that it has exclusive control of the domain name, under Section 18 (a)(b)(3).

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 be updated and reissued at least every seven (7) days, and the nextUpdate field value SHALL NOT be more than 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 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/Confidentiality 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

	Certificate issued on or before 31 Dec 2010	Certificate issued after 31 Dec 2010
Digest algorithm	MD5 (NOT RECOMMENDED), SHA-1	SHA-1*, SHA-256, SHA-384 or SHA-512
RSA	2048 bit (An end-entity certificate MAY, in addition, chain to an EV-enabled 1024-bit RSA root CA certificate key.)	2048 bit
ECC	224, 233, 256 or 283 bits	224, 233, 256 or 283 bits

2. Subordinate CA Certificates

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

3. Subscriber Certificates

	Certificate issued on or before 31 Dec 2010	Certificate issued after 31 Dec 2010
Digest algorithm	SHA-1	SHA1*, SHA-256, SHA-384 or SHA-512
RSA	1024 bit or 2048 bit (Note: subscriber certificates containing a 1024 bit RSA key MUST expire on or before 31 Dec 2010)	2048 bit
ECC	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 5280.

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 5280]

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 5280.

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 5280]

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.

(f) extKeyUsage

Either the value id-kp-serverAuth [RFC5280] or id-kp-clientAuth [RFC5280] or both values MUST be present. Other values SHOULD NOT be present.

All other fields and extensions set in accordance to RFC 5280.

Appendix B4

Foreign Organization Name Guidelines

NOTE: This appendix is only relevant to EV applications from countries that do not have Latin character organization name registrations. More specific information for particular countries may be added to this appendix in the future.

Where an EV Applicant's organization name is not registered with a QGIS in Latin characters and the applicant's foreign character organization name and registration have been verified with a QGIS in accordance with these Guidelines, VeriSign MAY include a Latin character organization name in the EV certificate. In such a case, the CA MUST follow the procedures laid down in this appendix.

Romanized Names

In order to include a transliteration/Romanization of the registered name, the Romanization MUST be verified by VeriSign using a system officially recognized by the Government in the Applicant's jurisdiction of incorporation.

If VeriSign can not rely on a transliteration/Romanization of the registered name using a system officially recognized by the Government in the Applicant's jurisdiction of incorporation, then it MUST rely on one of the options below, in order of preference:

- A system recognized by the International Standards Organization (ISO),
- A system recognized by the United Nations or
- A Lawyers Opinion confirming the Romanization of the registered name.

English Name

In order to include a Latin character name that is not a Romanization of the registered name in the EV certificate, VeriSign MUST verify that the Latin character name is:

- Included in the Articles of Incorporation (or equivalent document) filed as part of the organization registration, or
- Recognized by a QGTIS in the Applicant's Jurisdiction of Incorporation as the applicant's recognized name for tax filings, or
- Confirmed with a QIIS to be the name associated with the registered organization, or
- Confirmed by a lawyer's opinion letter to be the trading name associated with the registered organization.

Country Specific Procedures

F-1. Japan

In addition to the procedures set out above:

- The Hepburn method of Romanization is acceptable for Japanese Romanizations.
- VeriSign MAY verify the Romanized transliteration of Applicant's formal legal name with either a QIIS or a lawyer's opinion letter.
- VeriSign MAY use the Financial Services Agency to verify an English Name. When used, VeriSign MUST verify that the English name is recorded in the audited Financial Statements filed with the Financial Services Agency.
- When relying on Articles of Incorporation to verify an English Name, the Articles of Incorporation MUST be accompanied either: by a document, signed with the original Japanese Corporate Stamp, that proves that the Articles of Incorporation are authentic

and current, or by a lawyer's opinion letter. VeriSign MUST verify the authenticity of the Corporate Stamp.

