



TeliaSonera Server Certificate Policy and Certification Practice Statement – v.1.3

**TeliaSonera Server
Certificate Policy and
Certification Practice Statement**

CA name	OID
TeliaSonera Server CA v1 TeliaSonera Server CA v2	1.3.6.1.4.1.271.2.3.1.1.15
TeliaSonera Extended Validation SSL CA v1	1.3.6.1.4.1.271.2.3.1.1.17

Revision Date: 16th April 2015

Version: 1.3

Published by: TeliaSonera

Copyright © TeliaSonera

Copyright © TeliaSonera

No part of this document may be reproduced, modified or distributed in any form or by any means, in whole or in part, or stored in a database or retrieval system, without prior written permission of TeliaSonera.

However, permission generally applies for reproducing and disseminating this CPS in its entirety provided that this is at no charge and that no information in the document is added to, removed or changed.

Table of Contents

Table of Contents	III
Revision History	VII
1 INTRODUCTION	8
1.1 Overview.....	8
1.2 Document name and identification	8
1.3 PKI participants	9
1.3.1 Certification authorities	9
1.3.2 Registration authorities	9
1.3.3 Subscribers	9
1.3.4 Relying parties	9
1.3.5 Other participants.....	9
1.4 Certificate usage.....	9
1.4.1 Appropriate certificate uses	9
1.4.2 Prohibited certificate uses.....	10
1.5 Policy administration.....	10
1.5.1 Organization administering the document	10
1.5.2 Contact person.....	10
1.5.3 Person determining CPS suitability for the policy.....	10
1.5.4 CPS approval procedures.....	11
1.6 Definitions and acronyms	11
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES	12
2.1 Repositories.....	12
2.1.1 CPS Repository	12
2.1.2 Revocation Information Repository.....	12
2.1.3 Certificate Repository	12
2.2 Publication of certification information	12
2.3 Time or frequency of publication.....	12
2.4 Access controls on repositories	12
3 IDENTIFICATION AND AUTHENTICATION	13
3.1 Naming	13
3.1.1 Types of names	13
3.1.2 Need for names to be meaningful.....	13
3.1.3 Anonymity or pseudonymity of Subscribers	13
3.1.4 Rules for interpreting various name forms.....	14
3.1.5 Uniqueness of names	14
3.1.6 Recognition, authentication, and role of trademarks	14
3.2 Initial identity validation.....	14
3.2.1 Method to prove possession of private key	14
3.2.2 Authentication of organization identity.....	14
3.2.3 Authentication of individual identity.....	14
3.2.4 Non-verified Subscriber information	15
3.2.5 Validation of authority	15
3.2.6 Criteria for interoperation	15
3.3 Identification and authentication for re-key requests	15
3.3.1 Identification and authentication for routine re-key.....	15
3.3.2 Identification and authentication for re-key after revocation.....	15
3.4 Identification and authentication for revocation request	15
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	17
4.1 Certificate Application.....	17
4.1.1 Who can submit a certificate application	17
4.1.2 Enrollment process and responsibilities	17
4.2 Certificate application processing	17
4.2.1 Performing identification and authentication functions	17
4.2.2 Approval or rejection of certificate applications	18

4.2.3	Time to process certificate applications.....	18
4.3	Certificate issuance	18
4.3.1	CA actions during certificate issuance.....	18
4.3.2	Notification to Subscriber by the CA of issuance of certificate	18
4.4	Certificate acceptance	18
4.4.1	Conduct constituting certificate acceptance	18
4.4.2	Publication of the certificate by the CA.....	18
4.4.3	Notification of certificate issuance by the CA to other entities.....	18
4.5	Key pair and certificate usage	18
4.5.1	Subscriber private key and certificate usage.....	18
4.5.2	Relying party public key and certificate usage	19
4.6	Certificate renewal.....	19
4.6.1	Circumstance for certificate renewal.....	19
4.6.2	Who may request renewal.....	19
4.6.3	Processing certificate renewal requests	19
4.6.4	Notification of new certificate issuance to Subscriber	19
4.6.5	Conduct constituting acceptance of a renewal certificate	19
4.6.6	Publication of the renewal certificate by the CA	19
4.6.7	Notification of certificate issuance by the CA to other entities.....	20
4.7	Certificate re-key.....	20
4.8	Certificate modification	20
4.9	Certificate revocation and suspension.....	20
4.9.1	Circumstances for revocation	20
4.9.2	Who can request revocation	20
4.9.3	Procedure for revocation request	20
4.9.4	Revocation request grace period.....	21
4.9.5	Time within which CA must process the revocation request	21
4.9.6	Revocation checking requirement for relying parties.....	21
4.9.7	CRL issuance frequency.....	21
4.9.8	Maximum latency for CRLs.....	21
4.9.9	On-line revocation/status checking availability	21
4.9.10	On-line revocation checking requirements	22
4.9.11	Other forms of revocation advertisements available	22
4.9.12	Special requirements regarding key compromise	22
4.9.13	Circumstances for suspension.....	22
4.9.14	Who can request suspension	22
4.9.15	Procedure for suspension request.....	22
4.9.16	Limits on suspension period	22
4.10	Certificate status services.....	22
4.10.1	Operational characteristics	22
4.10.2	Service availability	22
4.10.3	Optional features.....	22
4.11	End of subscription	22
4.12	Key escrow and recovery	22
4.12.1	Key escrow and recovery policy and practices.....	22
4.12.2	Session key encapsulation and recovery policy and practices	23
5	FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS	24
6	TECHNICAL SECURITY CONTROLS	25
6.1	Key pair generation and installation.....	25
6.1.1	Key pair generation.....	25
6.1.2	Private key delivery to Subscriber	25
6.1.3	Public key delivery to certificate issuer	25
6.1.4	CA public key delivery to relying parties.....	25
6.1.5	Key sizes.....	25
6.1.6	Public key parameters generation and quality checking	25
6.1.7	Key usage purposes (as per X.509 v3 key usage field)	25
6.2	Private key protection and cryptographic module engineering controls	25
6.2.1	Cryptographic module standards and controls	25
6.2.2	Private key (n out of m) multi-person control.....	25

