VeriSign Trust Network European Directive Supplemental Policies

Version 1.0

Effective Date: September 19, 2001

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

VeriSign Trust Network European Directive Supplemental Policies

Revision date: September 4, 2001

Trademark Notice

TABLE OF CONTENTS

1. Introduction

The VeriSign Trust Network European Directive Supplemental Policies (referred to in this document as the singular acronym "EDSP") is a supplement to the VeriSign Trust Network Certificate Policies ("CP"). The purpose of the EDSP is to facilitate compliance with the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for Electronic Signatures (the "Directive").[1] The Directive is intended to facilitate the use of Electronic Signatures and establishes requirements for "Qualified Certificates" that support certain types of Electronic Signatures.

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

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

VeriSign, Inc. ("VeriSign") is the leading provider of trusted infrastructure services to web sites, enterprises, electronic commerce service providers, and individuals. The company's domain name, digital certificate, and payment services provide the critical web identity, authentication, and transaction infrastructure that online businesses require to conduct secure e-commerce and communications. The VeriSign Trust 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. VeriSign 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").

---

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

[2] European Telecommunications Standards Institute, Policy requirements for certification authorities issuing qualified certificates § 5.1 (ETSI TS 101 456 V1.1.1 Dec. 2000) [hereinafter referred to as the "ETSI Policy Document"].

[3] Although designations DL1 and DL2 do not appear in the Directive itself, the EDSP 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 EDSP.

[4] ETSI Policy Document § 5.2.

[5] European Telecommunications Standards Institute, Qualified certificate profile § 1 (ETSI TS 101 862 V1.1.1 Dec. 2000) [hereinafter referred to as the "Qualified Certificate Profile"].

[6] *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 EDSP is a supplement to the CP setting forth requirements that VTN Participants (including Affiliates, Customers, Subscribers, 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 EDSP 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") may 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 EDSP is an evolving document and my change as new or modified requirements emerge.

Most of the footnotes to this EDSP 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 EDSP. In other words, when a sentence in the EDSP 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 EDSP.

As a supplement to the CP, the EDSP does not attempt to address all topics relating to the VTN. In some instances, the EDSP 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 EDSP 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 EDSP comprise the members of the VeriSign Trust Network Policy Management Authority ("PMA"). The PMA is responsible for proposing changes to the CP, supplemental policies to the CP, and other policy documents; updating these documents, and soliciting comments on them. The PMA also oversees compliance with the requirements of these documents.

1.1 Overview

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

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

> "denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:
> - in electronic form, or
> - not based upon a qualified certificate, or
> - not based upon a qualified certificate issued by an accredited certification-service-provider, or
> - not created by a secure signature creation-device."[7]

"'Electronic signature' means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication."[8]

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

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

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

Article 6 of the Directive,[10] however, creates special liability rules relating to the use 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.

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.[11] The DL1 supplemental policy set forth in this EDSP 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,

---

[7] Directive art. 5(2).
[8] Directive art. 2(1).
[9] Directive art. 2(2).
[10] Directive art. 6.
[11] *See* ETSI Policy Document § 5.1.

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

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

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

> "Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device: (a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and (b) are admissible as evidence in legal proceedings."[12]

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.[13] The DL2 supplemental policy set forth in this EDSP 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

[12] Directive art. 5(1).
[13] *See* ETSI Policy Document § 5.1.

- permit Subscribers to create digital signatures, by the use of such Certificates and private key protection token, that have the benefit of the treatment of Advanced Electronic Signatures created in conjunction with an SSCD under Article 5(1) of the Directive.

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

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

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

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

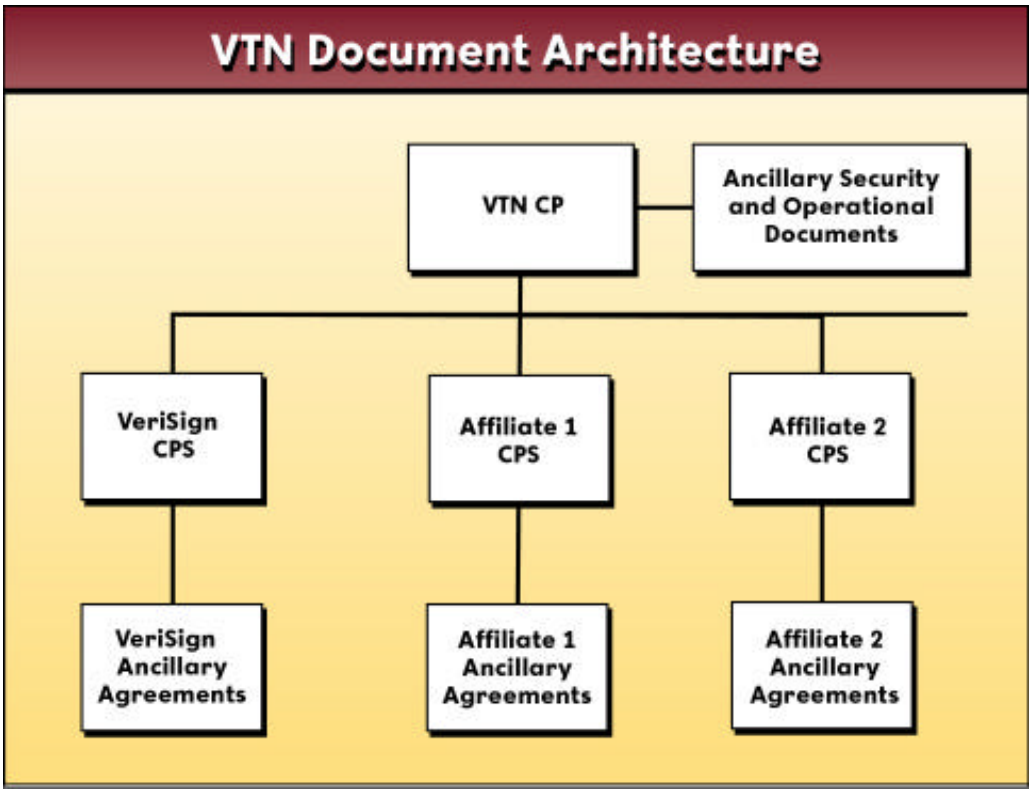

Figure 1 - VTN Document Architecture

This EDSP is another ancillary security and operational document supplementing the CP. As such, the EDSP within the VTN document architecture stands above CPSs and the ancillary agreements used by VeriSign and Affiliates. As with the CP and other ancillary security and operational documents, VeriSign and the PMA maintains this EDSP.

(b) Knowledge Assumed by the EDSP

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

(c) Compliance with Applicable Standards

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

(d) Policy Overview

The EDSP defines two supplemental 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 supplemental 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 a 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.[14]

[14] CP § 1.1.1.

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 OnSite Customer or Client OnSite Lite Customer entity (i) as an officer, director, employee, partner, contractor, intern, or other person within the entity, (ii) as a member of a VeriSign registered community of interest, or (iii) as a person maintaining a relationship with the entity where the entity has business or other records providing appropriate assurances of the identity of such person (*e.g.*, a customer).

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

1.2 Identification

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

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

1.3 Community and Applicability

The community governed by this EDSP 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 EDSP 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 OnSite 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 EDSP.

1.3.2 Registration Authorities

Registration Authorities governed by the EDSP 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 OnSite Lite Customers, (3) Server OnSite Customers, (4) Global Server OnSite 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 EDSP.

1.3.3 End Entities

DL1 and DL2 Certificates are client Certificates issued only to individual end-user Subscribers. Subscribers may or may not be Affiliated Individuals in relation to a legal person or other organizational entity.

1.3.4 Applicability

1.3.4.1 Suitable Applications

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

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

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

1.3.4.2 Restricted Applications

In addition to the restrictions in CP § 1.3.4.2, Subscribers of DL2 Certificates shall be used to create digital signatures only in connection with the use of an SSCD.[17]

[15] *See* ETSI Policy Document § 5.3.2.
[16] *See* ETSI Policy Document § 5.3.1.
[17] *See* ETSI Policy Document § 6.2(e).

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 EDSP is the VTN Policy Management Authority. The address for the PMA is:

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

1.4.2 Contact Person

Address inquiries about the EDSP to cp@verisign.com or to the following address:

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

1.4.3 Person Determining CPS Suitability for the Policy

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

2. General Provisions

2.1 Obligations (DL1-2)

2.1.1 CA Obligations

CAs (*see* EDSP § 1.3.1) shall perform the obligations applicable to CAs that appear elsewhere within the EDSP. By performing CA obligations that appear in the CP and EDSP, a CA thereby

meets the general CA obligations set forth in the ETSI Policy Document.[18] Also, a CA's obligation to take commercially reasonable efforts to bind Subscribers and Relying Parties using Subscriber Agreements and Relying Party Agreements under CP § 2.1.1 satisfies the requirement for CAs to place obligations on Subscribers[19] and Relying Parties.[20] 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 EDSP, notwithstanding any delegation of front-end functions or back-end functions to another entity.[21] CAs shall also perform any obligations set forth in certificate content or incorporated by reference in the Certificate. Such obligations include, but are not limited to, obligations appearing in the Relying Party Agreement referred to in the Certificate.[22] Finally, CAs shall perform their services in accordance with the applicable Affiliate's CPS.[23]

Affiliates' CPSs 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.[24]

Subscriber Agreements shall be in writing and in readily understandable language. [25] Furthermore, Subscriber Agreements shall contain the following terms required by the Directive and the ETSI Policy Document:[26]

- 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 EDSP § 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,[27]
- 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

[18] *See* ETSI Policy Document § 6.1.
[19] *See* Directive annex II(k); ETSI Policy Document §§ 6.2, 7.1(e), 7.3.1(a).
[20] *See* ETSI Policy Document §§ 6.3, 7.1(e).
[21] *See* ETSI Policy Document § 7.4.1(a); CP § 1.3.1.
[22] *See* ETSI Policy Document §§ 7.1.4, 7.1.8.
[23] The specific obligations within this paragraph correspond to § 6.1 of the ETSI Policy Document.
[24] *See* ETSI Policy Document § 7.5.1(a)-(b).
[25] *See* Directive annex II(k); ETSI Policy Document §§ 7.3.1(b), 7.3.4(b).
[26] *See* Directive annex II(k); ETSI Policy Document §§ 7.3.1(h), 7.3.4(a), 7.3.5(b).
[27] *See* CP § 2.2.1.1.

in the event of CA termination (*see* EDSP § 4.9) under the same conditions required by this EDSP,
- 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).