Appendix C: History of Changes

History of changes: version 3.8.1

Section	Description
Section 6.3.2 footnote 20	Added: "With the exception of the VeriSign Automated Administration certificate ..."
Appendix B1 Section 8	Updated maximum validity period from one year to thirteen months
Appendix B1 Section 22(d)(3)	Created section 22(d)(3)
Appendix B1 Section 25	Deleted: "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." Replaced this paragraph with content consistent with published errata to the EV Guidelines. Also included a definition of renewal consistent with the Guidelines.
Appendix B3 Section 3	Added: "(f) extKeyUsage"
Appendix B1-B4 and throughout document	Replaced all references to RFC 3280 with RFC 5280

History of changes: version 3.8

Section	Description
Section 6.3.2 – table 8	Updated validity period for Online CA to End-Entity Organizational Subscriber from 3 to 5 years. Fn 17. updated fn to include the "Class 3 Secure Server Operational Administrator CA" Fn 20. Added a footnote that "At a minimum, the Distinguished Name of four and five year validity SSL certificates is reverified after three years from date of certificate issuance"

History of changes: version 3.7

Section	Description
Section 1.3.1	Added: "VeriSign also operates the "VeriSign Universal Root Certification Authority". The "VeriSign Universal Root Certification Authority" is not defined under a particular certificate Class, and may issue any class of Subordinate CA."
Section 6.3.2	Deleted: "VeriSign also operates the VeriSign Class 3 International Server CA which is an online CA signed by a PCA. The validity of this CA may exceed the validity periods described in Table 8 above in order to meet certain contractual obligations with browser vendors regarding the use of SGC/step up technology, and ensure continued interoperability of certificates offering this capability." Added : "VeriSign also operates the "VeriSign Class 3 International Server CA" and the "Class 3 Open Financial

	Exchange CA - G2" which are online CAs signed by a PCA. The validity of these CAs may exceed the validity periods described in Table 8 above to ensure continued interoperability of certificates offering SGC and OFX capability."
Section 6.3.2	Deleted: "Affected CAs shall not be extended beyond December 31, 2010 in terms of this exception" Added: "This exception may not be used to extend a CA's validity beyond a 13 year total validity, and shall not be made available after April 30, 2011."
Section 6.3.2	Added Footnote: "1 Certificate validity periods may be extended beyond the limits set in Section 6.3.2 for certificates using stronger encryption algorithms or key lengths are used, e.g. the use of SHA 2 or ECC algorithms and/or the use of 2048 bit or larger keys."
Section 7.1.3	Added two algorithms: 1. sha256withRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsads(113549) pkcs(1) pkcs-1(1) 11} 2. ecdsa-with-Sha384 OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 3}
Appendix B1 Section 16 (a)	Updated to allow for verification of address of a or a Parent/Subsidiary Company
Appendix B1 Section 5	Added Non-Commercial Entity Subjects
Appendix B1 Section 6(a)3 – table 1	Added: Non-Commercial Entities: V1.0, Clause 5.(3)
Appendix B1 Section 14	Added: Government Entities and Non-Commercial Entities
Appendix B1 Section 19	Added Prior Equivalent Authority
Appendix B4	Updated Appendix A4 in line with published errata to the EV Guidelines
Definitions	Added: "Country": "Sovereign State": "International Organization": "Parent Company" Updated "Subsidiary Company" to be a majority owned and not a wholly owned company.

History of changes: version 3.6

Section	Description
Section 4.1.2.1	Changed " demonstrating possession of the private key corresponding to the public key delivered to VeriSign." to "demonstrating possession and/or exclusive control of the private key corresponding to the public key delivered to VeriSign. "
Section 6.1.1	Changed " 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. " To "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, at a minimum , meets the requirements of FIPS 140-1 level 3. "
Section 6.2.5	Deleted: "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."
Section 6.3.2	Added "In terms of Section 6.3.2 of the VTN CP, the VeriSign PMA has approved an exception to extend a limited number CAs beyond the specified limits, in order to ensure uninterrupted PKI services during CA key pair migration. Affected CAs shall not be extended beyond December 31, 2010 in terms of this exception. "