6.2.3	Private key escrow.....	25
6.2.4	Private key backup	25
6.2.5	Private key archival.....	25
6.2.6	Private key transfer into or from a cryptographic module	26
6.2.7	Private key storage on cryptographic module	26
6.2.8	Method of activating private key	26
6.2.9	Method of deactivating private key	26
6.2.10	Method of destroying private key.....	26
6.2.11	Cryptographic module rating.....	26
6.3	Other aspects of key pair management.....	26
6.3.1	Public key archival	26
6.3.2	Certificate operational periods and key pair usage periods	26
6.4	Activation data	26
6.4.1	Activation data generation and installation	26
6.4.2	Activation data protection	26
6.4.3	Other aspects of activation data	26
7	CERTIFICATE, CRL, AND OCSP PROFILES	27
7.1	Certificate profile.....	27
7.1.1	Version number(s)	27
7.1.2	Certificate extensions	28
7.1.3	Algorithm object identifiers.....	28
7.1.4	Name forms	29
7.1.5	Name constraints.....	29
7.1.6	Certificate policy object identifier	29
7.1.7	Usage of Policy Constraints extension	29
7.1.8	Policy qualifiers syntax and semantics	29
7.1.9	Processing semantics for the critical Certificate Policies extension	29
7.2	CRL profile.....	29
7.2.1	Version number(s)	30
7.2.2	CRL and CRL entry extensions	30
7.3	OCSP profile.....	30
7.3.1	Version number(s)	30
7.3.2	OCSP extensions	30
8	COMPLIANCE AUDIT AND OTHER ASSESSMENTS.....	32
8.1	Frequency or circumstances of assessment	32
8.2	Identity/qualifications of assessor	32
8.3	Assessor's relationship to assessed entity	32
8.4	Topics covered by assessment	32
8.5	Actions taken as a result of deficiency.....	32
8.6	Communication of results	32
9	OTHER BUSINESS AND LEGAL MATTERS	33
9.1	Fees.....	33
9.1.1	Certificate issuance or renewal fees.....	33
9.1.2	Certificate access fees.....	33
9.1.3	Revocation or status information access fees	33
9.1.4	Fees for other services	33
9.1.5	Refund policy	33
9.2	Financial responsibility	33
9.3	Confidentiality of business information	33
9.4	Privacy of personal information	33
9.5	Intellectual property rights.....	33
9.6	Representations and warranties	33
9.7	Disclaimers of warranties.....	33
9.8	Limitations of liability.....	34
9.9	Indemnities	34
9.10	Term and termination.....	34
9.10.1	Term.....	34
9.10.2	Termination.....	34

- 9.10.3 Effect of termination and survival..... 34
- 9.11 Individual notices and communications with participants34
- 9.12 Amendments34
 - 9.12.1 Procedure for amendment 34
 - 9.12.2 Notification mechanism and period..... 34
 - See 9.12.1..... 34
 - 9.12.3 Circumstances under which OID must be changed 34
- 9.13 Dispute resolution provisions.....35
- 9.14 Governing law.....35
- 9.15 Compliance with applicable law35
- 9.16 Miscellaneous provisions.....35
- 9.17 Other provisions.....35
- ACRONYMS36**
- DEFINITIONS.....37**

Revision History

<u>Version</u>	<u>Version date</u>	<u>Change</u>	<u>Author</u>
1.0	11 th June 2012	The first official version	TeliaSonera CA Policy Management team
1.01	11 th September 2012	Fixed minor errors in references	TeliaSonera CA Policy Management team
1.02	21 st December 2012	Added OCSP support, In validation a call back to technical contact person is an option, Fixed AIA extension description, Mandatory 2048 bit RSA key length	TeliaSonera CA Policy Management team
1.1	3 rd May 2013	Geographical definition to Server Certificates, Suspension no more used, small technical fixes	TeliaSonera CA Policy Management team
1.2	3rd April 2014	All Subject fields except O and OU will refer to registered O location. Small fixes and clarifications.	TeliaSonera CA Policy Management team
1.3	16 th April 2015	Extended Validation (EV) certificate processes were included, TeliaSonera Server CA v2 added, CA must understand all extensions in 3.2.4, validity max limited to 3y, OCSP specification rewritten, small clarifications in many places, fixed contact details	TeliaSonera CA Policy Management team

1 INTRODUCTION

1.1 Overview

A Certification Practice Statement (CPS) is a Certification Authority's (CA) description of the practices it follows when issuing certificates. The purpose of this CPS is to describe the procedures that the TeliaSonera Server CA v1-2 and TeliaSonera Extended Validation SSL CA v1 use when issuing certificates, and that all Registration Authorities, Subscribers and Relying Parties shall follow in connection with these certificates.

This CPS describes the procedures and routines which apply when registering and completing a certificate and for revoking and revocation checking of certificates. This CPS will refer to separate TeliaSonera Production CPS, which describes the premises, procedures and routines which apply for the Production of TeliaSonera CA Services.

This CPS generally conforms to the IETF PKIX Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework (also known as RFC 3647). This document is divided into nine sections:

- Section 1 - provides an overview of the policy and set of provisions, as well as the types of entities and the appropriate applications for certificates.
- Section 2 - contains any applicable provisions regarding identification of the entity or entities that operate repositories; responsibility of a PKI participant to publish information regarding its practices, certificates, and the current status; frequency of publication; and access control on

published information.

- Section 3 - covers the identification and authentication requirements for certificate related activity.
- Section 4 - deals with certificate life-cycle management and operational requirements including application for a certificate, revocation, suspension, audit, archival and compromise.
- Section 5 - covers facility, management and operational controls (physical and procedural security requirements).
- Section 6 - provides the technical controls with regard to cryptographic key requirements.
- Section 7 - defines requirements for certificate, Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) formats. This includes information on profiles, versions, and extensions used.
- Section 8 - addresses topics covered and methodology used for assessments/audits; frequency of compliance audits or assessments; identity and/or qualifications of the personnel performing the audit or assessment; actions taken as a result of deficiencies found during the assessment; and who is entitled to see results of an assessment.
- Section 9 - covers general business and legal matters: the business issues of fees, liabilities, obligations, legal requirements, governing laws, processes, and confidentiality.

This CPS and all certificates containing the OID value 1.3.6.1.4.1.271.2.3.1.1.15 conform to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [This CPS and all certificates containing the OID value 1.3.6.1.4.1.271.2.3.1.1.17 conform to the current version of the](#) Guidelines For The Issuance And Management Of Extended Validation Certificates. Documents are published at <http://www.cabforum.org>. In the event of any inconsistency between this document and those Documents, those Documents take precedence over this document.

TeliaSonera Server certificates (also called "SSL certificates") provide a mean for relaying parties to identify the legal owner of the server. It also guarantees that the owner named in the Subject owns or manages the domain names used in server names. TeliaSonera Server and Extended Validation certificates are always organization validated (OV) certificates meaning that CA has verified name of the entity that controls the website from official registers.

TeliaSonera Extended Validation ("EV") Certificates are intended to provide enhanced assurance of the identity of the legal entity that controls a website, including the entity's name, address of Place of Business, Jurisdiction of Incorporation or Registration, and Registration Number. EV Certificates may be issued to Private Organizations, Government Entities, International Organization Entities, and Business Entities.

