

---

# VeriSign<sup>®</sup> Trust Network European Directive CP



**Version 1.2**

**September 17, 2010**



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

---

## VeriSign® Trust Network European Directive Supplemental Policies

© 2010 Symantec Corporation. All rights reserved.  
Printed in the United States of America.

Revision date: September 2010

### Important – Acquisition Notice

On August 9, 2010, Symantec Corporation completed the acquisition of VeriSign Inc's Authentication division. As a result Symantec is now the registered owner of this Certificate Practices Statement document and the PKI Services described within this document.

However a hybrid of references to both "VeriSign" and "Symantec" shall be evident within this document for a period of time until it is operationally practical to complete the re-branding of the Certification Authorities and services. Any references to VeriSign as a corporate entity should be strictly considered to be legacy language that solely reflects the history of ownership. Symantec may continue use of the "VeriSign" brand name, for example, as part of the "VeriSign® Trust Network".

### Trademark Notice

Symantec, the Symantec logo, and the Checkmark Logo are the registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. The VeriSign logo, VeriSign Trust and other related marks are trademarks and service marks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed by Symantec Corporation. Other names may be trademarks 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 Symantec Corporation.

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 Symantec Corporation.

Requests for any other permission to reproduce these VeriSign® Trust Network European Directive Supplemental Policies (as well as requests for copies) must be addressed to Symantec Corporation, 350 Ellis Street, Mountain View, CA 94043 USA Attn: Practices Development. Tel: +1 650.527.8000 Fax: +1 650.527.8050 Net: [practices@verisign.com](mailto:practices@verisign.com).

# TABLE OF CONTENTS

<b>1. Introduction</b> .....	<b>1</b>	2.8.3	Disclosure of Certificate Revocation/Suspension Information	19	
1.1	Overview	2	2.8.4	Release to Law Enforcement Officials	19
1.2	Identification	7	2.8.5	Release as Part of Civil Discovery	19
1.3	Community and Applicability	8	2.8.6	Disclosure Upon Owner’s Request	19
1.3.1	Certification Authorities	8	2.8.7	Other Information Release Circumstances	20
1.3.2	Registration Authorities	8	2.9	Intellectual Property Rights (DL1-2)	20
1.3.3	End Entities	8	2.9.1	Property Rights in Certificates and Revocation Information	20
1.3.4	Applicability	9	2.9.2	Property Rights in the CP	20
1.3.4.1	Suitable Applications	9	2.9.3	Property Rights in Names	20
1.3.4.2	Restricted Applications	9	2.9.4	Property Rights in Keys and Key Material	20
1.3.4.3	Prohibited Applications	9	<b>3. Identification and Authentication</b> .....	<b>20</b>	
1.4	Contact Details	9	3.1	Initial Registration	20
1.4.1	Specification Administration Organization	9	3.1.1	Types of Names (DL1-2)	20
1.4.2	Contact Person	10	3.1.2	Need for Names to be Meaningful (DL1-2)	20
1.4.3	Person Determining CPS Suitability for the Policy	10	3.1.3	Rules for Interpreting Various Name Forms (DL1-2)	20
<b>2. General Provisions</b> .....	<b>10</b>	3.1.4	Uniqueness of Names (DL1-2)	21	
2.1	Obligations (DL1-2)	10	3.1.5	Name Claim Dispute Resolution Procedure (DL1-2)	21
2.1.1	CA Obligations	10	3.1.6	Recognition, Authentication, and Role of Trademarks (DL1-2)	21
2.1.2	RA Obligations	12	3.1.7	Method to Prove Possession of Private Key (DL1-2)	21
2.1.3	Subscriber Obligations	13	3.1.8	Authentication of Organization Identity (DL1-2)	21
2.1.4	Relying Party Obligations	13	3.1.9	Authentication of Individual Identity (DL1-2)	21
2.1.5	Repository Obligations	14	3.2	Routine Rekey (Renewal) (DL1-2)	22
2.2	Liability (DL1-2)	14	3.3	Rekey After Revocation (DL1-2)	22
2.2.1	Certification Authority Liability	14	3.4	Revocation Request (DL1-2)	23
2.2.1.1	Certification Authority Warranties to Subscribers and Relying Parties	14	<b>4. Operational Requirements</b> .....	<b>23</b>	
2.2.1.2	Certification Authority Disclaimers of Warranties	14	4.1	Certificate Application (DL1-2)	23
2.2.1.3	Certification Authority Limitations of Liability	14	4.1.1	Certificate Applications for End-User Subscriber Certificates	23
2.2.1.4	Force Majeure	15	4.1.2	Certificate Applications for CA or RA Certificates	23
2.2.2	Registration Authority Liability	15	4.2	Certificate Issuance (DL1-2)	24
2.2.3	Subscriber Liability	15	4.2.1	Issuance of Qualified Certificates	24
2.2.4	Relying Party Liability	15	4.2.2	Issuance of CA and RA Certificates	24
2.3	Financial Responsibility (DL1-2)	15	4.3	Certificate Acceptance (DL1-2)	25
2.3.1	Indemnification by Subscribers and Relying Parties	15	4.4	Certificate Suspension and Revocation (DL1-2)	25
2.3.2	Fiduciary Relationships	15	4.4.1	Circumstances for Revocation	25
2.3.3	Administrative Processes	15	4.4.2	Who Can Request Revocation	25
2.4	Interpretation and Enforcement (DL1-2)	16	4.4.3	Procedure for Revocation Request	25
2.4.1	Governing Law	16	4.4.4	Revocation Request Grace Period	25
2.4.2	Severability, Survival, Merger, Notice	16	4.4.5	Circumstances for Suspension	25
2.4.3	Dispute Resolution Procedures	16	4.4.6	Who Can Request Suspension	25
2.5	Fees (DL1-2)	17	4.4.7	Procedure for Suspension Request	26
2.6	Publication and Repository (DL1-2)	17	4.4.8	Limits on Suspension Period	26
2.6.1	Publication of CA Information	17	4.4.9	CRL Issuance Frequency (If Applicable)	26
2.6.2	Frequency of Publication	17	4.4.10	Certificate Revocation List Checking Requirements	26
2.6.3	Access Controls	17	4.4.11	On-Line Revocation/Status Checking Availability	26
2.6.4	Repositories	18	4.4.12	On-Line Revocation Checking Requirements	26
2.7	Compliance Audit (DL1-2)	18			
2.8	Confidentiality and Privacy (DL1-2)	18			
2.8.1	Types of Information to be Kept Confidential and Private	19			
2.8.2	Types of Information Not Considered Confidential or Private	19			