Subscriber Agreements shall be communicated to Certificate Applicants before they submit enrollment information and with means that preserve the integrity of the Subscriber Agreements.[28] 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.[29]

Relying Party Agreements shall be in writing and in readily understandable language. [30] Furthermore, Relying Party Agreements shall contain the following terms required by the ETSI Policy Document:[31]

- 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 EDSP § 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* EDSP § 1.3.2) shall perform the obligations applicable to RAs that appear elsewhere within the EDSP. 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

[28] *See* ETSI Policy Document § 7.3.1(a)-(b).
[29] *See* ETSI Policy Document § 7.3.2(b).
[30] *See* ETSI Policy Document § 7.3.4(b).
[31] *See* ETSI Policy Document § 7.3.4(a).

use Subscriber Agreements, they shall meet the requirements of EDSP § 2.1.1. Server Service Centers and ASB Providers shall use Relying Party Agreements meeting the requirements set forth in EDSP § 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.[32]

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.[33] In addition, though, a Subscriber 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.[34]

2.1.4 Relying Party Obligations

Relying Parties meeting the requirements of CP § 2.1.4 and other provisions of the CP thereby meet the obligations imposed on Relying Parties by the ETSI Policy Document.[35]

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.[36] The provisions of this EDSP § 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,[37]

[32] *See* ETSI Policy Document § 7.5.1(a)-(b).
[33] *See* ETSI Policy Document § 6.2(a)-(d), (g).
[34] *See* ETSI Policy Document § 6.2(e)-(f).
[35] *See* ETSI Policy Document §§ 6.3, 6.3(a)-(c).
[36] *See* ETSI Policy Document § 6.4.
[37] *See* Directive art. 6(1)(a).

- 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,[38]
- Where an OnSite Customer uses OnSite Key Manager to generate an end-user Subscriber key pair, or a CA pregenerates a key pair on an end-user Subscriber hardware token, the public key of such key pair can be used to verify digital signatures created with the corresponding private key,[39] 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.[40]

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[41] 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.[42] The amount of such a limitation of liability and limit on the value of transactions shall not exceed the limitation of liability applicable either within or outside the context of the NetSure Protection 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.[43]

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 EDSP § 2.2.1.1.

2.2.3 Subscriber Liability

No stipulation.

---

[38] *See* Directive art. 6(1)(b).
[39] *See* Directive art. 6(1)(c).
[40] *See* Directive art. 6(2).
[41] *See* Directive art. 6(1)(a).
[42] *See* Directive art. 6(3)-(4).
[43] *See* Directive art. 6(3)-(4).

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.

2.3.3 Administrative Processes

The requirement of financial responsibility and adequate errors and omissions insurance satisfy the Directive's requirements for financial resources sufficient to meet the Directive's requirements and bear the risk of liability for damages.[44]

2.4 Interpretation and Enforcement (DL1-2)

2.4.1 Governing Law

Pursuant to EDSP §§ 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, the following laws shall govern the enforceability, construction, interpretation, and validity of this EDSP, 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 EDSP. Agreements incorporating the EDSP by reference may have their own governing law provisions, provided that:

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

[44] *See* Directive annex II(h); ETSI Policy Document § 7.5.1(e)-(f).

separate and apart from the remaining provisions of any such agreements, subject to any limitations appearing in applicable law.

This EDSP is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information. In specific, the provision of services by a given Affiliate or Customer of an Affiliate is subject to the laws of EU Member Countries interpreting and implementing the Directive, which the EU Member Countries may modify from time to time. Requirements specific to a given EU Member Country shall appear in an Affiliate's CPS.

2.4.2 Severability, Survival, Merger, Notice

No stipulation.

2.4.3 Dispute Resolution Procedures

Affiliates' CPSs and/or agreements shall have policies and procedures for the resolution of complaints and disputes received from Subscribers, Relying Parties, other customers, or other parties about the provisioning of electronic trust services or any other related matters. Affiliates shall ensure that Customers within their Subdomains wishing to approve Certificate Applications for DL1 and DL2 Certificates agree to abide by such dispute resolution procedures.[45]

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

2.5 Fees (DL1-2)

No stipulation.

2.6 Publication and Repository (DL1-2)

2.6.1 Publication of CA Information

The requirement that VeriSign and Affiliates maintain a publicly-available repository making Certificates available satisfies the requirement for making Certificates available as necessary to Subscribers and Relying Parties.[46] 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 and relying party terms and conditions.[47] Revocation services, revocation status information, and Relying Party Agreements shall be available twenty-four (24)

[45] *See* ETSI Policy Document § 7.5(h).
[46] *See* Directive annex II(b), (l); ETSI Policy Document § 7.3.5.
[47] *See* Directive annex II(b), (l); ETSI Policy Document §§ 7.3.5(c), (f), 7.3.6, 7.3.6(k).

hours per day, seven (7) days per week.[48] The Relying Party Agreement shall be readily identifiable within the repository of a VeriSign or an Affiliate.[49] Upon system failure, or repository service unavailability, or other factors that are not under the control of VeriSign or an Affiliate, VeriSign or an Affiliate shall ensure that repository services are restored within the time limits set forth in CP § 4.8.4, EDSP § 4.8.4, and the applicable CPS.

2.6.2 Frequency of Publication

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

2.6.3 Access Controls

The controls imposed by VeriSign and Affiliates to prevent unauthorized persons from adding, deleting, or modifying repository entries under CP § 2.6.3 are intended to protect the integrity and authenticity of Certificate status information pursuant to the ETSI Policy Document.[50] More specifically, VeriSign and Affiliates shall use Trustworthy Systems for their repositories holding Qualified Certificates to store them in a verifiable form so that:

- Only authorized persons can make entries or changes,
- Information can be checked for authenticity,
- Qualified Certificates are publicly available for retrieval in only those cases for which the Subscriber's consent has been obtained, and
- Any technical changes resulting in a Compromise of these security requirements are apparent to the operator.[51]

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 under CP § 2.7 shall include a module to determine the CA's or RA's compliance with the applicable portion of the EDSP, the QCP public and QCP public + SSCD certificate policies in the ETSI Policy Document, and the Directive.[52] 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. An audit by an independent third party indicating compliance with the ETSI Policy Document and DL1 or DL2 satisfies the requirements of this EDSP § 2.7.

[48] *See* ETSI Policy Document §§ 7.3.5(e), 7.3.6(h)-(i).
[49] *See* ETSI Policy Document § 7.3.5(d).
[50] *See* ETSI Policy Document § 7.3.6(j); *see also* Directive annex II(b).
[51] *See* Directive annex II(l).
[52] *See* ETSI Policy Document § 5.4.1(b).

2.8 Confidentiality and Privacy (DL1-2)

VeriSign, Affiliates, and Customers shall comply with the requirements of applicable national data protection legislation when obtaining Certificate Application information.[53] In addition, they shall, in accordance with the Directive and ETSI Policy Document, [54] 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.[55] They shall also comply with the applicable EU Member Country's information retention legislation and may comply with its legislation to implement accreditation of CAs. VeriSign, Affiliates, and Customers shall collect personal data only directly from the Certificate Applicant, or after the explicit consent of the Certificate Applicant, and only insofar as it is necessary for the purposes of issuing and maintaining the Certificate. The data may not be collected or processed for any other purposes without the explicit consent of the Certificate Applicant.[56] Information considered confidential and private under applicable privacy policies shall be protected from loss, destruction, damage, falsification, and unauthorized or unlawful processing.[57]

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 or there is a legal requirement for disclosure.[58] This requirement shall appear in the privacy policies of Affiliates.

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.[59]

---

[53] *See* ETSI Policy Document § 7.3.1(k).
[54] *See* Directive art. 8(1); ETSI Policy Document § 7.4.10(b).
[55] Council Directive 1995/46/EC, 1995 O.J. (L 281) 31.
[56] *See* Directive art. 8(2).
[57] *See* ETSI Policy Document § 7.4.10(a), (c).
[58] *See* ETSI Policy Document § 7.4.10(d).
[59] *See* ETSI Policy Document § 7.4.11(c).

2.8.6 Disclosure Upon Owner's Request

Subscribers shall have access to registration and other information relating to him or herself.[60]

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 VeriSign retains all Intellectual Property Rights in and to this EDSP.

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.[61] 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.

[60] *See* ETSI Policy Document § 7.4.11(c).
[61] Directive art. 8(3).

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

No stipulation.

3.1.4 Uniqueness of Names (DL1-2)

The requirement in CP § 3.1.4 that names within a CA's domain are unique satisfies the requirement of the ETSI Policy Document.[62]

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 VeriSign-approved method, except where a key pair is generated by a CA on behalf of a Subscriber. This CP provision meets the requirement for a CA to ensure that the Subscriber has possession of the private key corresponding to the public key to be certified, except where a key pair is generated by the CA.[63]

3.1.8 Authentication of Organization Identity (DL1-2)

Not applicable.

3.1.9 Authentication of Individual Identity (DL1-2)

The identity of Class 2 and Class 3 Certificate Applicants must be authenticated, as noted in CP § 3.1.9, which shall be in accordance with national law.[64] Affiliates' procedures for the authentication of individual identity shall be approved by VeriSign prior to an Affiliate beginning its operations as CA or RA to issue or approve Certificate Applications for DL1 1-2 individual Certificates or as a provider of services to Customers issuing or approving Certificate Applications for DL 1-2 individual Certificates.