TeliaSonera SSL or EV Certificates do not, however, provide any guarantee that the Subject named in the Certificate is trustworthy, honest or reputable in its business dealings, or safe to do business with. Issued certificates only establish that TeliaSonera CA verified that the business was legally organized, used domain names were owned or managed by the Subject and in EV case also that the Subject really had the used physical address as of the date that the Certificate was issued.

1.2 Document name and identification

This CPS is titled TeliaSonera Server Certificate CPS and the CPS name of this CPS is {TELIASONERA-SERVER-CPS-1}.

This CPS is also a Certificate Policy for TeliaSonera server and EV certificates. The certificates issued according to this CPS contain Certificate policy object identifier corresponding to the applicable certificate type. The routines and roles resulting from this CPS apply only in connection with certificates referring to the following Certificate policy object identifiers:

Certificate type	Issuing CA	Certificate policy object identifier
Standard SSL server certificates	TeliaSonera Server CA v1 TeliaSonera Server CA v2	1.3.6.1.4.1.271.2.3.1.1.15
Extended validation (EV) certificates	TeliaSonera Extended Validation SSL CA v1	1.3.6.1.4.1.271.2.3.1.1.17

“TeliaSonera Server CA v2” was introduced in 2014-11-06 to bring SHA256 algorithm to complement TeliaSonera's SSL certificate offering. Since then the default algorithm in SSL certificates has been SHA256 and older SHA1 has been used only in special circumstances. Otherwise v1 and v2 policies are identical.

This CPS also refers to the TeliaSonera Production CPS with the name {TELIASONERA-PRODUCTION-CPS-2}.

1.3 PKI participants

TeliaSonera server and EV certificates are issued to devices (e.g. web servers) possessed by Customers of TeliaSonera or by TeliaSonera. All of the participating organizations shall undertake what's stated in this Certification Practice Statement.

1.3.1 Certification authorities

The Certification Authority operating in compliance with this Certification Practice Statement is TeliaSonera. The name of the Certification Authority in the “Issuer” field of the certificate is TeliaSonera Server CA v1, TeliaSonera Server CA v2 or TeliaSonera Extended Validation SSL CA v1.

TeliaSonera Server CA v1, TeliaSonera Server CA v2 and TeliaSonera Extended Validation SSL CA v1 are subordinate CAs of TeliaSonera Root CA v1. TeliaSonera Root CA has its own CP and CPS describing the management of the certificate life cycle of subordinate CA certificates signed by it. The title of that CPS is TeliaSonera Root CPS and its CPS name is {TELIASONERA-ROOT-CPS-2}.

The Certification Authorities are responsible for managing the certificate life cycle of end entity certificates signed by the CAs. This will include:

- creating and signing of certificates binding Subjects with their public key
- promulgating certificate status through CRLs and/or OCSP responders

1.3.2 Registration authorities

The CA's units authorized to perform registration functions, Customers acting as Customers of certification services and authorized by CA, or other organizations selected and authorized as RAs, with which the CA makes written agreements, can act as Registration Authorities. Through those agreements, RAs are obliged to follow this CPS for their part.

Typically RA is responsible for the following activities on behalf of a CA:

- identification and authentication of certificate subjects
- initiate or pass along revocation requests for certificates
- approve applications for renewal or re-keying certificates

1.3.3 Subscribers

The Subscriber is the organization or legal entity that makes an agreement with the CA about issuance of a certificate to a Device in its possession (Subject). The Subscriber shall ensure that the Subject fulfils the obligations defined in this CPS and the conditions of the certification services.

The Subject of a certificate is a Device with installed software capable of utilizing the private key stored in the Device.

1.3.4 Relying parties

The Relying Party is a Customer, which utilizes certificates for securing the organization's internal or external activities. The Relying Party can also be a company, organization or a private person having business with the Customer.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Certificates under this CPS are issued to servers or devices to be used for the following applications:

- Subject authentication
- verification of digital data origin and integrity
- confidentiality of digital data

TeliaSonera server certificates can be used, for example, to identify servers and secure SSL/TLS session.

1.4.2 Prohibited certificate uses

Applications using certificates issued under this CPS shall take into account the key usage purpose stated in the “Key Usage” and “Extended Key Usage” extension fields of the certificate.

Additionally, the key usage purposes and limitations possibly stated in the contract between the Subscriber and the CA shall be taken into account when using certificates.

1.5 Policy administration

1.5.1 Organization administering the document

TeliaSonera CA Policy Management Team is the responsible authority for reviewing and approving changes to this CPS. Written and signed comments on proposed changes shall be directed to the listed web form or to TeliaSonera contact as described in Section 1.5.2. Decisions with respect to the proposed changes are at the sole discretion of the TeliaSonera CA Policy Management Team.

Contact information:

http://support.partnergate.sonera.com/support_cps_feedback_en.html

1.5.2 Contact person

Contact person in matters related to this CPS:

TeliaSonera CA Product Manager

Email: cainfo@sonera.com

Phone: +358 (0) 20401

Internet: <https://repository.trust.teliasonera.com/>

Other contact information:

Customer Service: +358 (0) 800 17000

Technical Customer Service: +358 (0) 800 19101

Revocation Service: +358 (0) 800 156677

1.5.3 Person determining CPS suitability for the policy

TeliaSonera CA Policy Management Team is the administrative entity for determining this Certification Practice Statement (CPS) suitability to the applicable policies.

1.5.4 CPS approval procedures

TeliaSonera CA Policy Management Team will review any modifications, additions or deletions from this CPS and determine if modifications, additions or deletions are acceptable and do not jeopardize operations or the security of the production environment.

1.6 Definitions and acronyms

A list of definitions and acronyms can be found at the end of this document.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

2.1.1 CPS Repository

A full text version of this CPS is published at <http://repository.trust.teliasonera.com/>.

2.1.2 Revocation Information Repository

OCSP is the recommended Revocation Information Repository. It can be found from <http://ocsp.trust.teliasonera.com>.

Certificate Revocation Lists (CRLs) are published in the TeliaSonera LDAP directory and on the TeliaSonera website:

Issuing CA	CRL addresses
TeliaSonera Server CA v1	http://crl-3.trust.teliasonera.com/teliasoneraservercav1.crl (ldap://crl-1.trust.teliasonera.com/cn=TeliaSonera%20Server%20CA%20v1,o=TeliaSonera?certificaterevocationlist;binary)
TeliaSonera Server CA v2	http://crl-3.trust.teliasonera.com/teliasoneraservercav2.crl (ldap://crl-1.trust.teliasonera.com/cn=TeliaSonera%20Server%20CA%20v2,o=TeliaSonera?certificaterevocationlist;binary)
TeliaSonera Extended Validation SSL CA v1	http://crl-3.trust.teliasonera.com/teliasoneraextendedvalidationsslcav1.crl (ldap://crl-1.trust.teliasonera.com/cn=TeliaSonera%20Extended%20Validation%20SSL%20CA%20v1,o=TeliaSonera?certificaterevocationlist;binary)

If OCSP is not used then http based CRL repository is recommended. It is listed at first on certificate's CDP extension.