4.4.13	Other Forms of Revocation Advertisements Available .....	26	6.1.1	Key Pair Generation (DL1-2) .....	36
4.4.14	Checking Requirements for Other Forms of Revocation Advertisements.....	26	6.1.2	Private Key Delivery to Entity.....	37
4.4.15	Special Requirements Regarding Key Compromise .....	26	6.1.2.1	Private Key Delivery to Entity – DL1.....	37
4.5	Security Audit Procedures (DL1-2).....	26	6.1.2.2	Private Key and SSCD Delivery to Entity – DL2 .....	37
4.5.1	Types of Events Recorded.....	27	6.1.3	Public Key Delivery to Certificate Issuer (DL1-2) .....	38
4.5.2	Frequency of Processing Log.....	27	6.1.4	CA Public Key Delivery to Users (DL1-2).....	38
4.5.3	Retention Period for Audit Log.....	27	6.1.5	Key Sizes (DL1-2).....	38
4.5.4	Protection of Audit Log .....	27	6.1.6	Public Key Parameters Generation (DL1-2).....	38
4.5.5	Audit Log Backup Procedures .....	27	6.1.7	Parameter Quality Checking (DL1-2).....	38
4.5.6	Audit Collection System .....	28	6.1.8	Hardware/Software Key Generation (DL1-2)....	39
4.5.7	Notification to Event-Causing Subject.....	28	6.1.9	Key Usage Purposes (As per X.509 v3 Key Usage Field) (DL1-2) .....	39
4.5.8	Vulnerability Assessments .....	28	6.2	Private Key Protection .....	39
4.6	Records Archival (DL1-2).....	28	6.2.1	Standards for Cryptographic Modules (DL1-2).....	39
4.6.1	Types of Events Recorded.....	28	6.2.2	Private Key (n out of m) Multi-Person Control (DL1-2) .....	40
4.6.2	Retention Period for Archive .....	28	6.2.3	Private Key Escrow (DL1-2).....	40
4.6.3	Protection of Archive .....	29	6.2.4	Private Key Backup (DL1-2).....	40
4.6.4	Archive Backup Procedures.....	29	6.2.5	Private Key Archival (DL1-2).....	40
4.6.5	Requirements for Time-Stamping of Records...	29	6.2.6	Private Key Entry into Cryptographic Module (DL1-2) .....	40
4.6.6	Archive Collection System.....	29	6.2.7	Method of Activating Private Key.....	40
4.6.7	Procedures to Obtain and Verify Archive Information.....	29	6.2.7.1	DL1 Certificates.....	40
4.7	Key Changeover (Renewal) (DL1-2).....	29	6.2.7.2	DL2 Certificates.....	41
4.8	Compromise and Disaster Recovery (DL1-2) .....	29	6.2.8	Method of Deactivating Private Key (DL1-2) ...	41
4.8.1	Computing Resources, Software, and/or Data Are Corrupted .....	29	6.2.9	Method of Destroying Private Key (DL1-2).....	41
4.8.2	Entity Public Key is Revoked .....	29	6.3	Other Aspects of Key Pair Management (DL1-2).....	41
4.8.3	Entity Key is Compromised.....	30	6.3.1	Public Key Archival .....	41
4.8.4	Secure Facility After a Natural or Other Type of Disaster .....	30	6.3.2	Usage Periods for the Public and Private Keys..	41
4.9	CA Termination (DL1-2).....	30	6.4	Activation Data (DL1-2) .....	41
<b>5.</b>	<b>Physical, Procedural, and Personnel Security Controls (DL1-2).....</b>	<b>31</b>	6.4.1	Activation Data Generation and Installation.....	41
5.1	Physical Controls.....	32	6.4.2	Activation Data Protection.....	41
5.1.1	Site Location and Construction .....	32	6.4.3	Other Aspects of Activation Data.....	41
5.1.2	Physical Access.....	32	6.5	Computer Security Controls (DL1-2).....	42
5.1.3	Power and Air Conditioning .....	32	6.5.1	Specific Computer Security Technical Requirements .....	42
5.1.4	Water Exposures .....	32	6.5.2	Computer Security Rating .....	43
5.1.5	Fire Prevention and Protection.....	32	6.6	Life Cycle Technical Controls (DL1-2) .....	43
5.1.6	Media Storage .....	33	6.6.1	System Development Controls .....	43
5.1.7	Waste Disposal.....	33	6.6.2	Security Management Controls .....	43
5.1.8	Off-Site Backup .....	33	6.6.3	Life Cycle Security Ratings.....	44
5.2	Procedural Controls .....	33	6.7	Network Security Controls (DL1-2).....	44
5.2.1	Trusted Roles .....	33	6.8	Cryptographic Module Engineering Controls (DL1-2)44	
5.2.2	Number of Persons Required Per Task .....	34	<b>7.</b>	<b>Certificate and CRL Profile (DL1-2).....</b>	<b>45</b>
5.2.3	Identification and Authentication for Each Role	34	7.1	Certificate Profile .....	45
5.3	Personnel Controls.....	34	7.1.1	Version Number(s) .....	45
5.3.1	Background, Qualifications, Experience, and Clearance Requirements.....	35	7.1.2	Certificate Extensions.....	46
5.3.2	Background Check Procedures .....	35	7.1.3	Algorithm Object Identifiers.....	46
5.3.3	Training Requirements .....	35	7.1.4	Name Forms .....	46
5.3.4	Retraining Frequency and Requirements .....	35	7.1.5	Name Constraints.....	46
5.3.5	Job Rotation Frequency and Sequence.....	36	7.1.6	Certificate Policy Object Identifier.....	46
5.3.6	Sanctions for Unauthorized Actions.....	36	7.1.7	Usage of Policy Constraints Extension.....	47
5.3.7	Contracting Personnel Requirements .....	36	7.1.8	Policy Qualifiers Syntax and Semantics .....	47
5.3.8	Documentation Supplied to Personnel .....	36	7.1.9	Processing Semantics for the Critical Certificate Policy Extension .....	47
<b>6.</b>	<b>Technical Security Controls .....</b>	<b>36</b>	7.2	CRL Profile .....	47
6.1	Key Pair Generation and Installation.....	36	<b>8.</b>	<b>Specification Administration (Class 1-3).....</b>	<b>47</b>
			8.1	Specification Change Procedures .....	47

8.1.1	Items that Can Change Without Notification ....	47
8.1.2	Items that Can Change with Notification .....	48
8.1.2.1	List of Items .....	48
8.1.2.2	Notification Mechanism .....	48
8.1.2.3	Comment Period.....	48
8.1.2.4	Mechanism to Handle Comments.....	48
8.1.3	Changes Requiring Changes in the Certificate Policy OID or CPS Pointer.....	49
8.2	Publication and Notification Policies.....	49
8.2.1	Items Not Published in the EDP or CPS .....	49
8.2.2	Distribution of the EDP and CPSs .....	49
8.3	CPS Approval Procedures .....	49
<b>Acronyms and Definitions .....</b>		<b>50</b>
	Table of Acronyms .....	50
	Definitions .....	51
	Cross-Reference of ETSI Definitions to CP Definitions.....	52
<b>Change History .....</b>		<b>53</b>

# 1. Introduction

***Please refer to the Acquisition Notice (page ii) for an explanation of the naming, licensing and ownership information referenced throughout this document.***

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”).<sup>1</sup> The Directive is intended to facilitate the use of Electronic Signatures and establishes requirements for “Qualified Certificates” that support certain types of Electronic Signatures.

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”).<sup>2</sup> The EDP defines two policies that supplement the CP, referred to here as “Directive Level 1” (“DL1”) and “Directive Level 2” (“DL2”).<sup>3</sup> DL1 and DL2 correspond, respectively, to the “QCP public” certificate policy and “QCP public + SSCD” certificate policy defined in the ETSI Policy Document.<sup>4</sup> Finally, the EDP supplements the certificate profile developed by ETSI (the “Qualified Certificate Profile”),<sup>5</sup> 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.<sup>6</sup>

*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.