Section 7.1	Update "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 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 ("RFC 5280")." To "VeriSign Certificates conform generally to (a) ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 and (b) RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 ("RFC 5280")."
Section 7.1.2.1	Deleted "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" Added: "Note: The nonRepudiation bit is not required to be set in these Certificates because the PKI industry has not yet reached a consensus as to what the nonRepudiation bit means. Until such a consensus emerges, the nonRepudiation bit might not be meaningful for potential Relying Parties. Moreover, the most commonly used applications do not always respect the nonRepudiation bit. Therefore, setting the bit might not help Relying Parties make a trust decision. Consequently, this CPS does not require that the nonRepudiation bit be set. It may be set in the case of dual key pair signature Certificates issued through Managed PKI Key Manager, or as otherwise requested. Any dispute relating to non-repudiation arising from the use of a digital certificate is a matter solely between the Subscriber and the Relying Party(s). VeriSign shall incur no liability in relation thereto." Added footnote: "The nonRepudiation bit may also be referred to as ContentCommitment in Digital Certificates in accordance with the X.509 standard."
Section 9.13.2	Updated Jurisdiction from Santa Clara County, California to Fairfax County, Virginia
Section 9.14	Updated Governing Law from State of California to Commonwealth of Virginia

History of changes: version 3.5

Section 6.2.5	Deleted: "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." Added: "Upon expiration of a VeriSign CA Certificate, the key pair associated with the certificate will be securely retained for a period of at least 5 years using hardware cryptographic modules that meet the requirements of this CPS. These CA key pairs shall not be used for any signing events after their expiration date, unless the CA Certificate has been renewed in terms of this CPS."
Section 6.2.10	Deleted: "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."
Section 6.3.2	Added: "End user Subscriber Certificates that are renewals of existing subscriber certificates may have a longer validity period (up to 3 months)."
Section 6.3.2 – table 8	Updated "Online CA to End-Entity Organizational Subscriber" to reflect a validity "Normally up to 3 years".
Section 7.1.4	Clarification added that an OU pointing to a Relying party Agreement in the Subject name is optional as long as the Relying Party Agreement is linked to from the Policyextension.
Section 9.8	Updated Liability Caps for Netsure to \$50,000 US to \$250,000 US. From \$1,000 US to \$1,000,000.00 US
Definitions	"NetSure Protection Plan": Updated definition with correct CPS Section reference. Added: "Principal Individual", "Subsidiary Company", "Registration Agency"
Appendix B1-B4	Updated EV procedures in line with Version 1.0 of the EV Guidelines issued by the CA/Browser Forum.

History of changes: version 3.4

Section 1.1	Added Footnote: "Authenticated Content Signing Certificates (ACS) are issued by a non-VTN CA. However, reference is made to these certificates in certain sections of this VeriSign CPS, for ACS customers to understand certain procedural differences used for these certificates."
Section 3.2.3 Table 7	Added Verification requirements for Shared Service Provider Certificates for non federal entities: "The identity of the Certificate Subscriber is verified substantially in compliance with the requirements of the X.509 Certificate Policy for the US Department of Homeland Security Public Key Infrastructure (PKI)"

Section 3.3.1	Added a response from a verified e-mail address for the Corporate Contact as an alternative to a challenge phrase
Section 4.6.3	Added a response from a verified e-mail address for the Corporate Contact as an alternative to a challenge phrase
Section 4.9.7	Deleted: "CRLs for CA Certificates shall be issued at least quarterly" Added: "CRLs for CA Certificates shall be issued at least annually"
Section 6.3.2	Added: "VeriSign also operates the VeriSign Class 3 International Server CA which is an online CA signed by a PCA. The validity of this CA may exceed the validity periods described in Table 8 above in order to meet certain contractual obligations with browser vendors regarding the use of SGC/step up technology, and ensure continued interoperability of certificates offering this capability."
Section 7.1.2.1	Updated to specify that: "The criticality field of the KeyUsage extension is generally set to TRUE for CA certificates and may be set to either TRUE, or FALSE for end entity Subscriber certificates."
Section 7.1.2.1- Table 10	Updated CA Criticality from "False" to "True"
Section 9.3.3	Added: "VeriSign secures private information from compromise and disclosure to third parties."
Definitions	Deleted "Affiliate Audit Program Guide"