2.1.3 Certificate Repository

All issued certificates are stored in the local database of the CA system. Certificates may also be published to other repositories if it is a part of the TeliaSonera CA Service or agreed with a Customer. EV certificates may be distributed to external directories as required by Certificate Transparency specification at <http://www.certificate-transparency.org/>.

2.2 Publication of certification information

It is TeliaSonera's duty to make the following information available:

- a) This CPS
- b) Certificate revocation lists and revocation status of revoked certificates
- c) Issued CA certificates and cross certificates for cross-certified CAs

TeliaSonera may publish and supply certificate information in accordance with applicable legislation.

Each published certificate revocation list (CRL) provides all processed revocation information at the time of publication for all revoked certificates of which the revocation list is intended to give notification.

TeliaSonera supplies CA certificates for all public CA keys provided these can be used for verifying valid certificates.

Subscribers will be notified that a CA may publish information submitted by them to publicly accessible

directories in association with certificate information. The publication of this information will be within the limits of sections 9.3 and 9.4.

2.3 Time or frequency of publication

Updates to this CPS are published in accordance with the provisions specified in section 9.12.

Revocation information publication provisions are specified in section 4.9.

All issued certificates are stored in the local database of the CA system promptly on issuing. Certificates may also be published to other repositories if it is a part of the TeliaSonera CA Service or agreed with a customer.

2.4 Access controls on repositories

This CPS, CRLs and CA certificates are publicly available. Only authorized CA personnel have access to Subscriber certificates stored in the local database of the CA system.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

An X.501 Distinguished Name (DN) is used as an unambiguous name of the Subject in the "Subject" field of the certificate. The name always includes the following attributes:

	Description – Server	Description – EV SSL
commonName (CN, OID 2.5.4.3)	A single host domain name (FQDN) or IP address which is owned or controlled by the Subject and to be associated with the Subject's server. Such server MAY be owned and operated by the Subject or another entity (e.g., a hosting service). The CN value is always one of the values contained in the Certificate's subjectAltName extension.	A single host domain name (FQDN) which is owned or controlled by the Subject and to be associated with the Subject's server. Such server MAY be owned and operated by the Subject or another entity (e.g., a hosting service). Wildcard certificates are not allowed. The CN value is always one of the values contained in the Certificate's subjectAltName extension.
OrganizationName (O, OID 2.5.4.10)	Customer in relation to which the Subject is identified. Common variations or abbreviations may also be used provided that the name owner is unambiguous.	Subject's full legal organization name as listed in the official records of the Incorporating or Registration Agency. Common abbreviations may be used in prefix or suffix parts.
Locality (L, OID: 2.5.4.7)	City name. A component of the address of the physical location of the Subject's Place of Business.	City name. A component of the address of the physical location of the Subject's Place of Business.
Country (ST, OID: 2.5.4.6)	Two character country code. A component of the address of the physical location of the Subject's Place of Business.	Two character country code. A component of the address of the physical location of the Subject's Place of Business.
subjectAltName:dNSName	One or more host domain names (FQDN) which are owned or controlled by the Subject and to be associated with the Subject's server. Such server MAY be owned and operated by the Subject or another entity (e.g., a hosting service). Wildcard names are allowed.	One or more host domain names (FQDN) which are owned or controlled by the Subject and to be associated with the Subject's server. Such server MAY be owned and operated by the Subject or another entity (e.g., a hosting service). Wildcard names are not allowed.
subjectAltName:iPAddress	One or more IP addresses which are owned or controlled by the Subject and to be associated with the Subject's server. Such server MAY be owned and operated by the Subject or another entity (e.g., a hosting service).	Not allowed
jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)	N/A. May be used like in EV.	Two character country code of the country in which the subject is registered
businessCategory (OID: 2.5.4.15)	N/A. May be used like in EV.	One of the following strings: "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity" depending how the Subject qualifies in CA validation.
serialNumber (OID: 2.5.4.5)	May be used like in EV. Optional in normal SSL certificates.	Registration Number (e.g. Business ID or organization number) assigned to the Subject by the Incorporating or Registration Agency.

Additionally, the "Subject" field may include following attributes depending on the usage purpose of the certificate:

	Description – Server	Description – EV SSL
organizationalUnit Name (OU,OID:2.5.4.11)	Organizational unit defined by the Subscriber. This attribute may also be a DBA, tradename, trademark, address, location, or other text that refers to the specific Legal Entity in the field OrganizationName.	Organizational unit defined by the Subscriber. This attribute may also be a DBA, tradename, trademark, address, location, or other text that refers to the specific Legal Entity in the field OrganizationName.
streetAddress (OID: 2.5.4.9)	Optional. Street address. A component of the address of the physical location of the Subject's Place of Business.	Optional. Street address. A component of the address of the physical location of the Subject's Place of Business.
postalCode (OID: 2.5.4.17)	Optional. Postal code. A component of the address of the physical location of the Subject's Place of Business.	Optional. Postal code. A component of the address of the physical location of the Subject's Place of Business.
State or province (ST, OID: 2.5.4.8)	Not recommended. A country or province name. A component of the address of the physical location of the Subject's Place of Business.	Not recommended. A country or province name. A component of the address of the physical location of the Subject's Place of Business.

Additional Distinguished Name (DN) or Subject Alternative Name attributes may be used as necessary providing that CA is able to verify that the additional attributes belong to the Subject.

3.1.2 Need for names to be meaningful

Names will be meaningful as stated in the section 3.1.1.

3.1.3 Anonymity or pseudonymity of Subscribers

Names will be meaningful as stated in the section 3.1.1.

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

The Subject name stated in a certificate will be unique for all certificates issued within the domain of the CA, and conform to X.500 standards for name uniqueness. Subject name uniqueness means that the CA will not issue certificates with identical names to different organizations. However, the CA may issue several certificates to the same organization, and in that case the Subject names in those certificates may be the same.

3.1.6 Recognition, authentication, and role of trademarks

The priority to entity names is given to registered trademark holders.

TeliaSonera reserves the right not to issue such a certificate, or to revoke a certificate that has already been issued, when there is a name claim dispute involved concerning the certificate contents.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The CA verifies the possession of the private key by verifying the electronic signature included in the PKCS #10 certificate request. The request is accepted only when signed with the private key associated with the public key to be certified.

3.2.2 Authentication of organization identity

TeliaSonera CA or its authorized resellers do the authentication and verification of the certificate request data as described in this chapter. The data for verification is given to the CA either in hand-signed SSL certificate service agreement (Full SSL agreement) or in web order form of SSL or EV certificate. Data may be given to CA in the PKCS#10 certificate signing request or separately on the order form so that the latter will override the former if both exist.