Symantec Corporation (“Symantec”) 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 Network SM (“VTN”) is a global public key infrastructure (“PKI”) established to support the use of digital certificates (“Certificates”) in both wired and wireless applications. Symantec offers VTN services together with a global network of affiliates (“Affiliates”) throughout the world, many of whom are located within jurisdictions in the European Community (“EC”).

---

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

<sup>2</sup> 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”].

<sup>3</sup> 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.

<sup>4</sup> ETSI Policy Document § 5.2.

<sup>5</sup> 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”].

<sup>6</sup> See Qualified Certificate Profile § 1.

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.”<sup>7</sup>

“‘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.”<sup>8</sup>

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.”<sup>9</sup>

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 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.<sup>10</sup> 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

---

<sup>7</sup> Directive art. 5(2).

<sup>8</sup> Directive art. 2(1); ETSI Policy Document §3.1.

<sup>9</sup> Directive art. 2(2); ETSI Policy Document §3.1.

<sup>10</sup> See ETSI Policy Document § 5.1.

- 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.”<sup>11</sup>

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.<sup>12</sup> 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:

- 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.

---

<sup>11</sup> Directive art. 5(1).

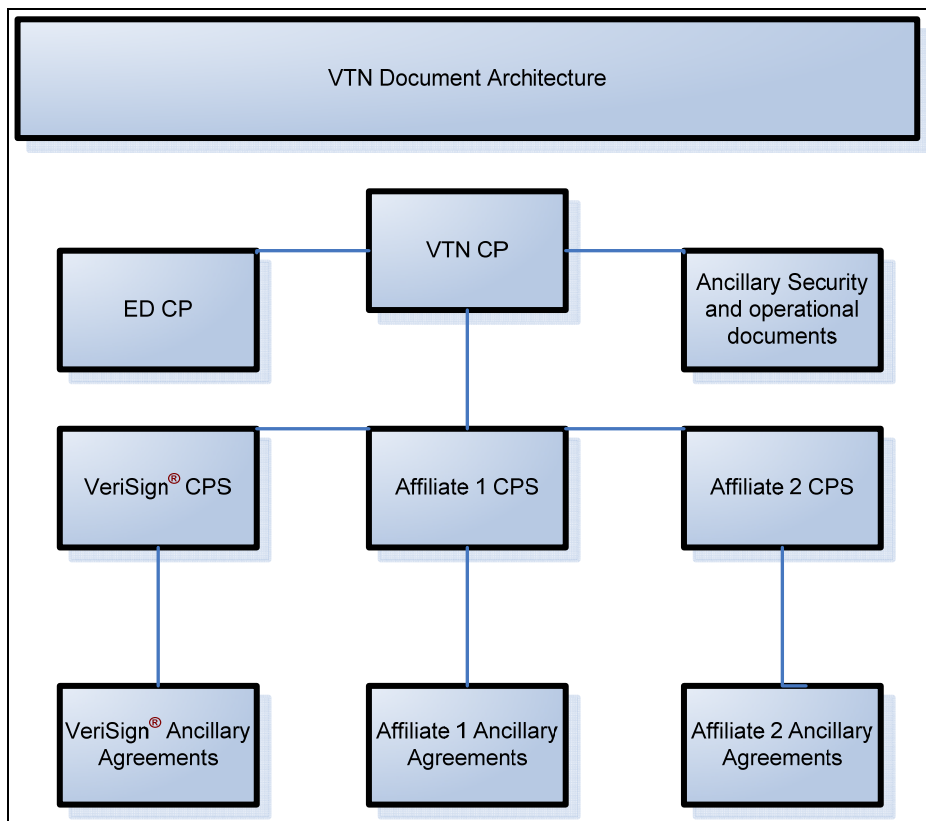
<sup>12</sup> See ETSI Policy Document § 5.1.

## (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 Symantec Legal Repository at <http://www.verisign.com/repository/index.html>. The CP is also available in hardcopy form upon request sent to: Symantec Corporation, 350 Ellis Street, 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 Symantec Security Policy, the Security and Audit Requirements (SAR) Guide, the Enterprise Security Guide, the Affiliate Practices Legal Requirements Guidebook, and the Key Ceremony Reference Guide.

Figure 1 depicts the relationship between the CP and other practices documents within the VTN documentation architecture which reflects the governing order of the documents. The ancillary security and operational documents are above all CPs and ancillary agreements used by Symantec or an Affiliate within the VTN documentation architecture. The EDP also stands above all CPs and ancillary agreements used by Symantec and Affiliates.



**Figure 1 - VTN Document Architecture**

Together with the CP and other ancillary security and operational documents, Symantec and the PMA maintains this EDP.

## **(b) Knowledge Assumed by the EDP**

This EDP assumes that the reader is generally familiar with Digital Signatures, PKIs, Symantec'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, Symantec 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 interoperation easier for persons using or considering using VTN services that comply with the Directive.

While Symantec 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. Symantec 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 check's 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.<sup>13</sup>

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 Symantec 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**

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

---

<sup>13</sup> CP § 1.1.1.

### **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 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.<sup>14</sup>

---

<sup>14</sup> See ETSI Policy Document § 4.4

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

### **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.<sup>15</sup>

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.<sup>16</sup>

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.<sup>17</sup>

#### **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:

---

<sup>15</sup> See ETSI Policy Document § 5.3.2.

<sup>16</sup> See ETSI Policy Document § 5.3.1.

<sup>17</sup> See ETSI Policy Document § 6.2(e).

VeriSign® Trust Network Policy Management Authority  
c/o Symantec Corporation  
350 Ellis Street  
Mountain View, CA 94043 USA  
+1 (650) 527-8000 (voice)  
+1 (650) 527-8050 (fax)  
[practices@verisign.com](mailto:practices@verisign.com)

## 1.4.2 Contact Person

Address inquiries about the EDP to [practices@verisign.com](mailto:practices@verisign.com) or to the following address:

Symantec Corporation  
350 Ellis Street  
Mountain View, CA 94043 USA  
Attn: Practices Development – EDP  
+1 (650) 527-8000 (voice)  
+1 (650) 527-8050 (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 Symantec 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.<sup>18</sup> 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.<sup>19</sup> 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 another entity.<sup>20</sup> 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

---

<sup>18</sup> See ETSI Policy Document § 6.1.

<sup>19</sup> See ETSI Policy Document §§ 6.3, 7.1(e).

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

appearing in the Relying Party Agreement referred to in the Certificate.<sup>21</sup> Finally, CAs shall perform their services in accordance with the applicable Affiliate's CPS.<sup>22</sup>

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.<sup>23</sup>

Subscriber Agreements shall be in writing and in readily understandable language.<sup>24</sup> 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:<sup>25</sup>

- 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,<sup>26</sup>
- 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
- 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

---

<sup>21</sup> See ETSI Policy Document § 6.3?

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

<sup>23</sup> See ETSI Policy Document § 7.5.1(a)-(b).

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

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

<sup>26</sup> See CP § 2.2.1.1.

Agreements.<sup>27</sup> 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.<sup>28</sup>

Relying Party Agreements shall be in writing and in readily understandable language.<sup>29</sup>

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

- 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 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.<sup>31</sup>

---

<sup>27</sup> See ETSI Policy Document § 7.3.1(a)-(b).

<sup>28</sup> See ETSI Policy Document § 7.3.2(b).

<sup>29</sup> See ETSI Policy Document § 7.3.4(b).

<sup>30</sup> See ETSI Policy Document § 7.3.4(a).