The authentication of DL1 and DL2 Qualified Certificates is based on the direct or indirect personal (physical) presence of the Certificate Applicant before an agent of the Affiliate or OnSite Customer, or before a notary public, authorized entity, or other official with comparable authority within the Certificate Applicant's jurisdiction. [65] 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 against a well-recognized form of government-

[62] *See* ETSI Policy Document § 7.3.3(d).
[63] *See* ETSI Policy Document § 7.3.1(j).
[64] *See* Directive annex II(d), (g); ETSI Policy Document § 7.3.1.
[65] *See* ETSI Policy Document § 7.3.1(c).

issued identification, such as a passport, driver's license, or national identity card, and one other identification credential. The credential shall include the full name of the Certificate Applicant (including surname and given name), as well as:

- date and place of birth (in accordance with national conventions for registering births),
- a nationally recognized identity number, or
- other attributes that may be used, insofar as possible, to distinguish the Certificate Applicant from persons with the same name.[66]

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 EDSP § 3.1.8 shall be consistent with applicable national law.[67]

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.[68]

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 Subscriber is still valid.[69] This procedure is for the purpose of ensuring that the person seeking to renew an end-user Subscriber Certificate is in fact the Subscriber of the Certificate, as required by CP § 3.2.1.[70]

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 Subscriber is still valid.[71] This procedure is for the purpose of ensuring that the person seeking to rekey is in fact the Subscriber of the Certificate, as required by CP § 3.3.[72]

---

[66] *See* ETSI Policy Document § 7.3.1(d).
[67] *See* ETSI Policy Document § 7.3.1(c).
[68] *See* ETSI Policy Document § 7.3.1(c).
[69] *See* ETSI Policy Document § 7.3.2(a).
[70] *See* Directive annex II(d), (g); ETSI Policy Document § 7.3.2.
[71] *See* ETSI Policy Document § 7.3.2(a).
[72] *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.[73]

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 EDSP §§ 2.1.1, 2.1.2,[74]
- The Certificate Applicant shall present evidence of identity consistent with EDSP § 3.1.9,[75] 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.[76]

Records retained in accordance with EDSP § 4.6 shall include the information used to authenticate the Certificate Applicant's identity (including any reference number on the documentation used for authentication and any limitations on its validity)[77] and a record of the signed subscriber agreement, whether in paper or electronic form.[78]

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 EDSP §§ 2.1.1, 2.1.2, and
- Records retained under EDSP § 4.6 shall also include the Subscriber's assent to any such changes.[79]

4.1.2 Certificate Applications for CA or RA Certificates

No stipulation.

---

[73] *See* ETSI Policy Document §§ 7.3.6, 7.3.6(c).
[74] *See* ETSI Policy Document § 7.3.1(a)-(b).
[75] *See* ETSI Policy Document § 7.3.1(d).
[76] *See* ETSI Policy Document § 7.3.1(f).
[77] *See* ETSI Policy Document § 7.3.1(g).
[78] *See* ETSI Policy Document § 7.3.1(h); *see also* ETSI Policy Document § 7.3.1(i).
[79] *See* ETSI Policy Document § 7.3.2(b)-(c).

4.2 Certificate Issuance (DL1-2)

4.2.1 Issuance of End-User Subscriber 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.[80] 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 EDSP § 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.[81]

The issuance of Certificates under EDSP § 3.2 is, as a technical matter, rekeying rather than a recertification of a previously-certified public key.[82]

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.[83] 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 EDSP § 5.3, including their non-discrimination requirement and training requirements,[84]
- Is obligated to make its services available to all applicants whose activities fall within its declared field of operation,[85]
- Is a legal entity,[86] which shall be confirmed as part of the authentication of the potential CA or RA organization,[87]
- Has a system or systems for quality and information security management appropriate for the certification services it is providing,[88] which, in the case of potential Affiliates, shall be confirmed as part of a Security and Practices Review performed under the CP,[89]
- Can meet the financial responsibility obligations of CP § 2.3 and EDSP § 2.3,[90]
- Can meet the dispute resolution requirements of EDSP § 2.4.3,[91]
- In the case of Affiliates, has a properly documented agreement and contractual relationship in place with its Superior Entity and any Customer approving Certificate Applications for Qualified Certificates,[92] and

---

[80] *See* ETSI Policy Document § 7.3.5(a).
[81] *See* Directive annex II(g); ETSI Policy Document §§ 7.3.3, 7.3.3(b)-(c).
[82] Therefore ETSI Policy Document § 7.3.2(d) does not apply.
[83] *See* Directive annex II(a); ETSI Policy Document § 7.5.
[84] *See* ETSI Policy Document § 7.5(a), (g).
[85] *See* ETSI Policy Document § 7.5.1(b).
[86] *See* ETSI Policy Document § 7.5(c).
[87] *See* CP § 3.1.8.2.
[88] *See* ETSI Policy Document § 7.5(d).
[89] *See* CP § 2.7.
[90] *See* ETSI Policy Document § 7.5(e)-(f).
[91] *See* ETSI Policy Document § 7.5(h).

- 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.[93]

4.3 Certificate Acceptance (DL1-2)

No stipulation.

4.4 Certificate Suspension and Revocation (DL1-2)

The ETSI Policy Document does not set 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,[94] 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.[95] When an end-user Subscriber uses a Challenge Phrase to request revocation, this requirement is met because the Certificate is automatically revoked upon validation of the revocation request. The Subscriber whose Certificate was revoked shall be informed of the revocation.[96] Certificates that are revoked shall not be reinstated as valid Certificates.[97]

4.4.4 Revocation Request Grace Period

No stipulation.

4.4.5 Circumstances for Suspension

Not applicable.

---

[92] *See* ETSI Policy Document § 7.5(i).
[93] *See* ETSI Policy Document § 7.5(j).
[94] *See* ETSI Policy Document § 7.3.6(a).
[95] *See* ETSI Policy Document § 7.3.6(b).
[96] *See* ETSI Policy Document § 7.3.6(e).
[97] *See* ETSI Policy Document § 7.3.6(f).

4.4.6 Who Can Request Suspension

Not applicable.

4.4.7 Procedure for Suspension Request

Not applicable.

4.4.8 Limits on Suspension Period

Not applicable.

4.4.9 CRL Issuance Frequency (If Applicable)

The requirement in CP § 4.4.9 that CRLs for end-user Subscriber Certificates shall be issued at least once per day meets the daily CRL-issuing requirement of the ETSI Policy Document.[98] 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 EDSP § 6.[99] A new CRL may be published before the stated time of the next CRL to be issued.[100]

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.

[98] *See* ETSI Policy Document § 7.3.6(g).
[99] *See* ETSI Policy Document § 7.3.6(g).
[100] *See* ETSI Policy Document § 7.3.6(g).

4.5 Security Audit Procedures (DL1-2)

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.[101]

4.5.1 Types of Events Recorded

When Processing Centers, Service Center, OnSite 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,[102] and
- All events relating to the lifecycle of CA keys.[103]
- In addition, Processing Centers generating RA or end-user Subscriber key pairs for placement on tokens and OnSite Customers using OnSite Key Manager shall log all events relating to the lifecycle of keys managed by such CAs.[104] If applicable, CAs issuing DL2 Certificates shall log all events relating to the preparation of SSCDs.[105]

The events and data logged shall be documented in Affiliates' CPSs.[106] The retention of event logs as provided in CP § 4.5 and EDSP § 4.5 facilitates holding personnel accountable for their activities.[107]

4.5.2 Frequency of Processing Log

The requirement of monitoring and alarm facilities in CP § 4.5.2 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.[108]

4.5.3 Retention Period for Audit Log

No stipulation.

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.[109]

---

[101] *See* Directive annex II(c); ETSI Policy Document § 7.4.11(d).
[102] *See* Directive annex II(i); ETSI Policy Document §§ 7.4.11, 7.4.11(h), (l), (o).
[103] *See* ETSI Policy Document § 7.4.11(k).
[104] *See* ETSI Policy Document § 7.4.11(m).
[105] *See* ETSI Policy Document § 7.4.11(n).
[106] *See* ETSI Policy Document § 7.4.11(g).
[107] *See* ETSI Policy Document § 7.4.6(f).
[108] *See* ETSI Policy Document § 7.4.6(i), (l).
[109] *See* ETSI Policy Document § 7.4.11(f).

4.5.5 Audit Log Backup Procedures

No stipulation.

4.5.6 Audit Collection System

No stipulation.

4.5.7 Notification to Event-Causing Subject

No stipulation.

4.5.8 Vulnerability Assessments

No stipulation.

4.6 Records Archival (DL1-2)

4.6.1 Types of Events Recorded

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

- The types of documents presented by Certificate Applicants in connection with their Certificate Applications;
- A record of unique identification data, numbers, or a combination thereof (e.g., a Certificate Applicant's driver's license or national identification card number) of identification documents, if applicable;
- The identity of the Affiliate, OnSite Customer, Gateway Customer, or ASB Provider that receives and accepts Certificate Applications; and
- A validation plan showing the methods used to validate identification documents.[110]

In addition, Affiliates, OnSite 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.[111]

[110] *See* ETSI Policy Document § 7.4.11(i).
[111] *See* ETSI Policy Document § 7.4.11(i).

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 § 4.6.2 is likely sufficient to meet the appropriateness requirement of the ETSI Policy Document.[112] This section is subject to any applicable Member Country-specific record retention requirements.

4.6.3 Protection of Archive

The protections of archived records against unauthorized viewing, modification, deletion, or other tampering by storage within a Trustworthy System meets the confidentiality and integrity requirements of the ETSI Policy Document.[113] The records retention requirements of section 4.6 shall be subject to the privacy and confidentiality requirements of CP § 2.8 and EDSP § 2.8 and the data projection legislation within the EU.[114]

4.6.4 Archive Backup Procedures

No stipulation.