TeliaSonera CA verifies the organization name (O) of a new Customer by checking the existence of the company, its legal name, business identity code and other relevant organization information from an official business register maintained by an applicable government agency (e.g. "ytj.fi" in Finland). The list of applicable trusted registries are maintained in CA internal instructions. . Subject's registration number and address components (street, postalcode, locality, stateOrProvince, country) are typically verified using the same register. In EV validation the verified registration number is added to the serialNumber attribute of a certificate. The address components may be added to the certificate. Mandatory attributes must have a successfully verified value. Metadata such as '-', '.' or 'unknown' are not allowed in these attributes.

TeliaSonera verifies domain names and IP addresses from a trusted database maintained by a reliable third party registrar e.g. "domain.fi" (for domain ".fi"), iis.se (for domain ".se"), ripe.net (for IP addresses) and "www.networksolutions.com/whois-search" (for non-country domains), that as of the date the Certificate was issued, the Applicant either had the right to use, or had control of, the Fully-Qualified Domain Name(s) and IP address(es) listed in the Certificate, or was authorized by a person having such right or control (e.g. under a Principal-Agent or Licensor-Licensee relationship) to obtain a Certificate containing the Fully-Qualified Domain Name(s) and IP address(es). Connection to the third party database is SSL/TLS protected when applicable. In domain verification the domain name ownership is approved if the registered domain/IP owner is a Parent/Subsidiary Company of the Applicant or the ownership is registered to the old name/entity of the same Applicant. In such cases a reliable proof of company structure or name change must be available.

If the Subject Identity Information is to include a name, DBA, trade name or trademark the CA verifies the Applicant's right to use the name from applicable government agency responsible of such names (e.g. "ytj.fi" in Finland).

TeliaSonera may use its previously documented verification data. Old verification data will expire in three years in SSL verification and in thirteen months in EV verification or earlier if the data had an internal expiration date. Old verification data including organization name, address components, Parent/Subsidiary/name change relationships, authorization documents and domain/IP ownership are stored related to organization's registration number. Other subject values are verified each time separately. In FullSSL service such verification can be done by the Customer Registration Officer and TeliaSonera only verifies the Organization names and domain ownerships. In all cases TeliaSonera CA regularly validates that all Registration Officers have done the verification of all subject fields correctly.

Alternatively the Registration Officer may use another allowed authentication or verification methods listed in the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" (regarding SSL certificates) or "Guidelines For The Issuance And Management Of Extended Validation Certificates (regarding EV certificates) published at <http://www.cabforum.org>. If such special verification method is used, it is always separately approved by a supervising TeliaSonera PKI board.

3.2.3 Authentication of individual identity

The procedures to authenticate the identity of the Subscriber vary between the different TeliaSonera Server Certificate services:

SSL order via public web form	TeliaSonera authenticates the administrative (or technical) contact person defined in the certificate application by calling the contact person via the Customer's PBX number or when there is no switchboard, by making a call to some other number in the organization, which is looked up from a trusted phone directory maintained by a third party.
--------------------------------------	--

<p>EV certificate order via public web form</p>	<p>CA requires that administrative contact person (Contract signer) makes a web Subscriber contract with CA. Contract is verified by calling to him/her like above in SSL order authentication. His/her identity and authority on behalf of the Applicant to do contracts is verified. After the initial authentication he/she will get an order confirmation email message from each EV order. Each confirmation message can be used to cancel the contract or authorization.</p> <p>In the EV contract at least one technical contact person representing the Applicant is authorized by Contract Signer to order EV certificates. In EV terms he/she is the Certificate Requester and the Certificate Approver. Authorization is given to the email address that will get the approved EV certificates. Each EV order is authenticated by CA by making a call to technical contact like above in the SSL order authentication.</p>
<p>Internal TeliaSonera SSL or EV certificates or when CA has direct access to Applicant employee register</p>	<p>When employee register is available CA verifies that both technical and administrative contact persons are using normal Applicant company email addresses AND both persons are active employees in the Company according to the employee register. Normal web application authentication described above must be used instead of this if the requirements are not completely fulfilled.</p>
<p>SSL order using TeliaSonera's self service software</p>	<p>The Customer can make an agreement with TeliaSonera to act as a Registration Officer within the Customer Organization (Full SSL Service) and to register TeliaSonera Server certificates using TeliaSonera's RA system for Customers. The Customer Registration Officer is restricted to register certificates only within their own Organizations (O) and the domain names and other values authorized by the CA. Before enabling the service or adding new authorized Organization or domain names, the CA verifies the organization identity and the domain names as described in the section 3.2.2.</p> <p>When registering Subjects, the identity of the Registration Officer is verified by means of the Registration Officers' certificate issued by a TeliaSonera CA.</p>

3.2.4 Non-verified Subscriber information

The Registration Officer is obliged to always review all subject information and initiate additional checking routines if there are any unclear Subject values. Only well-known certificate extensions are verified and others are accepted only if CA is aware of the reason for including the extension.

Domain name ownership of domains in email addresses is not verified by TeliaSonera except when Applicant's employee register is used for authority verification.

The value in OrganizationalUnit field is not verified unless it includes a name, DBA, tradename, trademark, address, location, or other text that refers to a specific Legal Entity. If such value is used TeliaSonera verifies that the Applicant has a right to use it according to a reliable data source.

3.2.5 Validation of authority

<p>SSL order via public web form</p>	<p>TeliaSonera verifies that the administrative contact person defined in the certificate application is employed by the Customer by calling the contact person via the Customer's PBX number or when there is no switchboard, by making a call to some other number in the organization, which is looked up from a directory maintained by a third party.</p>
---	--

EV order via public web form	TeliaSonera verifies that the administrative contact person (Contract Signer) has the authority to do contracts on behalf of the Customer. He/she must be an employee of the Applicant and have an applicable manager or director title or similar role according to certificate application. This title or role is verified via the Company switchboard or via other data source available excluding the person him/herself.
SSL order using TeliaSonera's self-service software	The Administrative Contact Person, who grants the necessary initial authorizations in the Customer, has been identified in the service agreement or order. TeliaSonera verifies that the Organization has authorized the certificate service by contacting the contact person specified in the agreement by phone, mail or other similar methods. A Registration Officer in a Customer has the right to define new Registration Officers. Authorization is based on multi-factor authentication to TeliaSonera's self-service software (typically certificate and PIN code).

3.2.6 Criteria for interoperation

Not applicable.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

No special routine exists for renewal of TeliaSonera Server certificates. In Subject registration the same process will be followed as in the initial registration. The previous verification data may be utilized by CA if it is not expired.