<sup>31</sup> See ETSI Policy Document § 7.5.1(a)-(b).

### 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.<sup>32</sup> 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.<sup>33</sup>

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
  - ii) Control over the subjects 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.<sup>34</sup>

---

<sup>32</sup> See ETSI Policy Document § 6.2(a)-(d), (g).

<sup>33</sup> See ETSI Policy Document § 6.2(e)-(f).

<sup>34</sup> See ETSI Policy Document §§ 6.3, 6.3(a)-(c).

## 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.<sup>35</sup> 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,<sup>36</sup>
- 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,<sup>37</sup>
- Where an Managed PKI Customer uses Managed PKI Key Manager to generate an end-user Subscriber key pair, or a CA pre-generates 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,<sup>38</sup> and
- 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.<sup>39</sup>

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 Certificate<sup>40</sup> 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.<sup>41</sup> The amount of such

---

<sup>35</sup> See ETSI Policy Document § 6.4.

<sup>36</sup> See Directive art. 6(1)(a).

<sup>37</sup> See Directive art. 6(1)(b).

<sup>38</sup> See Directive art. 6(1)(c).

<sup>39</sup> See Directive art. 6(2).

<sup>40</sup> See Directive art. 6(1)(a).

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

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.<sup>42</sup>

#### 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.<sup>43</sup>

### 2.2.3 Subscriber Liability

The liability (and/or limitation thereof) of Subjects and Subscribers complies with ETSI Policy<sup>44</sup>

### 2.2.4 Relying Party Liability

No stipulation.

## 2.3 Financial Responsibility (DL1-2)

### 2.3.1 Indemnification by Subscribers and Relying Parties

No stipulation.

### 2.3.2 Fiduciary Relationships

No stipulation<sup>45</sup>

### 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.<sup>46</sup>

---

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

<sup>43</sup> :ETSI Policy Document Annex A

<sup>44</sup> :ETSI Policy Document Annex A

<sup>45</sup> ETSI Policy Document Annex A (1) C

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

## **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 law<sup>47</sup>, 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:

- 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

---

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

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.<sup>48</sup>

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 Symantec and Affiliates maintain a publicly-available repository making Certificates available satisfies the requirement for making Certificates available as necessary to Subscribers and Relying Parties.<sup>49</sup> The requirement that repositories includes revocation information concerning VTN Certificates and the applicable Relying 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.<sup>50</sup> Revocation services, revocation status information, and Relying Party Agreements shall be available twenty-four (24) hours per day, seven (7) days per week.<sup>51</sup> The Relying Party Agreement shall be readily identifiable within the repository of a Symantec or an Affiliate.<sup>52</sup> Upon system failure, or repository service unavailability, or other factors that are not under the control of Symantec or an Affiliate, Symantec 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 Symantec 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.<sup>53</sup> More specifically, Symantec 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,

---

<sup>48</sup> See ETSI Policy Document § 7.3.4(a), 7.5(f).

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

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

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

<sup>52</sup> See ETSI Policy Document § 7.3.5(d).

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

- 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.<sup>54</sup>

## **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 Directive.<sup>55</sup> 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.<sup>56</sup> In addition, they shall, in accordance with the Directive and ETSI Policy Document,<sup>57</sup> 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.<sup>58</sup> 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. Symantec, 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.<sup>59</sup> Information

---

<sup>54</sup> See Directive annex II(1).

<sup>55</sup> See ETSI Policy Document § 5.4.1(b).

<sup>56</sup> See ETSI Policy Document § 7.4.10).

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

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

<sup>59</sup> See Directive art. 8(2).

considered confidential and private under applicable privacy policies shall be protected from loss, destruction, damage, falsification, and unauthorized or unlawful processing.<sup>60</sup>

### **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.<sup>61</sup> This requirement shall appear in the privacy policies of Affiliates.

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

- \_ Registration<sup>62</sup>
- \_ Confidentiality of records<sup>63</sup>
- \_ Protecting access to personal information<sup>64</sup>
- \_ User consent<sup>65</sup>

### **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 laws<sup>66</sup>. 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.<sup>67</sup>

---

<sup>60</sup> See ETSI Policy Document § 7.4.10(a), (c).

<sup>61</sup> See ETSI Policy Document § 7.4.10(d).

<sup>62</sup> See ETSI Policy Document § 7.3.1.

<sup>63</sup> See ETSI clauses 7.4.11(a) and 7.3.3(f)

<sup>64</sup> See ETSI clauses 7.4.6

<sup>65</sup> See ETSI Policy Document § 7.3.1(i)

<sup>66</sup> See ETSI Policy Document § 7.4.11(c).

<sup>67</sup> See ETSI Policy Document § 7.4.11(c).

## **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.

### **2.9.2 Property Rights in the CP**

VTN Participants acknowledge that Symantec 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.<sup>68</sup> 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.

---

<sup>68</sup> Directive art. 8(3).

### **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.<sup>69</sup>

### **3.1.5 Name Claim Dispute Resolution Procedure (DL1-2)**

No stipulation.

### **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 Symantec-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.<sup>70</sup>

### **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.<sup>71</sup>

### **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.<sup>72</sup> 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);

---

<sup>69</sup> See ETSI Policy Document § 7.3.3(e).

<sup>70</sup> See ETSI Policy Document § 7.3.1(k).

<sup>71</sup> See ETSI Policy Document 7.3.1 (e)

<sup>72</sup> See ETSI Policy Document § 7.3.1(c).

- 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.<sup>73</sup>

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.<sup>74</sup>

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.<sup>75</sup>

### **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.<sup>76</sup> 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.<sup>77</sup> 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.<sup>78</sup> 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.<sup>79</sup>

---

<sup>73</sup> See ETSI Policy Document § 7.3.1(d).

<sup>74</sup> See ETSI Policy Document § 7.3.1(c).

<sup>75</sup> See ETSI Policy Document § 7.3.1(c).

<sup>76</sup> See ETSI Policy Document § 7.3.2(a).

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

<sup>78</sup> See ETSI Policy Document § 7.3.2(a).

<sup>79</sup> See Directive annex II(d); ETSI Policy Document § 7.3.2.

### **3.4 Revocation Request (DL1-2)**

The requirement that revocation requests be authorized and validated is satisfied by compliance with CP § 3.4.<sup>80</sup>

## **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,<sup>81</sup>
- The Certificate Applicant shall present evidence of identity consistent with EDP § 3.1.9,<sup>82</sup> 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.<sup>83</sup>

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)<sup>84</sup> 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.<sup>85</sup>

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.<sup>86</sup>

#### **4.1.2 Certificate Applications for CA or RA Certificates**

No stipulation.

---

<sup>80</sup> See ETSI Policy Document §§ 7.3.6, 7.3.6(c).

<sup>81</sup> See ETSI Policy Document § 7.3.1(a)-(b).

<sup>82</sup> See ETSI Policy Document § 7.3.1(d).

<sup>83</sup> See ETSI Policy Document § 7.3.1(h).

<sup>84</sup> See ETSI Policy Document § 7.3.1(f).

<sup>85</sup> See ETSI Policy Document § 7.3.1(i); *see also* ETSI Policy Document § 7.3.1(j).