4.6.5 Requirements for Time-Stamping of Records

See EDSP § 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 CP § 4.8.1 meet the corresponding requirements of the ETSI Policy Document.[115]

---

[112] *See* Directive annex II(i); ETSI Policy Document §§ 7.3.1(i), 7.4.11(e).
[113] *See* ETSI Policy Document § 7.4.11(a)-(b); *see also* ETSI Policy Document § 7.4.10(a), (c).
[114] *See* ETSI Policy Document § 7.4.11(a)-(b), (j).
[115] *See* ETSI Policy Document § 7.4.5(b), (g).

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.[116]

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.[117]

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.[118] 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.[119] 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 non-VeriSign CA (Affiliate, Client OnSite Customer, Gateway Customer, or ASB Customer) is terminated, such CA shall ensure that potential disruptions to Subscribers and Relying Parties resulting from the cessation of the CA's services are minimized.[120] Such CA shall implement a termination plan required under CP § 4.9, which shall include:

- Providing notice to parties affected by the termination, such as Subscribers, Relying Parties, and Customers,
- 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 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 key under CP § 6.2.9.2.[121]

Such non-VeriSign 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

[116] *See* ETSI Policy Document § 7.4.8(b).
[117] *See* ETSI Policy Document § 7.4.8(b) note 1.
[118] *See* ETSI Policy Document § 7.4.8(a); *see also* Directive annex II(a).
[119] *See* ETSI Policy Document § 7.4.8; *see also* ETSI Policy Document §§ 7.3.5(e), 7.3.6(h), (i).
[120] *See* ETSI Policy Document § 7.4.9; *see also* Directive annex II(a).
[121] *See* ETSI Policy Document § 7.4.9(a); *see also* Directive annex II(i).

itself.[122] Affiliates' CPSs shall implement the foregoing requirements and shall state whether unexpired unrevoked certificates will be revoked in connection with the termination.[123]

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.[124] Such security policies shall include administrative and management procedures that are adequate and correspond to recognized standards, as more particularly set forth in CP § 5 and this EDSP § 5.[125] 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.[126]

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

- Operational procedures and responsibilities;
- Secure systems planning and acceptance;
- Protection from malicious software;
- Housekeeping;
- Network management;
- Active monitoring of audit journals, event analysis, and followup;
- Media handling and security; and
- Data and software exchange.[127]

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.[128] Ultimately, however, senior management of the CA or RA has the responsibility for ensuring that its practices, including security practices, are properly implemented.[129]

5.1 Physical Controls

5.1.1 Site Location and Construction

The site location and construction requirements of CP § 5.1.1, which implement the requirements of the Security and Audit Requirements Guide and the Enterprise Security Guide, meet the ETSI Policy Document's requirements of physical protection within clearly defined security

[122] *See* ETSI Policy Document § 7.4.9(b).
[123] *See* ETSI Policy Document § 7.4.9(c).
[124] *See* ETSI Policy Document §§ 7.4.1(d), 7.4(b).
[125] *See* Directive annex II(e); ETSI Policy Document § 7.4.1.
[126] *See* ETSI Policy Document § 7.4.1(c).
[127] *See* ETSI Policy Document § 7.4.5(h) note 2.
[128] *See* ETSI Policy Document § 7.4.5(h) note 2.
[129] *See* ETSI Policy Document § 7.1(g).

perimeters around the Certificate generation, Subscriber device provision, and revocation management services.[130] 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.[131] These controls also protect against equipment, information, media, and software relating to CA services being taken offsite without authorization.[132]

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.[133]

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.[134] 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. [135]

5.1.4 Water Exposures

See EDSP § 5.1.3.

5.1.5 Fire Prevention and Protection

See EDSP § 5.1.3.

5.1.6 Media Storage

The media handling controls of CP § 5.1.6 satisfy the ETSI Policy Document's media security requirements.[136]

5.1.7 Waste Disposal

The waste disposal controls of CP § 5.1.7 satisfy the ETSI Policy Document's media disposal security requirement.[137]

---

[130] *See* ETSI Policy Document § 7.4.4(e).
[131] *See* ETSI Policy Document § 7.4.4(b)-(c); *see also* ETSI Policy Document § 7.4.4(f).
[132] *See* ETSI Policy Document § 7.4.4(g).
[133] *See* ETSI Policy Document § 7.4.6(h).
[134] *See* ETSI Policy Document § 7.4.4(a), (d).
[135] *See* ETSI Policy Document § 7.4.4(f).
[136] *See* ETSI Policy Document § 7.4.5(c), (e).

5.1.8 Off-Site Backup

No stipulation.

5.2 Procedural Controls

VeriSign, Affiliates, and Customers shall ensure that their systems are secure and correctly operated, with minimal risk of failure.[138] VeriSign, Affiliate, and Customer personnel shall perform administrative and management procedures and processes in accordance with their respective security policies.[139]

5.2.1 Trusted Roles

The security policies of VeriSign, Affiliates, and Customers shall clearly identify trusted roles.[140] CA/RA personnel hired to become Trusted Persons filling Trusted Positions shall be formally appointed pursuant to personnel security practices approved by senior management responsible for security.[141]

Trusted Positions shall include:

- Security personnel who administer the implementation of security practices;
- Administrators who approve Certificate Applications or the revocation of Certificates;
- System administrators, who install, configure, and maintain CA or RA Trustworthy Systems for enrollment, Certificate issuance, SSCD provision, and revocation management;
- System operators, who are responsible for operating CA or RA Trustworthy Systems on a day-to-day basis and who are authorized to perform system backups and recoveries; and
- System auditors, who are authorized to view and maintain archives and audit logs of the CA or RA trustworthy systems.[142]

VeriSign, Affiliates, and Customers shall establish and implement procedures for all Trusted Positions and administrative roles that have an impact on the provision of their services.[143]

5.2.2 Number of Persons Required Per Task

Security roles and responsibilities, as specified in VeriSign's, Affiliates', and Customers' security policies, shall be documented in job descriptions.[144] 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

---

[137] *See* ETSI Policy Document § 7.4.5(c), (e).
[138] *See* Directive annex II(e); ETSI Policy Document § 7.4.5.
[139] *See* ETSI Policy Document § 7.4.3(d).
[140] *See* ETSI Policy Document § 7.4.3(b).
[141] *See* ETSI Policy Document § 7.4.3(h).
[142] *See* ETSI Policy Document § 7.4.3(g).
[143] *See* ETSI Policy Document § 7.4.5(d).
[144] *See* ETSI Policy Document § 7.4.3(b).

that personnel shall be given the lowest level of privileges needed to perform their job functions.[145]

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.[146]

5.3 Personnel Controls

VeriSign, Affiliates, and Customers shall ensure that their personnel and hiring practices enhance and support the trustworthiness of their services.[147] VeriSign, Affiliates, and Customers shall employ a sufficient number of personnel necessary to provide their services in the context of the type, range, and volume of work performed.[148]

VeriSign, Affiliate, and Customer personnel holding Trusted Positions, senior executives, and senior staff members shall be free from conflicting interests, such as commercial, financial, or other pressures, that might prejudice the impartiality of their operations or adversely influence trust in the services they provide.[149] The organization within VeriSign, Affiliates, and Customers into which Administrators or other personnel performing Certificate generation and revocation management are hired shall be independent of other organizations in connection with the decisions of such Administrators or other personnel relating to establishing, provisioning, revoking, and maintaining services.[150] The parts of the organization of VeriSign, Affiliates, and Customers concerned with Certificate generation and revocation management shall have a documented structure that safeguards the impartiality of operations.[151]

VeriSign, Affiliates, and Customers shall develop and utilize in their hiring practices job descriptions developed to support the separation of duties, least privilege concept, determining position sensitivity based on duties and access levels, background screening, and employee training and awareness. Where appropriate, such job descriptions shall differentiate between general functions and CA/RA-specific functions and shall include skill and experience requirements.[152]

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.[153] In addition, managerial personnel hired by VeriSign, Affiliates, and Customers shall possess expertise or receive on-the-job training in

---

[145] *See* ETSI Policy Document § 7.4.3(c).
[146] *See* ETSI Policy Document § 7.4.6(e).
[147] *See* Directive annex II(e); ETSI Policy Document § 7.4.3.
[148] *See* ETSI Policy Document § 7.5.1(g).
[149] *See* ETSI Policy Document §§ 7.4.3(f), 7.5.2(a).
[150] *See* ETSI Policy Document § 7.5.2(a).
[151] *See* ETSI Policy Document § 7.5.2(b).
[152] *See* ETSI Policy Document § 7.4.3(c).
[153] *See* ETSI Policy Document §§ 7.4.3(a), 7.5.1(g).

Electronic Signature technology and familiarity with security procedures for personnel with security responsibilities.[154]

5.3.2 Background Check Procedures

Subject to limitations imposed by local law, the background check procedures required by CP § 5.3.2 will uncover criminal convictions. VeriSign, Affiliates, and Customers shall not appoint to Trusted Positions any person who is known to have a conviction for a serious crime or other offence that affects his or her suitability for the position for which he or she is a candidate. Such person shall not have access to the responsibilities or privileges granted to a Trusted Position until all background checks are completed.[155] Where local law precludes VeriSign, Affiliates, or Customers from obtaining information on criminal convictions, they are (subject to applicable law) entitled to ask candidates for Trusted Positions or management roles to provide such information, and candidates' refusal to provide such information shall be grounds for cancellation of offers of employment or the termination of existing personnel undergoing a periodic post-hiring background check.[156]

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.[157]

5.3.4 Retraining Frequency and Requirements

No stipulation.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

No stipulation.