3.3.2 Identification and authentication for re-key after revocation

After revocation of a Subject's certificate, if the Subscriber wants to have a new certificate, then the same process will be followed as in the initial registration. The previous verification data may be utilized by CA if it is not expired.

3.4 Identification and authentication for revocation request

Revocation by Customer

In cases where a Customer can issue SSL certificates using TeliaSonera's self-service software, the Subscriber shall submit a request for certificate revocation to the Registration Officer of its own organization, who has additionally the rights of a Revocation Officer. The Revocation Officer in the Customer is responsible for the verification of the authenticity of the request to revoke the certificate. The identity of the Revocation Officer in the Customer is verified based on a certificate.

Revocation by the Revocation Service of the CA

The Subscriber or Registration Officer in a Customer shall submit a request for certificate revocation to the Revocation Service by telephone or by e-mail. The revocation service checks that the origin of the request is the Customer who owns the certificate using message details. The Revocation Service may make a call back to the Customer and ask certain detailed data. This data is compared with the information recorded about the Subject or Subscriber at registration, and if necessary, with information in the agreements made with the Subscriber or with the Customer. If the data match the certificate will be revoked.

In certain situations where there is an identified risk of abuse of the private key or when it is obvious that the authorized use of the key is prevented, it may be necessary to revoke the certificate on request of someone else but the above mentioned entities. In that case the verification of the authenticity of the revocation request can require other authentication methods. In cases where reliable verification cannot be immediately performed the CA may revoke the certificate to reduce risks.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

SSL or EV order via public web form	Manually processed Certificate application can be submitted by a representative of the Organization, which possesses the Device to which the certificate is applied. If the application is submitted by a different organization from the organization that owns the domain name or the IP address (e.g. by an IT service provider), the application must be authorized by the organization owning the domain name or IP address.
SSL order using TeliaSonera's self-service software	Automatically processed Certificate application can be submitted by an authorized Registration Officer in a Customer that has made a SSL Service agreement with TeliaSonera. Authorized TeliaSonera personnel can also submit these applications for devices of TeliaSonera.

TeliaSonera will issue server certificates only to organizations that are registered in the European Economic Area. The European Economic Area (EEA) comprises the countries of the European Union (EU), plus Iceland, Liechtenstein and Norway.

TeliaSonera may refuse to issue certificates to organizations registered in countries where TeliaSonera cannot reliably validate information on the certificate application.

4.1.2 Enrollment process and responsibilities

SSL or EV order via public web form	<p>A certificate to a Device (an EV or SSL server certificate) is applied by filling in a form that is publicly available at TeliaSonera's web site. A Certificate Signing Request (CSR) that is a standard format certificate request generated by the Device shall be attached to the form. The completed application forms are directed to TeliaSonera's RA office where the sufficiency of the application is checked.</p> <p>Before the application can be submitted, the Subscriber has to accept the Subscriber responsibilities and terms and conditions of the service.</p>
SSL order using TeliaSonera's self-service software	<p>A Registration Officer in a Customer applies for certificates to Devices (SSL server certificates) directly from the CA system by using the self-service application provided by TeliaSonera. The application will print all relevant certificate request values on screen for final review. If accepted by the Registration Officer and the CA configuration the request is processed automatically. It may contain only pre-defined Domain Name and Organization Name values allowed to this Customer.</p> <p>Only TeliaSonera Registration Officers may add new allowed Domain Name or Organization Name values for Customers. New values are always verified according to 3.2.</p> <p>The Customer is bound through a SSL Service Agreement with TeliaSonera. Customer's Registration Officers also accept Customer Responsibilities when they logon to TeliaSonera's self-service application for the first time.</p>

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

TeliaSonera performs identification and authentication of Subject and Subscriber information in accordance with the section 3.2.

4.2.2 Approval or rejection of certificate applications

TeliaSonera will approve a certificate application if it meets the requirements documented in this CPS and there are no other reasons to reject the application. All other certificate applications will be rejected.

The Subscriber will be informed on why the certificate application was rejected and on how to proceed to be approved.

4.2.3 Time to process certificate applications

SSL or EV order via public web form	TeliaSonera process the applications within reasonable time frame.
SSL order using TeliaSonera's self service software	The certificate request is processed automatically by TeliaSonera's RA and CA systems immediately after the request is submitted.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

If the certificate application is approved, the CA issues the certificate. The CA system accepts only such certificate requests the origin of which can be authenticated. The certificate is created by the CA according to the information contained in the certificate request and configured for the Customer. However, the CA may overwrite or delete some certificate information using pre-defined certificate profile specific standard values.

4.3.2 Notification to Subscriber by the CA of issuance of certificate

SSL or EV order via public web form	Subscriber is informed of the acceptance or rejection of the certificate request. TeliaSonera's RA office delivers a web link to the contact person for fetching of the certificate.
SSL order using TeliaSonera's self-service software	The certificate is available for the Customer's Registration Officer in the RA tool after the issuance.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The Subscriber is considered to have accepted the certificate when the private key associated with it has been used, or when the certificate has been installed into a Device.

4.4.2 Publication of the certificate by the CA

TeliaSonera will not publish Subscriber certificates to a publicly available repository if not agreed upon with the Customer. EV certificates may be distributed to external directories as required by Certificate Transparency specification at <http://www.certificate-transparency.org/>.

4.4.3 Notification of certificate issuance by the CA to other entities

EV certificates may be distributed to external directories as required by Certificate Transparency specification at <http://www.certificate-transparency.org/>.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The Subscriber shall only use certificates and their associated key pairs for the purposes identified in this CPS and in applicable agreements with TeliaSonera. Issued certificates contain information which

defines suitable areas of application for the certificate and its associated keys. Area of application labelling takes place in accordance with X.509 and chapter 7 of this CPS. For more information regarding appropriate Subscriber key usage see sections 1.4.1 and 6.1.7.

The Subscriber shall protect the Subject private key from unauthorized use and discontinue the use of the Subject private key immediately and permanently in case the private key is compromised.

4.5.2 Relying party public key and certificate usage

Prior to accepting a TeliaSonera Server certificate, a relying party is responsible to:

- a) Verify that the certificate is appropriate for the intended use;
- b) Check the validity of the certificate, i.e. verify the validity dates and the validity of the certificate and issuance signatures; and
- c) Verify from a valid Certificate Revocation List (CRL) or other certificate status service provided by the CA that the certificate has not been revoked or suspended. If certificate status cannot be verified due to system failure or similar, the certificates shall not be accepted.

4.6 Certificate renewal

Certificate renewal is the re-issuance of a certificate with a new validity date using the same public key corresponding to the same private key.

4.6.1 Circumstance for certificate renewal

When the validity time of a certificate is about to end, the certificate can be renewed.