<sup>86</sup> 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.<sup>87</sup> 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.<sup>88</sup>

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

### 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.<sup>90</sup> 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,<sup>91</sup>
- Is obligated to make its services available to all applicants whose activities fall within its declared field of operation,<sup>92</sup>
- Is a legal entity,<sup>93</sup> which shall be confirmed as part of the authentication of the potential CA or RA organization,<sup>94</sup>
- Has a system or systems for quality and information security management appropriate for the certification services it is providing,<sup>95</sup> which, in the case of potential Affiliates, shall be confirmed as part of a Security and Practices Review performed under the CP,<sup>96</sup>
- Can meet the financial responsibility obligations of CP § 2.3 and EDP § 2.3,<sup>97</sup>
- Can meet the dispute resolution requirements of EDP § 2.4.3,<sup>98</sup>
- In the case of Affiliates, has a properly documented agreement and contractual relationship in place with its Superior Entity,<sup>99</sup> and

---

<sup>87</sup> See ETSI Policy Document § 7.3.5(a).

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

<sup>90</sup> See Directive annex II(a); ETSI Policy Document § 7.5.

<sup>91</sup> See ETSI Policy Document § 7.5(a), 7.4.3(a)

<sup>92</sup> See ETSI Policy Document § 7.5(b).

<sup>93</sup> See ETSI Policy Document § 7.5(c).

<sup>94</sup> See CP § 3.1.8.2.

<sup>95</sup> See ETSI Policy Document § 7.4.1(d).

<sup>96</sup> See CP § 2.7.

<sup>97</sup> See ETSI Policy Document § 7.5(d)-(e).

<sup>98</sup> See ETSI Policy Document § 7.5(f).

<sup>99</sup> See ETSI Policy Document § 7.5(g).

- 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,<sup>100</sup> 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.<sup>101</sup> 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.<sup>102</sup> Certificates that are revoked shall not be reinstated as valid Certificates.<sup>103</sup>

#### **4.4.4 Revocation Request Grace Period**

No stipulation.

#### **4.4.5 Circumstances for Suspension**

Not applicable.

#### **4.4.6 Who Can Request Suspension**

Not applicable.

---

<sup>100</sup> See ETSI Policy Document § 7.3.6(a).

<sup>101</sup> See ETSI Policy Document § 7.3.6(b).

<sup>102</sup> See ETSI Policy Document § 7.3.6(e).

<sup>103</sup> See ETSI Policy Document § 7.3.6(f).

#### **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.<sup>104</sup> 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.<sup>105</sup> A new CRL may be published before the stated time of the next CRL to be issued.<sup>106</sup>

#### **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.

#### **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.<sup>107</sup>

---

<sup>104</sup> See ETSI Policy Document § 7.3.6(g).

<sup>105</sup> See ETSI Policy Document § 7.3.6(g).

<sup>106</sup> See ETSI Policy Document § 7.3.6(g).

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

#### 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,<sup>108</sup> and
- All events relating to the lifecycle of CA keys.<sup>109</sup>
- 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.<sup>110</sup> If applicable, CAs issuing DL2 Certificates shall log all events relating to the preparation of SSCDs.<sup>111</sup>

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

#### 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.<sup>114</sup>

#### 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 5.5.2<sup>115</sup>.

#### 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.<sup>116</sup>

#### 4.5.5 Audit Log Backup Procedures

No stipulation.

---

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

<sup>109</sup> See ETSI Policy Document § 7.4.11(k).

<sup>110</sup> See ETSI Policy Document § 7.4.11(m).

<sup>111</sup> See ETSI Policy Document § 7.4.11(n).

<sup>112</sup> See ETSI Policy Document § 7.4.11(g).

<sup>113</sup> See ETSI Policy Document § 7.4.6(f).

<sup>114</sup> See ETSI Policy Document § 7.4.6(i), (k).

<sup>115</sup> See ETSI Policy Document § 7.4.11

<sup>116</sup> See ETSI Policy Document § 7.4.11(f).

#### **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.<sup>117</sup>

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.<sup>118</sup>

#### **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.<sup>119</sup> This section is subject to any applicable Member Country-specific record retention requirements.

---

<sup>117</sup> See ETSI Policy Document § 7.4.11(i).

<sup>118</sup> See ETSI Policy Document § 7.4.11(i).

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

### **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.<sup>120</sup> 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.<sup>121</sup>

### **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.

## ***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.<sup>122</sup>

### **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.<sup>123</sup> 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.

---

<sup>120</sup> See ETSI Policy Document § 7.4.11(a)-(b); see also ETSI Policy Document § 7.4.10(a), (c)., see also 7.4.6

<sup>121</sup> See ETSI Policy Document § 7.4.11(a)-(b), (j).

<sup>122</sup> See ETSI Policy Document § 7.4.5(b), (h),(i),(j)

<sup>123</sup> See ETSI Policy Document § 7.4.8(d).

- 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.<sup>124</sup> 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.<sup>125</sup> 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 all functions within one week satisfies the requirement in the ETSI Policy Document to restore operations "as soon as possible" after a disaster.<sup>126</sup> 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.<sup>127</sup> 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.<sup>128</sup>
- 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

<sup>124</sup> See ETSI Policy Document § 7.4.8(d)

<sup>125</sup> See ETSI Policy Document § 7.4.8(d); see also Directive annex II(a).

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

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

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

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.<sup>129</sup> Affiliates' CPS shall implement the foregoing requirements and shall state whether unexpired unrevoked certificates will be revoked in connection with the termination.<sup>130</sup>

## 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.<sup>131</sup> 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.<sup>132</sup> Also, the security infrastructure needed to implement the security policy and manage security shall be maintained at all 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.<sup>133</sup>

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 follow up;
- Media handling and security; and
- Data and software exchange.<sup>134</sup>

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.<sup>135</sup> Ultimately, however, senior management of the CA or RA has the responsibility for ensuring that its practices, including security practices, are properly implemented.<sup>136</sup>

---

<sup>129</sup> See ETSI Policy Document § 7.4.9(b).

<sup>130</sup> See ETSI Policy Document § 7.4.9(c).

<sup>131</sup> See ETSI Policy Document §§ 7.4.1(f),

<sup>132</sup> See Directive annex II(e); ETSI Policy Document § 7.4.1.

<sup>133</sup> See ETSI Policy Document § 7.4.1(e).

<sup>134</sup> See ETSI Policy Document § 7.4.5(k).

<sup>135</sup> See ETSI Policy Document § 7.4.5(k)

<sup>136</sup> See ETSI Policy Document § 7.1(f).

## **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 (SAR) 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.<sup>137</sup> 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.<sup>138</sup> These controls also protect against equipment, information, media, and software relating to CA services being taken offsite without authorization.<sup>139</sup>

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.<sup>140</sup>

### **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.<sup>141</sup> 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.<sup>142</sup>

### **5.1.4 Water Exposures**

See EDP § 5.1.3.

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

See EDP § 5.1.3.

---

<sup>137</sup> See ETSI Policy Document § 7.4.4(f).

<sup>138</sup> See ETSI Policy Document § 7.4.4(b)-(c); *see also* ETSI Policy Document § 7.4.4(g).

<sup>139</sup> See ETSI Policy Document § 7.4.4(h).

<sup>140</sup> See ETSI Policy Document § 7.4.6(h).

<sup>141</sup> See ETSI Policy Document § 7.4.4(a), (d).

<sup>142</sup> See ETSI Policy Document § 7.4.4(g).