5.3.7 Contracting Personnel Requirements

VeriSign, Affiliates, or Customers may use independent contractors to fill Trusted Positions pursuant to CP § 5.3.7. Nonetheless, they shall remain responsible for conformance with the procedures prescribed by this EDSP.[158]

---

[154] *See* ETSI Policy Document § 7.4.3(e).
[155] *See* ETSI Policy Document § 7.4.3(i).
[156] *See* ETSI Policy Document § 7.4.3(i) note 3.
[157] *See* ETSI Policy Document § 7.4.3(a).
[158] *See* ETSI Policy Document § 6.1.

5.3.8 Documentation Supplied to Personnel

The documentation that VeriSign, an Affiliate, or a Customer provides to its personnel pursuant to CP § 5.3.8 shall include its information security policy.[159]

6. Technical Security Controls

VeriSign, Affiliates, and Customers shall use Trustworthy Systems and products that are protected against modification and ensure the technical and cryptographic security of the processes supported by them.[160]

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.[161] Processing Centers shall generate CA keys in devices meeting the requirements of EDSP § 6.2.1.[162]

For DL2 Certificates, if the end-user Subscriber generates his or her own key pair, the key pair shall be generated within the Subscriber's SSCD.[163] Where Processing Centers pregenerate end-user Subscriber keys on tokens, including SSCDs, or Client OnSite Customers using OnSite Key Manager use the OnSite Key Manager Software to generate keys on behalf of end-user Subscribers, the Processing Center or Client OnSite Customer shall ensure that such keys are generated securely and the privacy of the end-user Subscriber's private key is assured.[164] One way in which this requirement may be met is using a suitable protection profile, defined in accordance with ISO 15048 or its equivalent.[165]

Article 9 of the Directive establishes an "Electronic-Signature Committee" to assist the European Commission.[166] A proposal exists currently for the establishment of a cryptographic advisory panel to assist the Committee.[167] 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.[168] 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

---

[159] *See* ETSI Policy Document § 7.4.1(b).
[160] *See* Directive annex II(f), (l); ETSI Policy Document § 7.4.7.
[161] *See* ETSI Policy Document § 7.2.1(a).
[162] *See* ETSI Policy Document § 7.2.1(b).
[163] *See* ETSI Policy Document § 6.2(f).
[164] *See* ETSI Policy Document § 7.2.9; *see also* Directive annex II(f), (g), (j).
[165] *See* ETSI Policy Document § 7.2.9 note 3.
[166] *See* Directive art. 9(1); *see also* ETSI Policy Document art. 10.
[167] *See* ETSI Policy Document §§ 6.2(d) note 1, 7.2.1(d) note 1, 7.2.8(b) note 1.
[168] *See* ETSI Policy Document §§ 6.2(d) note 1, 7.2.1(c), (d) note 1, 7.2.8(b) note 1.

"recognized as being fit for the purposes of qualified electronic signatures."[169] 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 OnSite Customers using OnSite Key Manager use the OnSite 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.[170]

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.[171]

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.[172]

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.[173]

---

[169] 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).
[170] *See* ETSI Policy Document § 7.2.8(c)-(d).
[171] *See* ETSI Policy Document § 7.2.8(c)-(d).
[172] *See* ETSI Policy Document § 7.2.9 & note 2.
[173] *See* ETSI Policy Document § 7.2.3; *see also* Directive annex II(g), (l).

6.1.5 Key Sizes (DL1-2)

The cryptographic advisory panel to assist the Electronic-Signature Committee referred to in EDSP § 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.[174] 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."[175] 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.

6.1.8 Hardware/Software Key Generation (DL1-2)

CA key pairs shall be generated in hardware meeting the requirements of EDSP § 6.2.1.[176] For Subscribers of DL2 Certificates generating their own keys, such generation shall take place on the SSCD hardware device they use.[177] Otherwise, end-user Subscriber 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 EDSP § 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.[178] Processing Centers shall protect CA keys in devices meeting the requirements of EDSP § 6.2.1.[179] 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.[180]

---

[174] *See* ETSI Policy Document §§ 6.2(d) note 1, 7.2.1(d) note 1, 7.2.8(b) note 1.
[175] ETSI Policy Document §§ 6.2(d), 7.2.1(d), 7.2.8(b).
[176] *See* ETSI Policy Document § 7.2.1(b).
[177] *See* ETSI Policy Document § 6.2(f).
[178] *See* ETSI Policy Document §§ 6.2(c), 7.2.2; *see also* Directive annex II(f), (g).
[179] *See* ETSI Policy Document § 7.2.2(a).
[180] *See* ETSI Policy Document § 7.2.5.

Where Client OnSite Customers using OnSite Key Manager use the OnSite Key Manager Software and Trustworthy Systems to deliver private keys to Subscribers or where private keys are pre-generated on hardware tokens, including SSCDs, the measures to protect such private keys shall conform to EDSP § 6.1.2.[181]

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 OnSite Customers, and ASB Customers within their Subdomains, on cryptographic modules that either:

- meet the requirements identified in FIPS 140-1 level 3 or utilize a set of controls that, as a whole, provide the level of security required by FIPS 140-1 level 3, or
- that are part of a Trustworthy System assured to EAL 4 or higher in accordance with ISO 15408 or equivalent security criteria, which assurance shall be in relation to a security target or protection profile that meets the requirements of the ETSI Policy Document, based on a risk analysis and taking into account physical and other non-technical security measures.[182]

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.[183]

6.2.3 Private Key Escrow (DL1-2)

CA private keys and end-user Subscriber signature private keys shall not be escrowed.[184] Therefore, notwithstanding the provision of CP § 6.2.3, Client OnSite Customers shall not use the OnSite Key Manager service to escrow end-user Subscribers' single private key (in single key pair systems). Client OnSite Customers wishing to use the OnSite Key Manager service shall use dual key pair systems and escrow only the decryption private keys of end-user Subscribers.

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.[185]

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

---

[181] *See* ETSI Policy Document § 7.2.8(c)-(d).
[182] *See* ETSI Policy Document §§ 7.2.1(b), 7.2.2(a).
[183] *See* ETSI Policy Document §§ 7.2.1(a), 7.2.2(c), 7.2.7(c).
[184] *See* Directive annex II(j); ETSI Policy Document § 7.2.4.
[185] *See* ETSI Policy Document § 7.2.2(c)-(d).

6.2.5 Private Key Archival (DL1-2)

CA private keys shall not be archived.

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

The encryption of CA private keys during the transfer from one cryptographic module to another as part of the backup process under CP § 6.2.6, and limiting exposure of CA private keys outside the cryptographic module to such backup procedures, meets the requirements in the ETSI Policy Document to prevent Compromises to CA private keys outside a cryptographic module.[186]

6.2.7 Method of Activating Private Key

6.2.7.1 DL1 Certificates

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

6.2.7.2 DL2 Certificates

In addition to the requirements of CP § 6.2.7.1, Subscribers of DL2 Certificates shall use an SSCD in connection with the use and activation of their private keys.[187]

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.[188]

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.[189]

---

[186] *See* ETSI Policy Document § 7.2.2(b), (e).
[187] *See* ETSI Policy Document § 6.2(e)-(f).
[188] *See* ETSI Policy Document § 7.2.6(a).
[189] *See* ETSI Policy Document § 7.2.6.

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 end-user Subscribers take steps to avoid use of their private keys.[190] *See also* EDSP § 6.1.2.2 (controls over the delivery of activation data used with SSCDs).

6.4.2 Activation Data Protection

See EDSP § 6.4.1.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls (DL1-2)

6.5.1 Specific Computer Security Technical Requirements

The requirement in CP § 6.5 that CA and RA functions take place on Trustworthy System consistent with the Security and Audit Requirements Guide (in the case of VeriSign and Affiliates) or the Enterprise Security Guide (in the case of OnSite 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.[191]

CP § 6.5.1 requires that Processing Centers, Service Centers, and OnSite 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.[192] 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.[193]

VeriSign, Affiliates, and Customers shall ensure effective administration of user access to maintain system security, including user account management, auditing, and timely modification or removal of access. Users include operators, Administrators, system administrators, and any users given direct access to the system.[194] Moreover, CA and RA personnel shall be successfully identified and authenticated before using critical applications related to certificate

[190] *See* ETSI Policy Document § 6.2(c).
[191] *See* ETSI Policy Document § 7.4.5(a).
[192] *See* Directive annex II(f); ETSI Policy Document § 7.4.6(a).
[193] *See* ETSI Policy Document § 7.4.6(a) note 1.
[194] *See* ETSI Policy Document §§ 7.4.5(c), 7.4.6.

management.[195] VeriSign, Affiliates, and Customers shall also ensure that access to information and application system functions is restricted in accordance with the entity's access control policy and that the CA/RA system provides sufficient computer security controls for the separation of Trusted Positions identified in a 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.[196]

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.[197]

CA system software for the issuance of Certificates shall enforce access control on attempts to add or delete Certificates or modify other associated information.[198] CA system software for the generation of Certificate status information shall enforce access control on attempts to modify Certificate status information.[199]

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.[200]

6.5.2 Computer Security Rating

The requirement that VeriSign, Affiliates, and Customers use Trustworthy Systems and products protected against modification may be ensured using, for example, systems conforming to a suitable protection profile (or profiles), defined in accordance with ISO 15408 or equivalent.[201] The risk analysis carried out on their services should identify critical services requiring Trustworthy Systems and the levels of assurance required.[202] *See also* EDSP § 6.2.1 (relating to the rating of CA systems that including cryptographic modules).