4.6.2 Who may request renewal

Renewal may be requested by the same persons as the initial certificate application as described in section 4.1.1.

4.6.3 Processing certificate renewal requests

SSL or EV order via public web form	Certificate renewal requests are processed like the initial certificate requests as described in section 4.2. CA may use the stored data of previous validations if available and such data is not expired.
SSL order using TeliaSonera's self-service software	<p>Registration Officer has an option to renew certificates using the tool provided by the CA, in which case the tool uses the old CSR file to renew the certificate.</p> <p>Registration Officer is responsible to ensure that the certificate information is still valid and that there are no other obstacles to the renewal.</p> <p>Certificate renewal and re-key requests may also be processed like the initial certificate requests as described in section 4.2.</p>

4.6.4 Notification of new certificate issuance to Subscriber

The Subscriber is notified as described in section 4.3.2

4.6.5 Conduct constituting acceptance of a renewal certificate

Conduct constituting acceptance of a renewal certificate is described in section 4.4.1.

4.6.6 Publication of the renewal certificate by the CA

Renewed certificates are published like initial certificates as described in section 4.4.2.

4.6.7 Notification of certificate issuance by the CA to other entities

EV certificates may be distributed to external directories as required by Certificate Transparency specification at <http://www.certificate-transparency.org/>.

4.7 Certificate re-key

Certificate re-key is the re-issuance of a certificate using new public and private keys.

The key pairs are generated by the Subscriber and the CA does not check if the certificate renewal request is made using the existing or a new key pair. However, TeliaSonera recommends that the Subscriber creates new key pair when renewing the certificate

Certificate re-key requests are processed as initial certificate requests as described in sections 4.1 – 4.4.

4.8 Certificate modification

Certificate modification is the re-issuance of the certificate due to changes in the certificate information other than the validity time (certificate renewal) or Subscriber's public key (certificate re-key).

Certificate modification requests are processed as initial certificate requests as described in sections 4.1 – 4.4.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

A certificate must be revoked under the following conditions:

1. Upon suspected or known compromise of the private key;
2. Upon suspected or known compromise of the media holding the private key;
3. Subject or subscriber information is known to be invalid or re-verification fails.
4. When there is an essential error in the certificate

A certificate may be revoked under the following conditions:

1. When any information in the certificate changes;
2. Upon termination of a Subject;
3. When a Subject no longer needs access to secured organizational resources;
4. When the certificate is redundant (for example, a duplicate certificate has been issued).
5. Customer's certificate contract with TeliaSonera has ended.
6. Any other reason that makes the certificate obsolete or threats related keys

TeliaSonera in its discretion may revoke a certificate under any circumstances, for example when an entity fails to comply with obligations set out in this CPS, any applicable agreement or applicable law. TeliaSonera will revoke a certificate at any time if TeliaSonera suspects that conditions may lead to a compromise of a Subscriber's keys or certificates.

4.9.2 Who can request revocation

The revocation of a certificate can be requested by:

1. A Subscriber or Registration Officer in the Customer that has made an application for a certificate on behalf of an organization, device or application; or
2. Personnel of TeliaSonera.
3. Owner of the server or device that possesses the certificate

4.9.3 Procedure for revocation request

Subscriber or Applicant may contact TeliaSonera Revocation Service by telephone or email and make a revocation request (look 1.5.2). Authorized TeliaSonera revocation staff then authenticates the identity of the originator of a revocation request according to section 3.4 and processes the revocation request using TeliaSonera's revocation system.

In case of SSL Service where the Customer can issue SSL certificates using TeliaSonera's self-service software, the Registration Officer in the Customer may also make the revocation using the self-service software.

When making a revocation request as above, TeliaSonera's system checks that the person making revocation request is authorized to do so and after that the certificate in question is revoked.

4.9.4 Revocation request grace period

The CA is available for revocation requests 24 hours per day, 7 days per week.

When a reason for the revocation of a certificate appears, the Subscriber shall immediately inform the Revocation Service. In case of SSL Service where the Customer can issue SSL certificates using TeliaSonera's self-service software, the Registration Officer shall revoke the certificate using the self-service software or inform TeliaSonera's Revocation Service immediately, when a reason for the revocation of a certificate comes to his notice.

The CA shall not be responsible for the damage caused by illicit use of the Subject's private key. The CA shall be responsible for the publication of the revocation information on the Certificate Revocation List according to the principles given in this CPS.

4.9.5 Time within which CA must process the revocation request

TeliaSonera processes revocation requests within reasonable time frame. There are no specific requirements for the processing time unless otherwise agreed with the Customer.

4.9.6 Revocation checking requirement for relying parties

Prior to using a certificate, it is the Relying Party's responsibility to check the status of all certificates in the certificate validation chain. A certificate cannot be reasonably relied on if the Relying Party does not diligently follow the certificate status checking procedures denoted below:

- A Relying Party shall ensure the authenticity and integrity of the CRLs or OCSP responses by checking the digital signature and the certification path related to it.
- The Relying Party shall also check the validity period of the CRL or OCSP response in order to make sure that the information is up-to-date.
- Certificates may be stored locally in the Relying Party's system, but the prevailing revocation status of each of those certificates shall be checked before use.
- If valid certificate status information cannot be obtained because of a system or service failure, not a single certificate must be trusted. The acceptance of a certificate in violation of this condition befalls at the Relying Party's own risk.

The Relying Party may acquire the checking of the CRLs as a service that shall follow the certificate status checking procedures denoted above.

4.9.7 CRL issuance frequency

The Revocation Status Service is implemented by publishing Certificate Revocation Lists (CRLs), electronically signed by the CA, in a public directory. The rules below are followed:

- A new CRL is published in the directory at intervals of **not more than 2 hours**.
- The validity time of a CRL is **forty-eight (48) hours**.

There may be several valid CRLs available at the same time. The one of those, which has been published as the latest, contains the most real time information.

4.9.8 Maximum latency for CRLs

CRLs are published to the TeliaSonera LDAP directory and updated automatically. Normally latency will be a matter of seconds.

4.9.9 On-line revocation/status checking availability

TeliaSonera is providing on-line revocation status checking via the OCSP protocol. The OCSP service address is added to certificate extension as defined by RFC2560.

4.9.10 On-line revocation checking requirements

In general all OCSP requests will be signed.

All responses will be signed by a private key corresponding to a public key certified by the CA on which the OCSP request is made.

The OCSP service is using real-time CA database information. The OCSP responder may use the previous status value for a certificate if it is fresher than two hours old (refresh time). In rare circumstances where the connection between OCSP and CA is broken the status information may be up to 48 hours old (grace period). OCSP responder will respond with an "unknown" status for certificates that do not exist in the CA database.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements regarding key compromise

No stipulation.

4.9.13 Circumstances for suspension

Suspension is not used after March 2013.