### **5.1.6 Media Storage**

The media handling controls of CP § 5.1.6 satisfy the ETSI Policy Document's media security requirements.<sup>143</sup> 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.<sup>144</sup>

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

No stipulation.

## **5.2 Procedural Controls**

Symantec, Affiliates, and Customers shall assess business and security risks and ensure that their systems are secure and correctly operated, with minimal risk of failure.<sup>145</sup> Symantec, Affiliate, and Customer personnel shall perform administrative and management procedures and processes in accordance with their respective security policies.<sup>146</sup>

### **5.2.1 Trusted Roles**

The security policies of Symantec, Affiliates, and Customers shall clearly identify trusted roles.<sup>147</sup> 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.<sup>148</sup>

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

---

<sup>143</sup> See ETSI Policy Document § 7.4.5(c), (f).

<sup>144</sup> See ETSI Policy Document § 7.4.5(c), (f).

<sup>145</sup> See Directive annex II(e); ETSI Policy Document § 7.4.5.

<sup>146</sup> See ETSI Policy Document § 7.4.3(e).

<sup>147</sup> See ETSI Policy Document § 7.4.3(c).

<sup>148</sup> See ETSI Policy Document § 7.4.3(i).

- System auditors, who are authorized to view and maintain archives and audit logs of the CA or RA trustworthy systems.<sup>149</sup>

Symantec, 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.<sup>150</sup>

## 5.2.2 Number of Persons Required Per Task

Security roles and responsibilities, as specified in Symantec's, Affiliates', and Customers' security policies, shall be documented in job descriptions.<sup>151</sup> Such job descriptions 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.<sup>152</sup>

## 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.<sup>153</sup>

## 5.3 Personnel Controls

Symantec, Affiliates, and Customers shall ensure that their personnel and hiring practices enhance and support the trustworthiness of their services.<sup>154</sup> Symantec, 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.<sup>155</sup>

Symantec, 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.<sup>156</sup> The organization within Symantec, 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.<sup>157</sup> The parts of the organization of Symantec, Affiliates, and Customers concerned with Certificate generation and revocation management shall have a documented structure that safeguards the impartiality of operations.<sup>158</sup>

Symantec, Affiliates, and Customers shall develop and utilize in their hiring practices job descriptions developed to support the separation of duties, least privilege concept, determining

<sup>149</sup> See ETSI Policy Document § 7.4.3(h).

<sup>150</sup> See ETSI Policy Document § 7.4.5(e).

<sup>151</sup> See ETSI Policy Document § 7.4.3(c).

<sup>152</sup> See ETSI Policy Document § 7.4.3(d).

<sup>153</sup> See ETSI Policy Document § 7.4.6(e).

<sup>154</sup> See Directive annex II(e); ETSI Policy Document § 7.4.3.

<sup>155</sup> See ETSI Policy Document § 7.4.3(a)

<sup>156</sup> See ETSI Policy Document §§ 7.4.3(g), 7.5(h)

<sup>157</sup> See ETSI Policy Document 7.5(h)

<sup>158</sup> See ETSI Policy Document 7.5(i)

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.<sup>159</sup>

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 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.<sup>160</sup> In addition, managerial personnel hired by Symantec, 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.<sup>161</sup>

### **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. Symantec, 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.<sup>162</sup> Where local law precludes Symantec, 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.<sup>163</sup>

### **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.<sup>164</sup>

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

No stipulation.

---

<sup>159</sup> See ETSI Policy Document § 7.4.3(d).

<sup>160</sup> See ETSI Policy Document §§ 7.4.3(a),

<sup>161</sup> See ETSI Policy Document § 7.4.3(f).

<sup>162</sup> See ETSI Policy Document § 7.4.3(j).

<sup>163</sup> See ETSI Policy Document § 7.4.3(i) note 4.

<sup>164</sup> See ETSI Policy Document § 7.4.3(a).

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

No stipulation.

### **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**

Symantec, 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.<sup>165</sup>

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

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

## **6. Technical Security Controls**

Symantec, 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.<sup>167</sup> 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.<sup>168</sup> Processing Centers shall generate CA keys in devices meeting the requirements of EDP § 6.2.1.<sup>169</sup> Affiliates requiring Common Criteria rated hardware use EAL 4+ rated version devices. The devices used by Symantec 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;<sup>170</sup>

---

<sup>165</sup> See ETSI Policy Document § 6.1.

<sup>166</sup> See ETSI Policy Document § 7.4.1(c).

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

<sup>168</sup> See ETSI Policy Document § 7.2.1(a).

<sup>169</sup> See ETSI Policy Document § 7.2.1(b).

<sup>170</sup> See ETSI Policy Document § 6.2(f).

Where Processing Centers pregenerate end-user Subscriber keys on tokens, including SSCDs, or Client Managed PKI Customers using Managed PKI Key Manager use the 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.<sup>171</sup> One way in which this requirement may be met is using a suitable protection profile, defined in accordance with ISO 15408 or its equivalent.<sup>172</sup>

Article 9 of the Directive establishes an "Electronic-Signature Committee" to assist the European Commission.<sup>173</sup> A proposal exists currently for the establishment of a cryptographic advisory panel to assist the Committee.<sup>174</sup> 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.<sup>175</sup> 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."<sup>176</sup> 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.<sup>177</sup> 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 private keys meet the requirements placed on CA-generated Subscriber keys in the ETSI Policy Document.<sup>178</sup>

---

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

<sup>172</sup> See ETSI Policy Document § 7.2.9 note 3.

<sup>173</sup> See Directive art. 9(1)

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

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

<sup>176</sup> 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).

<sup>177</sup> See ETSI Policy Document § 7.2.8(c)-(d).

<sup>178</sup> See ETSI Policy Document § 7.2.8(c)-(d).

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.<sup>179</sup>

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.<sup>180</sup>

### **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.<sup>181</sup> 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.”<sup>182</sup> 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.

### **6.1.7 Parameter Quality Checking (DL1-2)**

No stipulation.

---

<sup>179</sup> See ETSI Policy Document § 7.2.9 & note 2.

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

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

<sup>182</sup> ETSI Policy Document §§ 6.2(d), 7.2.1(d), 7.2.8(b).

### **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.<sup>183</sup> For Subjects of DL2 Certificates generating their own keys, such generation shall take place on the SSCD hardware device to be used for signing.<sup>184</sup> 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.<sup>185</sup> Processing Centers shall protect CA keys in devices meeting the requirements of EDP § 6.2.1.<sup>186</sup> 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.<sup>187</sup>

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 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.<sup>188</sup>

### **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,

---

<sup>183</sup> See ETSI Policy Document § 7.2.1(b).

<sup>184</sup> See ETSI Policy Document § 6.2(f).

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

<sup>186</sup> See ETSI Policy Document § 7.2.2(a).

<sup>187</sup> See ETSI Policy Document § 7.2.5.

<sup>188</sup> See ETSI Policy Document § 7.2.8(c)-(d).

based on a risk analysis and taking into account physical and other non-technical security measures<sup>189</sup>

## **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.<sup>190</sup> 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.<sup>191</sup>

## **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.<sup>192</sup>

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

## **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.<sup>193</sup>

## **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.

---

<sup>189</sup> See ETSI Policy Document §§ 7.2.1(b), 7.2.2(a).

<sup>190</sup> See ETSI Policy Document §§ 7.2.1(a), 7.2.2(c), 7.2.7(c).

<sup>191</sup> See Directive annex II(j); ETSI Policy Document § 7.2.4.