6.6 Life Cycle Technical Controls (DL1-2)

6.6.1 System Development Controls

An analysis of security requirements shall be carried out at the design and requirements specification stage of any systems development project undertaken with respect to the CA/RA software used by VeriSign, Affiliates, or Customers to ensure that security is built into IT

[195] *See* ETSI Policy Document § 7.4.6(e).
[196] *See* ETSI Policy Document § 7.4.5(d).
[197] *See* ETSI Policy Document § 7.4.5(g) & note 3; *see also* ETSI Policy Document § 7.4.6.
[198] *See* ETSI Policy Document § 7.4.6(k); *see also* Directive annex II(l).
[199] *See* ETSI Policy Document § 7.4.6(m); *see also* Directive annex II(l).
[200] *See* ETSI Policy Document § 7.4.6(i), (l).
[201] *See* ETSI Policy Document § 7.4.7 note 1.
[202] *See* ETSI Policy Document § 7.4.7 note 2.

systems.[203] Change control procedures shall be utilized for releases, modifications, and emergency software fixes for such software.[204]

6.6.2 Security Management Controls

VeriSign, Affiliates, and Customers shall maintain an inventory of all information assets and shall assign a classification of their protection requirements consistent with the risk analysis.[205] The configuration of Information Services systems supporting CA and RA functions shall be audited periodically, including under CP § 2.7 and EDSP § 2.7.[206] 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.[207]

Further, Processing Centers shall ensure the security of CA and RA cryptographic modules throughout their lifecycle.[208] More specifically, Processing Centers shall ensure that such cryptographic modules:

- Are not tampered with during shipment,[209]
- Are not tampered with while being stored,[210]
- Are functioning correctly,[211]
- 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 EDSP § 6.2.9.[212]

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls (DL1-2)

The requirement that VeriSign, Affiliates, and Customers protect communications using encryption and digital certificates satisfies the requirement that sensitive data be protected when exchanged over insecure networks.[213] Also, the confidentiality and integrity of registration data shall be protected, especially when being exchanged with the Subscriber or between distributed CA system components.[214] When registration data is exchanged with Processing Centers, or between OnSite Customers and their Superior Entities, the communicating parties shall authenticate themselves to each other.[215] Communications between Customers and Affiliates or

---

[203] *See* ETSI Policy Document § 7.4.7(a).
[204] *See* ETSI Policy Document § 7.4.7(b).
[205] *See* ETSI Policy Document § 7.4.2(a).
[206] *See* ETSI Policy Document § 7.4.6(h).
[207] *See* ETSI Policy Document § 7.4.5(f).
[208] *See* ETSI Policy Document § 7.2.7.
[209] *See* ETSI Policy Document § 7.2.7(a).
[210] *See* ETSI Policy Document § 7.2.7(b).
[211] *See* ETSI Policy Document § 7.2.7(d).
[212] *See* ETSI Policy Document § 7.2.7(e).
[213] *See* ETSI Policy Document § 7.4.6(b).
[214] *See* ETSI Policy Document § 7.3.3(e).
[215] *See* ETSI Policy Document § 7.3.3(f).

between Affiliates and VeriSign shall, in general, be secured so that the security of information among parties having distributed PKI responsibilities is maintained.[216]

6.8 Cryptographic Module Engineering Controls (DL1-2)

See CP § 6.2.1, EDSP § 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.[217]

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.[218] Third, CAs shall ensure that the SSCDs have been determined to meet the requirements of Annex III of the Directive by the applicable national body designated pursuant to Article 3(4) the Directive (if any).[219]

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,[220] as further specified in this EDSP § 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.[221] Also, the basic fields within Certificates required under CP § 7.1 adhere to the requirements of the Directive to include within Certificates:

- Signature-validation data (subject public key),[222]
- The beginning and end of their validity periods (valid from and valid to dates),[223]
- The identity code of the Certificate (serial number).[224]
- The Advanced Electronic Signature of the issuing certification-service-provider (digital signature of the CA).[225]

---

[216] *See* ETSI Policy Document § 7.4.1(e).
[217] *See* Directive annex III(1).
[218] *See* Directive annex III(2).
[219] Directive art. 3(4).
[220] *See* Qualified Certificate Profile § 1.
[221] *See* Qualified Certificate Profile § 4 (citing RFC 3039 Internet X.509 Public Key Infrastructure Qualified Certificates Profile [hereinafter "RFC 3039").
[222] *See* Directive annex I(e).
[223] *See* Directive annex I(f).
[224] *See* Directive annex I(g).
[225] *See* Directive annex I(h).

Processing Centers and Gateway Customers issuing DL1 and DL2 Certificates shall ensure that they have the profile set forth in this EDSP § 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 OnSite Customers, and ASB Customers within their Subdomains.

7.1.1 Version Number(s)

No stipulation.

7.1.2 Certificate Extensions

DL1 and DL2 Certificates shall contain a private extension containing an OID identifying the statement stating that the Certificate is issued in accordance with the Directive, as implemented in the country under which the applicable Affiliate is operating, in whose Subdomain the Certificate was issued. Such extension shall conform to the definition in section 4.2.1(2) of the Qualified Certificate Profile.[226] 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,[227] and
- An extension containing a statement indicating the record retention period applicable to the Certificate under CP § 4.6.1 and EDSP 4.6.1, in accordance with section 4.2.3 of the Qualified Certificate Profile.[228]

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.[229] The name of the Subscriber shall appear in the Subject field in accordance with CP § 7.1.4.[230]

7.1.5 Name Constraints

No stipulation.

---

[226] *See* Directive annex I(a); Qualified Certificate Profile § 4.2.1(2).
[227] *See* Directive annex I(j); Qualified Certificate Profile § 4.2.2.
[228] *See* Qualified Certificate Profile § 4.2.3.
[229] *See* Directive annex I(b); Qualified Certificate Profile § 4.1.
[230] *See* Directive annex I(c).

7.1.6 Certificate Policy Object Identifier

The object identifier for the Certificate policy corresponding to DL1 and DL2 is set forth in EDSP § 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 EDSP § 1.2. Note that the DL1 and DL2 policies, whose OIDs appear within the Certificate Policies extension Certificates issued under this EDSP, 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.[231] Moreover, by virtue of including the DL1 OID or DL2 OID, which refer to the policies of this EDSP containing limitations on the scope of the use of the Certificate, DL1 and DL2 Certificates contain such limitations.[232]

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 EDSP shall be made by the VeriSign Trust Network Policy Management Authority. Amendments shall either be in the form of a document containing an amended form of the EDSP or an update. Amended versions or updates shall be linked to the Practices Updates and Notices section of the VeriSign Repository located at: **https://www.verisign.com/repository/updates**. Updates supersede any designated or conflicting provisions of the referenced version of the EDSP. The PMA shall determine whether changes to the EDSP 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

[231] *See* Qualified Certificate Profile § 4.2.1(1); *see also* Directive annex I(a).
[232] *See* Directive annex I (i).

for maintaining their CPSs.[233] 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 EDSP § 8.3, publish the revised CPS as required under EDSP § 8.2.[234]

8.1.1 Items that Can Change Without Notification

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

8.1.2 Items that Can Change with Notification

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

8.1.2.1 List of Items

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

8.1.2.2 Notification Mechanism

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

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

[233] *See* ETSI Policy Document § 7.1(h).
[234] *See* ETSI Policy Document § 7.1(i).

8.1.2.3 Comment Period

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

8.1.2.4 Mechanism to Handle Comments

The PMA shall consider any comments on the proposed amendments. The PMA shall either (a) allow the proposed amendments to become effective without amendment, (b) amend the proposed amendments and republish them as a new amendment under EDSP § 8.1.2.2, or (c) withdraw the proposed amendments. The PMA is entitled to withdraw proposed amendments by notifying Affiliates and providing notice in the Practices Updates and Notices section of the VeriSign Repository. Unless proposed amendments are amended or withdrawn, they shall become effective upon the expiration of the comment period under Section 8.1.2.3.

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

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

8.2 Publication and Notification Policies

8.2.1 Items Not Published in the EDSP or CPS

Security documents and information in them considered confidential by VeriSign and the Affiliates are not disclosed to the public.[235]

8.2.2 Distribution of the EDSP and CPSs

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

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 EDSP and ultimately the Directive.[236]

---

[235] *See* ETSI Policy Document § 7.1(d) note 2.
[236] *See* ETSI Policy Document § 7.1(d).

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,[237]
- Such Affiliates shall write a CPS to address all the requirements addressed in this EDSP (which ultimately apply the requirements of the Directive, ETSI Policy Document, and Qualified Certificate Policy),[238] which CPS may be the same CPS written pursuant to the CP,
- Such CPS shall identify the requirements of VeriSign and their Customers, including their applicable procedures and practices,[239]
- Such Affiliates shall establish a high level management body with final authority and responsibility for approving the CPS,[240] and
- The Affiliate shall submit this CPS to VeriSign for approval under CP § 8.3.

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

Such CPSs demonstrate reliability of CAs within Affiliates' respective Subdomains necessary for providing Certification services.[241] 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.[242]

Acronyms and Definitions

Table of Acronyms

Acronym	Term
ANSI	The American National Standards Institute.
ASB	Authentication Service Bureau.
B2B	Business-to-business.
BXA	The United States Bureau of Export Administration of the United States Department of Commerce.
CA	Certification Authority.
CP	Certificate Policy.
CPS	Certification Practice Statement.
CRL	Certificate Revocation List.

[237] *See* ETSI Policy Document § 7.1(a).
[238] *See* ETSI Policy Document § 7.1(b).
[239] *See* ETSI Policy Document § 7.1(c).
[240] *See* ETSI Policy Document § 7.1(f).
[241] *See* ETSI Policy Document § 7.1 (citing Directive annex II(a)).
[242] *See* ETSI Policy Document § 7.1(c).

Acronym	Term
EAL	Evaluation assurance level (pursuant to the Common Criteria).
EDI	Electronic Data Interchange.
EDIFACT	EDI for Administration, Commerce, and Transport (standards established by the United Nations Economic Commission for Europe).
EDSP	European Directive Supplemental Policies
ETSI	European Telecommunications Standards Institute
FIPS	United State Federal Information Processing Standards.
ICC	International Chamber of Commerce.
ISO	International Organization for Standardization
KRB	Key Recovery Block.
LSVA	Logical security vulnerability assessment.
OCSP	Online Certificate Status Protocol.
OFX	Open Financial Exchange.
PCA	Primary Certification Authority.
PIN	Personal identification number.
PKCS	Public-Key Cryptography Standard.
PKI	Public Key Infrastructure.
PMA	Policy Management Authority.
QCP	Qualified Certificate Policy
RA	Registration Authority.
RFC	Request for comment.
SAS	Statement on Auditing Standards (promulgated by the American Institute of Certified Public Accountants).
S/MIME	Secure multipurpose Internet mail extensions.
SSCD	Secure-Signature-Creation Device
SSL	Secure Sockets Layer.
VTN	VeriSign Trust Network.
WAP	Wireless Application Protocol.
WTLS	Wireless Transport Layer Security.