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: " High assurance with extended validation certificates 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: o The certificate key pair is stored in hardware, and o VeriSign has authenticated the Organization in terms of this CPS and o When used to protect a server using SSL/TLS, the server is only accessible via a private network or intranet."
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"> • The challenge phrase is correctly used for the subsequent renewal certificate and: • The certificate Distinguished Name has not been changed, and • The Corporate and Technical Contact information remains unchanged from that which was previously verified, VeriSign will not have to reconfirm by telephone, confirmatory postal mail, or comparable procedure to the Certificate Applicant certain information about the organization, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Certificate Applicant is authorized to do so."
Section 7.2	Removed reference to RFC 5280
Section 7.2.1	Added that "Version 2 CRLs comply with the requirements of RFC 5280."
Section 9.2.1	Updated from: "Enterprise Customers shall maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention. This insurance requirement does not apply to governmental entities. VeriSign maintains such errors and omissions insurance coverage." to: "Enterprise Customers are encouraged to maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention. VeriSign maintains such errors and omissions insurance coverage."
Section 9.2.3	Updated Section title from "Insurance or Warranty Coverage for End-Entities" to "Extended Warranty Coverage"
Section 9.2.3	Replaced the following content: "The NetSure Protection Plan is an extended warranty program that applies within VeriSign's Subdomain of the VTN. Where it applies, the NetSure Protection Plan provides Subscribers receiving with protection against accidental occurrences such as theft, corruption, loss, or unintentional disclosure of the Subscriber's private key (corresponding to the public key in the Certificate), as well as impersonation and certain loss of use of the Subscriber's Certificate. The NetSure Protection Plan also provides protection to Relying Parties when they rely on Certificates covered by the NetSure Protection Plan. NetSure is a program provided by VeriSign and backed by insurance obtained from commercial carriers. For general information concerning the NetSure Protection Plan, and a discussion of which Certificates are covered by it, see http://www.verisign.com/netsure . The protections of the NetSure Protection Plan are also offered, for a fee, to Enterprise Customers of VeriSign. They can obtain protections under the NetSure Protection Plan subject to the terms of an appropriate agreement for this service. This service not only extends the protections of the NetSure Protection Plan to the Subscribers whose Certificate Applications are approved by the Enterprise Customer, it also extends these protections to the Enterprise Customer itself. For example, if a Managed PKI Customer approves a Certificate Application of an employee of the Managed PKI Customer, who uses the Certificate for the business purposes of the Managed PKI Customer, and if the Subscriber's actions cause a loss, the real party bearing the loss may be the Managed PKI Customer in its role as the Subscriber's employer. If covered by the NetSure Protection Plan, the Managed PKI Customer may submit a claim for the loss sustained because of the Subscriber's actions." With: "The NetSure Protection Plan is an extended warranty program that provides VeriSign SSL and code signing certificate subscribers with protection against loss or damage that is due to a defect in VeriSign's issuance of the certificate or other malfeasance caused by VeriSign's negligence or breach of its contractual obligations, provided that the subscriber of the certificate has fulfilled its obligations under the applicable service agreement. For general information concerning the NetSure Protection Plan, and a discussion of which Certificates are covered by it, see http://www.verisign.com/netsure "

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

Section 2.3	Changed reference to Section 8 to Section 9.12
-------------	--

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