<sup>192</sup> See ETSI Policy Document § 7.2.2(c)-(d).

<sup>193</sup> See ETSI Policy Document § 7.2.2(b), (e).

### 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.<sup>194</sup>

### 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.<sup>195</sup>

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

### 6.3.1 Public Key Archival

No stipulation.

### 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.<sup>196</sup>

## 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.<sup>197</sup> *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.

---

<sup>194</sup> See ETSI Policy Document § 6.2(e)-(f).

<sup>195</sup> See ETSI Policy Document § 7.2.6(a).

<sup>196</sup> See ETSI Policy Document § 7.2.6.

<sup>197</sup> See ETSI Policy Document § 6.2(c).

## 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 (SAR) Guide (in the case of Symantec 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.<sup>198</sup>

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.<sup>199</sup> In addition, however, the foregoing requirement shall apply to all Customers approving Certificate Applications for Qualified Certificates. Moreover, firewalls shall be configured to prevent protocols and accesses not required for the operation of the CA/RA.<sup>200</sup>

Symantec, 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.<sup>201</sup> Moreover, CA and RA personnel shall be successfully identified and authenticated before using critical applications related to certificate management.<sup>202</sup> Symantec, 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.<sup>203</sup> 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.<sup>204</sup>

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

---

<sup>198</sup> See ETSI Policy Document § 7.4.5(a).

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

<sup>200</sup> See ETSI Policy Document § 7.4.6(a) note 1.

<sup>201</sup> See ETSI Policy Document §§ 7.4.5(c), 7.4.6.

<sup>202</sup> See ETSI Policy Document § 7.4.6(e).

<sup>203</sup> See ETSI Policy Document § 7.4.6(d).

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

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

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

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.<sup>207</sup>

## **6.5.2 Computer Security Rating**

The requirement that Symantec, 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), defined in accordance with ISO/IEC 15408 [8] or equivalent standard.<sup>208</sup> The risk analysis carried out on their services should identify critical services requiring Trustworthy Systems and the levels of assurance required.<sup>209</sup> 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 Symantec, Affiliates, or Customers to ensure that security is built into IT systems.<sup>210</sup> Change control procedures shall be utilized for releases, modifications, and emergency software fixes for such software.<sup>211</sup>

### **6.6.2 Security Management Controls**

Symantec, 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.<sup>212</sup> 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.<sup>213</sup> 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.<sup>214</sup>

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).<sup>215</sup> More specifically, Processing Centers shall ensure that such cryptographic modules:

---

<sup>207</sup> See ETSI Policy Document § 7.4.6(i), (k).

<sup>208</sup> See ETSI Policy Document § 7.4.7 note 1.

<sup>209</sup> See ETSI Policy Document § 7.4.7 note 2.

<sup>210</sup> See ETSI Policy Document § 7.4.7(a).

<sup>211</sup> See ETSI Policy Document § 7.4.7(b).

<sup>212</sup> See ETSI Policy Document § 7.4.2(a).

<sup>213</sup> See ETSI Policy Document § 7.4.6(h).

<sup>214</sup> See ETSI Policy Document § 7.4.5(g).

<sup>215</sup> See ETSI Policy Document § 7.2.7.

- Are not tampered with during shipment,<sup>216</sup>
- Are not tampered with while being stored,<sup>217</sup>
- Are functioning correctly,<sup>218</sup>
- 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.<sup>219</sup>

### 6.6.3 Life Cycle Security Ratings

No stipulation.

### 6.7 Network Security Controls (DL1-2)

The requirement that Symantec, 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.<sup>220</sup> 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.<sup>221</sup> 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.<sup>222</sup> Communications between Customers and Affiliates or between Affiliates and Symantec shall, in general, be secured so that the security of information among parties having distributed PKI responsibilities is maintained.<sup>223</sup>

### 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.<sup>224</sup>

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.<sup>225</sup> Third, CAs shall ensure that the SSCDs have

<sup>216</sup> See ETSI Policy Document § 7.2.7(a).

<sup>217</sup> See ETSI Policy Document § 7.2.7(b).

<sup>218</sup> See ETSI Policy Document § 7.2.7(d).

<sup>219</sup> See ETSI Policy Document § 7.2.7(e).

<sup>220</sup> See ETSI Policy Document § 7.4.6(b).

<sup>221</sup> See ETSI Policy Document § 7.3.3(f).

<sup>222</sup> See ETSI Policy Document § 7.3.3(g).

<sup>223</sup> See ETSI Policy Document § 7.4.1(e).

<sup>224</sup> See Directive annex III(1).

<sup>225</sup> See Directive annex III(2).

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).<sup>226</sup>

## **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.

### **7.1 Certificate Profile**

DL1 and DL2 Certificates shall, in content, adhere to the Qualified Certificate Profile,<sup>227</sup> 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.<sup>228</sup> 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),<sup>229</sup>
- The beginning and end of their validity periods (valid from and valid to dates),<sup>230</sup>
- The identity code of the Certificate (serial number).<sup>231</sup>
- The Advanced Electronic Signature of the issuing certification-service-provider (digital signature of the CA).<sup>232</sup>
- 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.

---

<sup>226</sup> Directive art. 3(4).

<sup>227</sup> See Qualified Certificate Profile § 1.

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

<sup>229</sup> See Directive annex I(e).

<sup>230</sup> See Directive annex I(f).

<sup>231</sup> See Directive annex I(g).

<sup>232</sup> See Directive annex I(h).

### 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 section 4.2.1(2) of the Qualified Certificate Profile.<sup>233</sup> 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,<sup>234</sup> 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.<sup>235</sup>

### 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.<sup>236</sup> The name of the Subscriber shall appear in the Subject field in accordance with CP § 7.1.4.<sup>237</sup>

### 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.<sup>238</sup> Moreover, by virtue of including the DL1 OID or DL2 OID, which refer to the

---

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

<sup>234</sup> See Directive annex I(j); Qualified Certificate Profile § 4.2.2.

<sup>235</sup> See Qualified Certificate Profile § 4.2.3.

<sup>236</sup> See Directive annex I(b); Qualified Certificate Profile § 4.1.

<sup>237</sup> See Directive annex I(c).

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

policies of this EDP containing limitations on the scope of the use of the Certificate, DL1 and DL2 Certificates contain such limitations.<sup>239</sup>

### **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 PMA. 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 Symantec's Legal Repository located at: <http://www.verisign.com/repository/index.html>. 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.<sup>240</sup> 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.<sup>241</sup>

#### **8.1.1 Items that Can Change Without Notification**

Symantec 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.

---

<sup>239</sup> See Directive annex I (i).

<sup>240</sup> See ETSI Policy Document § 7.1(g).

<sup>241</sup> 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 Symantec Legal Repository, which is located at: <http://www.verisign.com/repository/index.html>. 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, Symantec and the PMA shall be entitled to make such amendments and identify them as material amendments by publication in the Symantec Legal Repository. Such amendments will be effective immediately upon publication. Within a reasonable time after publication, Symantec 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 Symantec Legal 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 Symantec Legal 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 Symantec and the Affiliates are not disclosed to the public.<sup>242</sup>

### **8.2.2 Distribution of the EDP and CPSs**

This EDP is published in electronic form within Symantec's Legal Repository at <http://www.verisign.com/repository/index.html>. The EDP is also available in hardcopy form upon request sent to: Symantec Corporation, 350 Ellis Street, 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.<sup>243</sup>

## **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.<sup>244</sup>
- 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),<sup>245</sup> which CPS may be the same CPS written pursuant to the CP,
- Such CPS shall identify the requirements of Symantec and their Customers, including their applicable procedures and practices,<sup>246</sup>
- Such Affiliates shall establish a high level management body with final authority and responsibility for approving the CPS,<sup>247</sup> and
- The Affiliate shall submit this CPS to Symantec for approval under CP § 8.3.