Definitions

Term	Definition
Administrator	A Trusted Person within the organization of a Processing Center, Service Center, OnSite Customer, or Gateway Customer that performs validation and other CA or RA functions.
Administrator Certificate	A Certificate issued to an Administrator that may only be used to perform CA or RA functions.
Advanced Electronic Signature	An Electronic Signature which meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using means that the signatory can maintain under his sole control; and (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Term	Definition
Affiliate	A leading trusted third party, for example in the technology, telecommunications, or financial services industry, that has entered into an agreement with VeriSign to be a VTN distribution and services channel within a specific territory.
Affiliate Audit Program Guide	A VeriSign document containing requirements for the Compliance Audits of Affiliates, including Certificate Management Control Objectives against which Affiliates will be audited.
Affiliate Practices Legal Requirements Guidebook	A VeriSign document setting forth requirements for Affiliate CPSs, agreements, validation procedures, and privacy policies, as well as other requirements that Affiliates must meet.
Affiliated Individual	A natural person that is related to a Client OnSite Customer, Client OnSite Lite Customer, or Gateway Customer entity (i) as an officer, director, employee, partner, contractor, intern, or other person within the entity, (ii) as a member of a VeriSign registered community of interest, or (iii) as a person maintaining a relationship with the entity where the entity has business or other records providing appropriate assurances of the identity of such person.
ASB Customer	An entity that contracts with VeriSign or an Affiliate to obtain Authentication Service Bureau services. An ASB Customer is a CA, and is named as such within the Certificates issued by its CA, but it outsources all CA functions to an ASB Provider.
ASB Provider	An entity (either VeriSign or an Affiliate) that offers Authentication Service Bureau services to ASB Customers. An ASB Provider acts as an outsourcing provider of back-end functions for an ASB Customer and as an RA for the ASB Customer.
Authentication Service Bureau	A service within the VTN by which VeriSign or an Affiliate performs most front-end RA and all back-end CA functions on behalf of an organization.
Automated Administration	A procedure whereby Certificate Applications are approved automatically if enrollment information matches information contained in a database.
Automated Administration Software Module	Software provided by VeriSign that performs Automated Administration.
Certificate	A message that, at least, states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key, identifies the Certificate's Operational Period, contains a Certificate serial number, and is digitally signed by the CA.
Certificate Applicant	An individual or organization that requests the issuance of a Certificate by a CA.
Certificate Application	A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.
Certificate Chain	An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.
Certificate Management	Criteria that an entity must meet in order to satisfy a Compliance

Term	Definition
Control Objectives	Audit.
Certificate Policies (CP)	This document, which is entitled "VeriSign Trust Network Certificate Policies" and is the principal statement of policy governing the VTN.
Certificate Revocation List (CRL)	A periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation.
Certificate Signing Request	A message conveying a request to have a Certificate issued.
Certification Authority (CA)	An entity authorized to issue, manage, revoke, and renew Certificates in the VTN.
Certification Practice Statement (CPS)	A statement of the practices that VeriSign or an Affiliate employs in approving or rejecting Certificate Applications and issuing, managing, and revoking Certificates, and requires its OnSite Customers and Gateway Customers to employ.
Challenge Phrase	A secret phrase chosen by a Certificate Applicant during enrollment for a Certificate. When issued a Certificate, the Certificate Applicant becomes a Subscriber and a CA or RA can use the Challenge Phrase to authenticate the Subscriber when the Subscriber seeks to revoke or renew the Subscriber's Certificate.
Class	A specified level of assurances as defined within the CP. See CP § 1.1.1.
Class 2 Individual ASB Certificate	A Class 2 individual Certificate issued by an ASB Provider on behalf of an ASB Customer CA.
Class 3 Organizational ASB Certificate	A Class 3 organizational Certificate issued by an ASB Provider on behalf of an ASB Customer CA.
Client OnSite Customer	An organization that has obtained OnSite services from VeriSign or an Affiliate, whereby the organization becomes a CA within the VTN to issue client Certificates. Client OnSite Customers outsource back-end functions of issuance, management, and revocation to VeriSign or the Affiliate, but retain for themselves the RA functions of approving or rejecting Certificate Applications and initiating revocations and renewals of Certificates.
Client OnSite Lite Customer	An organization that has obtained OnSite Lite services from VeriSign or an Affiliate, whereby the organization becomes a Registration Authority within the VTN to assist a VeriSign or Affiliate CA to issue client Certificates. This CA delegates to Client OnSite Lite Customers the RA functions of approving or rejecting Certificate Applications and initiating revocations and renewals of Certificates.
Client Service Center	A Service Center that is an Affiliate providing client Certificates either in the Consumer or Enterprise line of business.
Compliance Audit	A periodic audit that a Processing Center, Service Center, OnSite

Term	Definition
	Customer, or Gateway Customer undergoes to determine its conformance with VTN Standards that apply to it.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred.
Confidential/Private Information	Information required to be kept confidential and private pursuant to CP § 2.8.1.
Consumer, as in Consumer Service Center	A line of business that an Affiliate enters to provide client Retail Certificates to Certificate Applicants.
CRL Usage Agreement	An agreement setting forth the terms and conditions under which a CRL or the information in it can be used.
Customer	An organization that is either an OnSite Customer, Gateway Customer, or ASB Customer.
Digital Receipt	A data object created in connection with the VeriSign Digital Notarization Service and digitally signed by the Time-Stamping Authority that includes the hash of a document or set of data and a time-stamp showing that the document or data existed at a certain time.
Electronic Data Interchange (EDI)	The computer-to-computer exchange of business transactions, such as purchase orders, invoices, and payment advices in accordance with applicable standards.
Electronic Data Interchange Certificate (EDI Certificate)	A Class 3 organizational Certificate that allows for digital signatures on Electronic Data Interchange messages and for the encryption of EDI messages.
Electronic Signature	Data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication of that data.
Enterprise, as in Enterprise Service Center	A line of business that an Affiliate enters to provide OnSite services to OnSite Customers.
Enterprise Roaming Server	A server residing at the site of a Client OnSite Customer used in conjunction with the VeriSign Roaming Service to hold Roaming Subscribers' encrypted private keys and portions of symmetric keys used to encrypt and decrypt Roaming Subscribers' private keys.
Enterprise Security Guide	A document setting forth security requirements and practices for OnSite Customers and Gateway Customers.
Exigent Audit/Investigation	An audit or investigation by VeriSign where VeriSign has reason to believe that an entity's failure to meet VTN Standards, an incident or Compromise relating to the entity, or an actual or potential threat to the security of the VTN posed by the entity has occurred.
Gateway	A service offered by VeriSign or an Affiliate to allow an organization using a stand-alone Certificate server to become a CA within the VTN by having a VeriSign CA certify the organization's public key.
Gateway Administrator	An Administrator that performs validation or other RA functions for a Gateway Customer.

Term	Definition
Gateway Certificate	A Certificate issued to a Gateway Customer certifying its public key.
Gateway Customer	An organization that has obtained Gateway services from VeriSign or an Affiliate, whereby the organization becomes a CA within the VTN to issue Class 1 Certificates.
Global Server ID	A Class 3 organizational Certificate used to support SSL sessions between web browsers and web servers that are encrypted using strong cryptographic protection consistent with applicable export laws.
Global Server OnSite	A type of OnSite service that permits an organization to become an RA within the VTN to assist a VeriSign or Affiliate CA to issue Global Server IDs within designated domains. This CA delegates to Global Server OnSite Customers the RA functions of approving or rejecting Certificate Applications and initiating revocations and renewals of Global Server IDs.
Global Server OnSite Customer	An organization that has obtained Global Server OnSite services from VeriSign or an Affiliate.
Go Secure!	A suite of plug-and-play services building on OnSite services and designed to accelerate e-commerce applications.
Intellectual Property Rights	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.
Intermediate Certification Authority (Intermediate CA)	A Certification Authority whose Certificate is located within a Certificate Chain between the Certificate of the root CA and the Certificate of the Certification Authority that issued the end-user Subscriber's Certificate.
Key Ceremony Reference Guide	A document describing Key Generation Ceremony requirements and practices.
Key Generation Ceremony	A procedure whereby a CA's or RA's key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.
Key Manager Administrator	An Administrator that performs key generation and recovery functions for a Client OnSite Customer using OnSite Key Manager.
Key Recovery Block (KRB)	A data structure containing a Subscriber's private key that is encrypted using an encryption key. KRBs are generated using OnSite Key Manager software.
Key Recovery Service	A VeriSign service that provides encryption keys needed to recover a Key Recovery Block as part of a Client OnSite Customer's use of OnSite Key Manager to recover a Subscriber's private key.
Manual Authentication	A procedure whereby Certificate Applications are reviewed and approved manually one-by-one by an Administrator using a web-based interface.
NetSure Protection Plan	An extended warranty program, which is described in CP § 1.1.2.2.3.
Nonverified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the