---

<sup>242</sup> See ETSI Policy Document § 7.1(c) note 2.

<sup>243</sup> See ETSI Policy Document § 7.1(c).

<sup>244</sup> See ETSI Policy Document § 7.4.1(a).

<sup>245</sup> See ETSI Policy Document § 7.1(a).

<sup>246</sup> See ETSI Policy Document § 7.1(b).

<sup>247</sup> See ETSI Policy Document § 7.1(f).

These requirements may already be satisfied by Affiliates whose CPSs have been approved by Symantec, 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.<sup>248</sup> 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.<sup>249</sup>

## Acronyms and Definitions

### Table of Acronyms

<b>Acronym</b>	<b>Term</b>
<b>ANSI</b>	The American National Standards Institute.
<b>ASB</b>	Authentication Service Bureau.
<b>B2B</b>	Business-to-business.
<b>BXA</b>	The United States Bureau of Export Administration of the United States Department of Commerce.
<b>CA</b>	Certification Authority.
<b>CP</b>	Certificate Policy.
<b>CPS</b>	Certification Practice Statement.
<b>CRL</b>	Certificate Revocation List.
<b>EAL</b>	Evaluation assurance level (pursuant to the Common Criteria).
<b>EDI</b>	Electronic Data Interchange.
<b>EDIFACT</b>	EDI for Administration, Commerce, and Transport (standards established by the United Nations Economic Commission for Europe).
<b>EDP</b>	European Directive Policies
<b>ETSI</b>	European Telecommunications Standards Institute
<b>FIPS</b>	United State Federal Information Processing Standards.
<b>ICC</b>	International Chamber of Commerce.
<b>ISO</b>	International Organization for Standardization
<b>KRB</b>	Key Recovery Block.
<b>LSVA</b>	Logical security vulnerability assessment.
<b>OCSP</b>	Online Certificate Status Protocol.
<b>OFX</b>	Open Financial Exchange.
<b>PCA</b>	Primary Certification Authority.
<b>PIN</b>	Personal identification number.
<b>PKCS</b>	Public-Key Cryptography Standard.
<b>PKI</b>	Public Key Infrastructure.
<b>PMA</b>	Policy Management Authority.
<b>QCP</b>	Qualified Certificate Policy
<b>RA</b>	Registration Authority.
<b>RFC</b>	Request for comment.
<b>SAS</b>	Statement on Auditing Standards (promulgated by the American Institute of Certified Public Accountants).
<b>S/MIME</b>	Secure multipurpose Internet mail extensions.
<b>SSCD</b>	Secure-Signature-Creation Device

<sup>248</sup> See ETSI Policy Document § 7.1 (citing Directive annex II(a)).

<sup>249</sup> See ETSI Policy Document § 7.1(b).

<b>Acronym</b>	<b>Term</b>
<b>SSL</b>	Secure Sockets Layer.
<b>VTN</b>	VeriSign <sup>®</sup> Trust Network.
<b>WAP</b>	Wireless Application Protocol.
<b>WTLS</b>	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.

<b>Term</b>	<b>Definition</b>
<b>Advanced Electronic Signature</b>	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.
<b>Attribute</b>	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
<b>Certificate</b>	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.
<b>Certificate Policies (CP)</b>	The document, which is entitled "VeriSign <sup>®</sup> 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
<b>Certificate Revocation List (CRL)</b>	A periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates 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.
<b>Certification Authority (CA)</b>	An entity authorized and trusted by trusted by one or more users to issue, manage, revoke, and renew Certificates in the VTN.
<b>Certification-Service-Provider (CSP)</b>	An entity or a legal or natural person who issues certificates or provides other services related to electronic signatures
<b>Certification Practice Statement (CPS)</b>	A statement of the practices that Symantec 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.
<b>Electronic Signature</b>	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.
<b>Key Ceremony Reference Guide</b>	A document describing Key Generation Ceremony requirements and practices.
<b>Qualified Certificate</b>	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).
<b>Qualified Electronic Signature</b>	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.
<b>Qualified Certificate</b>	The certificate policy contained in this EDP which incorporates the

<b>Term</b>	<b>Definition</b>
<b>Policy (QCP)</b>	requirements laid down in annex I and annex II of the Directive 1999/93/EC EDP
<b>Relying Party</b>	Recipient of a certificate which acts in reliance on that certificate and/or digital signatures verified using that certificate
<b>Secure-Signature-Creation Device (SSCD)</b>	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).
<b>Server Gated Cryptography</b>	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.
<b>Server Service Center</b>	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.
<b>Signature-creation Data</b>	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.
<b>Signature-creation Device</b>	Configured software or hardware used to implement the signature-creation data
<b>Secure-signature-creation device</b>	Signature-creation device which meets the requirements laid down in annex III of Directive 1999/93/EC
<b>Signature-verification Data</b>	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.
<b>Subject</b>	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.
<b>Subscriber</b>	An entity subscribing with a Certification Authority on behalf of either itself or one or more subjects
<b>Time-Stamping Authority</b>	The Symantec entity that signs Digital Receipts as part of the Symantec Digital Notarization Service.
<b>Time-Stamping Authority CA</b>	The 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**

<b>Term as Defined in the ETSI Policy Document § 3.1</b>	<b>Corresponding Term in the CP</b>
<b>advanced electronic signature</b>	The term "digital signature" used in the CP is one form of Advanced Electronic Signature.
<b>certificate</b>	certificate
<b>certificate policy</b>	A certificate policy, but not necessarily the CP
<b>certification authority</b>	certification authority
<b>certification practice statement</b>	certification practice statement
<b>certification-service-provider</b>	In the context of the CP, certification authority
<b>electronic signature</b>	electronic signature
<b>qualified certificate</b>	This term has no analog within the CP.

<b>Term as Defined in the ETSI Policy Document § 3.1</b>	<b>Corresponding Term in the CP</b>
<b><i>qualified certificate policy</i></b>	This term has no analog within the CP.
<b><i>qualified electronic signature</i></b>	This term has no analog within the CP.
<b><i>relying party</i></b>	relying party
<b><i>signature-creation data</i></b>	signature private key
<b><i>signature-creation device</i></b>	hardware token used by a Subscriber
<b><i>secure-signature-creation device</i></b>	This term has no analog within the CP.
<b><i>signature-verification data</i></b>	public key
<b><i>subscriber</i></b>	Subscriber

## Change History

---

History of changes: version 1.2

<b>Description</b>	<b>Section &amp; Changes made</b>
Updated Trademarks Notices page & added Acquisition Notice.	Page ii.
Changes to identify Symantec Corporation acquisition & ownership of the VTN services.	Throughout document: <ul style="list-style-type: none"> <li>• Corporate owner &amp; contact information changed to Symantec Corporation</li> <li>• CA names and VTN branding continues to reflect the VeriSign name until such time that re-branding can occur.</li> </ul>