Term	Definition
	CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.
Non-repudiation	An attribute of a communication that provides protection against a party to a communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the identity associated with the sender is unknown. Note: only an adjudication by a court, arbitration panel, or other tribunal can ultimately prevent repudiation. For example, a digital signature verified with reference to a VTN Certificate may provide proof in support of a determination of Non-repudiation by a tribunal, but does not by itself constitute Non-repudiation.
OFX Certificate	A Class 3 organizational Certificate issued to a financial institution's server for use with the Open Financial Exchange specification.
Online Certificate Status Protocol (OCSP)	A protocol for providing Relying Parties with real-time Certificate status information.
OnSite	VeriSign's fully integrated managed PKI service that allows enterprise Customers of VeriSign and its Affiliates to distribute Certificates to individuals, such as employees, partners, suppliers, and customers, as well as devices, such as servers, routers, and firewalls. OnSite permits enterprises to secure messaging, intranet, extranet, virtual private network, and e-commerce applications.
OnSite Administrator	An Administrator that performs validation or other RA functions for an OnSite Customer.
OnSite Administrator's Handbook	A VeriSign document setting forth the operational requirements and practices for OnSite Customers.
OnSite Agreement	An agreement under which an organization becomes an OnSite Customer and agrees to be bound by VeriSign's or an Affiliate's CPS.
OnSite Certificate	A Certificate whose Certificate Application was approved by an OnSite Customer.
OnSite Control Center	A web-based interface that permits OnSite Administrators to perform Manual Authentication of Certificate Applications.
OnSite Customer	An organization that is one or more of the following: a Client OnSite Customer, a Client OnSite Lite Customer, a Server OnSite Customer, or a Global Server OnSite Customer.
OnSite Key Manager	A key recovery solution for those Client OnSite Customers choosing to implement key recovery under a special OnSite Agreement.
OnSite Key Management Service Administrator's Guide	A document setting forth the operational requirements and practices for Client OnSite Customers using OnSite Key Manager.

Term	Definition
OnSite Lite	A type of OnSite service that permits an organization to become a Registration Authority within the VTN to assist a VeriSign or Affiliate CA to issue client Certificates.
Open Financial Exchange (OFX)	A standard web-based specification for the electronic exchange of financial data among financial institutions, businesses, and consumers.
Operational Period	The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKCS #12	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
Policy Management Authority (PMA)	The organization within VeriSign responsible for promulgating this policy throughout the VTN.
Primary Certification Authority (PCA)	A CA that acts as a root CA for a specific Class of Certificates, and issues Certificates to CAs subordinate to it.
Processing Center	An organization (VeriSign or certain Affiliates) that creates a secure facility housing, among other things, the cryptographic modules used for the issuance of Certificates. In the Consumer and Web Site lines of business, Processing Centers act as CAs within the VTN and perform all Certificate lifecycle services of issuing, managing, revoking, and renewing Certificates. In the Enterprise line of business, Processing Centers provide lifecycle services on behalf of their OnSite Customers or the OnSite Customers of the Service Centers subordinate to them.
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system. The VTN PKI consists of systems that collaborate to provide and implement the VTN.
Qualified Certificate	A Certificate which meets the requirements laid down in annex I (of the Directive) and is provided by a certification-service-provider who fulfils the requirements laid down in annex II (of the Directive).
Qualified Electronic Signature	An Advanced Electronic Signature which is based on a Qualified Certificate and which is created by an Secure-Signature-Creation Device, as defined in article 5.1 of the Directive.
Registration Authority (RA)	An entity approved by a CA to assist Certificate Applicants in applying for Certificates, and to approve or reject Certificate Applications, revoke Certificates, or renew Certificates.
Relying Party	An individual or organization that acts in reliance on a certificate

Term	Definition
	and/or a digital signature.
Relying Party Agreement	An agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a Relying Party.
Retail Certificate	A Certificate issued by VeriSign or an Affiliate, acting as CA, to individuals or organizations applying one by one to VeriSign or an Affiliate on its web site.
Roaming Subscriber	A Subscriber using the VeriSign Roaming Service whose private key is encrypted and decrypted with a symmetric key that is split between the VeriSign Roaming Server and an Enterprise Roaming Server.
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
RSA Secure Server Certification Authority (RSA Secure Server CA)	The Certification Authority that issues Secure Server IDs.
RSA Secure Server Hierarchy	The PKI hierarchy comprised of the RSA Secure Server Certification Authority.
Secret Share	A portion of a CA private key or a portion of the activation data needed to operate a CA private key under a Secret Sharing arrangement.
Secret Sharing	The practice of splitting a CA private key or the activation data to operate a CA private key in order to enforce multi-person control over CA private key operations under CP § 6.2.2.
Secure Server ID	A Class 3 organizational Certificate used to support SSL sessions between web browsers and web servers.
Secure-Signature-Creation Device (SSCD)	A device, comprised of configured software or hardware used to implement a private key used to create a digital signature, which meets the requirements laid down in annex III (of the Directive).
Secure Sockets Layer (SSL)	The industry-standard method for protecting Web communications developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a Transmission Control Protocol/Internet Protocol connection.
Security and Audit Requirements Guide	A VeriSign document that sets forth the security and audit requirements and practices for Processing Centers and Service Centers.
Security and Practices Review	A review of an Affiliate performed by VeriSign before an Affiliate is permitted to become operational.
Server Gated Cryptography	A technology that permits web servers that have been issued a Global Server ID to create an SSL session with a browser that is encrypted using strong cryptographic protection.
Server OnSite	A type of OnSite service that permits an organization to become an RA within the VTN to assist a VeriSign or Affiliate CA to issue Secure Server IDs within designated domains. This CA delegates to Server OnSite Customers the RA functions of approving or rejecting

Term	Definition
	Certificate Applications and initiating revocations and renewals of Secure Server IDs.
Server OnSite Customer	An organization that has obtained Server OnSite services from VeriSign or an Affiliate.
Server Service Center	A Service Center that is an Affiliate providing Secure Server IDs and Global Server IDs either in the Web Site or Enterprise line of business.
Service Center	An Affiliate that does not house Certificate signing units for the issuance of Certificates for the purpose of issuing Certificates of a specific Class or type, but rather relies on a Processing Center to perform issuance, management, revocation, and renewal of such Certificates.
Subdomain	The portion of the VTN under control of an entity and all entities subordinate to it within the VTN hierarchy.
Subject	The holder of a private key corresponding to a public key. The term "Subject" can, in the case of an organizational Certificate, refer to the equipment or device that holds a private key. A Subject is assigned an unambiguous name, which is bound to the public key contained in the Subject's Certificate.
Subscriber	In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organizational Certificate, an organization that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. A Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate.
Subscriber Agreement	An agreement used by a CA or RA setting forth the terms and conditions under which an individual or organization acts as a Subscriber.
Superior Entity	An entity above a certain entity within a VTN hierarchy (the Class 1, 2, or 3 hierarchy).
Supplemental Risk Management Review	A review of an entity by VeriSign following incomplete or exceptional findings in a Compliance Audit of the entity or as part of the overall risk management process in the ordinary course of business.
Reseller	An entity marketing services on behalf of VeriSign or an Affiliate to specific markets.
Time-Stamping Authority	The VeriSign entity that signs Digital Receipts as part of the VeriSign Digital Notarization Service.
Time-Stamping Authority CA	The VeriSign CA that issued a special Class 3 organizational Certificate to the Time-Stamping Authority used to verify the digital signatures on Digital Receipts.
Trusted Person	An employee, contractor, or consultant of an entity within the VTN responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices as

Term	Definition
	further defined in CP § 5.2.1.
Trusted Position	The positions within a VTN entity that must be held by a Trusted Person.
Trustworthy System	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognized in classified government nomenclature.
Universal Service Center	An entity participating in the Universal Service Center Program.
Universal Service Center Program	A program by which entities market VeriSign's services to specific markets using a specialized software platform for managing complex, multi-tiered PKI deployment.
VeriSign Digital Notarization Service	A service offered to Client OnSite Customers that provides a digitally signed assertion (a Digital Receipt) that a particular document or set of data existed at a particular point in time.
VeriSign Repository	VeriSign's database of Certificates and other relevant VeriSign Trust Network information accessible on-line.
VeriSign Roaming Server	A server residing at VeriSign's Processing Center used in conjunction with the VeriSign Roaming Service to hold portions of symmetric keys used to encrypt and decrypt Roaming Subscribers' private keys.
VeriSign Roaming Service	The service offered by VeriSign that enables a Subscriber to download his or her private key and perform private key operations on different client terminals.
VeriSign Security Policy	The highest-level document describing VeriSign's security policies.
VeriSign Trust Network (VTN)	The Certificate-based Public Key Infrastructure governed by the VeriSign Trust Network Certificate Policies, which enables the worldwide deployment and use of Certificates by VeriSign and its Affiliates, and their respective Customers, Subscribers, and Relying Parties.
VTN Participant	An individual or organization that is one or more of the following within the VTN: VeriSign, an Affiliate, a Customer, a Universal Service Center, a Reseller, a Subscriber, or a Relying Party.
VTN Standards	The business, legal, and technical requirements for issuing, managing, revoking, renewing, and using Certificates within the VTN.
Web Host	An entity hosting the web site of another, such as an Internet service provider, a systems integrator, a Reseller, a technical consultant, and application service provider, or similar entity.
Web Host Program	A program that allows Web Hosts to enroll for Secure Server IDs and Global Server IDs on behalf of end-user Subscribers who are customers of the Web Hosts.
Web Site, as in Web Site Service Center	A line of business that an Affiliate enters to provide Secure Server ID and Global Server ID Retail Certificates one by one to

Term	Definition
	Certificate Applicants.
Wireless Application Protocol (WAP)	A standard for the presentation and delivery of wireless information and telephony services on mobile phones and other wireless terminals.
Wireless Transport Layer Security (WTLS)	A protocol that protects the communication of applications that operate using the Wireless Application Protocol, such as communications between a wireless handset and a server.
Wireless Transport Layer Security Certificate (WTLS Certificate)	A Class 3 organizational Certificate whose format is defined as part of the Wireless Application Protocol, which authenticates a Wireless Transport Layer Security server to a WTLS client and facilitates encrypted communication between the WTLS server and the WTLS client.

Cross-Reference of ETSI Definitions to CP Definitions

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