4.9.14 Who can request suspension

Suspension is not used after March 2013.

4.9.15 Procedure for suspension request

Suspension is not used after March 2013.

4.9.16 Limits on suspension period

Suspension is not used after March 2013.

4.10 Certificate status services

4.10.1 Operational characteristics

The primary method for status checking is OCSP Service. The CRLs are published in the TeliaSonera's LDAP directory and website as disclosed in chapter 2.1.2.

4.10.2 Service availability

The certificate status services are available 24 hours per day, 7 days per week.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

The end of a subscription as a result of no longer requiring the service, compromise, or termination of service (voluntary or imposed) may result in the immediate revocation of the certificate and the publishing of a CRL or other certificate status verification system.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

A Subscriber's digital signature private keys will not be escrowed.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

All stipulations regarding chapter **5 Facility Management, and Operational Control** are specified in "TeliaSonera Production CPS".

6 TECHNICAL SECURITY CONTROLS

All general stipulations regarding chapter 6 **Technical Security Controls** are specified in "TeliaSonera Production CPS".

The sections below are additions to the texts in the corresponding sections of the "TeliaSonera Production CPS" to complement and specify information concerning Subscriber key management.

6.1 *Key pair generation and installation*

6.1.1 **Key pair generation**

The Subscriber generates the key pair using server software or hardware security module. Third party key generation systems (e.g OpenSSL) can be used if the server itself isn't supporting key generation.

6.1.2 **Private key delivery to Subscriber**

Not applicable.

6.1.3 **Public key delivery to certificate issuer**

The public key is delivered digitally signed in a Certificate Signing Request (CSR) file and using an encrypted connection.

6.1.4 **CA public key delivery to relying parties**

Methods to deliver CA certificates to Subscribers and Relying Parties are described in TeliaSonera Production CPS.

6.1.5 **Key sizes**

The CA requires that the Subscribers generate at least 2048 bit RSA keys.

6.1.6 **Public key parameters generation and quality checking**

TeliaSonera may refuse to accept certificate request if it is containing a known weak RSA key.

6.1.7 **Key usage purposes (as per X.509 v3 key usage field)**

Issued certificates contain information which defines suitable areas of application for the certificate and its associated keys. The CA is not responsible for use other than the given key usage purposes. Area of application labeling takes place in accordance with X.509 and chapter 7.

6.2 *Private key protection and cryptographic module engineering controls*

6.2.1 **Cryptographic module standards and controls**

The Subscriber private keys are generated by the Subscribers and normally the private keys are stored in the software of a server.

6.2.2 **Private key (n out of m) multi-person control**

No stipulation.

6.2.3 **Private key escrow**

TeliaSonera does not escrow Subscriber private keys.

6.2.4 **Private key backup**

No backups are made of the Subscribers private keys by TeliaSonera.

6.2.5 **Private key archival**

TeliaSonera does not archive Subscriber private keys.

6.2.6 Private key transfer into or from a cryptographic module

No stipulation.

6.2.7 Private key storage on cryptographic module

No stipulation.

6.2.8 Method of activating private key

The Subscriber is responsible for the private key activation. The CA recommends that the Subscriber uses passwords or strong authentication methods to authenticate users to the server or other device before the private key is activated in accordance with section 6.4 and takes other appropriate measures for the logical and physical protection of the server or other device used to store private keys.

6.2.9 Method of deactivating private key

No stipulation.

6.2.10 Method of destroying private key

When the certificate has expired and has not been renewed, the private key related to it cannot be used any more in connection with certification services. The key is not returned to the CA to be destroyed but it remains in the possession of the Subscriber and should be destroyed by the Subscriber.

6.2.11 Cryptographic module rating

Subscriber is responsible for generation and protection of Subscriber private key.

6.3 Other aspects of key pair management

6.3.1 Public key archival

The CA stores the Subject public keys according to section 5.5 in the TeliaSonera Production CPS.

6.3.2 Certificate operational periods and key pair usage periods

The usage period of the Subscriber certificate shall not be longer than 3 years.

The same keys may be certified again on expiration of a certificate, although it is not recommended by the CA. The usage period of the Subject public and private keys shall not exceed the period during which the applied cryptographic algorithms and their pertinent parameters remain cryptographically strong enough or otherwise suitable.

6.4 Activation data

The Subscriber uses his private keys with the help of activation data.

6.4.1 Activation data generation and installation

The Subscriber is responsible for activation data generation and installation. The Subscriber is recommended to use passwords or strong authentication methods to authenticate users to servers or other devices before the private key is activated. If passwords are used, the CA recommends that Subscriber uses passwords that consists of sufficiently many characters and cannot be easily guessed or concluded.

6.4.2 Activation data protection

The Subscriber is recommended to keep his activation data appropriately protected from unauthorized access.

6.4.3 Other aspects of activation data

No stipulation.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

The contents definition of a certificate, in other words the certificate profile, defines the fields in a certificate. The certificate profile of the certificates follows the version 3 profile defined in the ITU X.509 standard. The profile of the certificates also follows the document RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

The basic fields used in certificates are listed in the table below:

Field name	Field description and contents
Version	This field states which of the certificate versions defined in the X.509 standard the certificate conforms to. The issued certificates conform to the version 3.
Serial number	The CA generates an individual serial number for every certificate. The number that has been given in this field is unique for every certificate created by the CA system. The software manages the uniqueness of the serial number automatically.
Signature algorithm	The signature algorithm is the set of mathematical rules according to which the CA software executes the signing of the certificate. Identifiers have been allocated for the algorithms that are generally used. The identifier of the algorithm used for the signing of the certificate is given in this field. The signature cannot be verified if the algorithm used is not known. The algorithm that is used for the signing of the certificates is sha1RSA or sha256RSA.
Issuer	This field states the name of the Issuer of the certificate. The Issuer name in the certificates of each CA has been described in section 1.3.1.
Validity	The validity of the certificate is that period of time during which the CA guarantees that it maintains status information of the certificate, in other words about the possible revocation of the certificate. This field states the date and time when the certificate comes into force, and the date and time after which the certificate is no more valid. The certificate can be trusted during its validity period if the certificate has not been published on the CRL.
Subject	This field identifies the Server or Device under whose possession the private key is, that corresponds to the public key contained in the certificate. The field includes the unambiguous name of the Subject. The contents of the field have been described in section 3.1.
Subject public key info	This field states the algorithm under which the public key of the Subject shall be used. The Subject's public key itself is also given in this field. The algorithms and key lengths of the Subject keys are described in section 6.1.5.

7.1.1 Version number(s)

All issued certificates are X.509 Version 3 certificates, in accordance with the PKIX Certificate and CRL Profile.

7.1.2 Certificate extensions

Certificate extensions will be supported in accordance with RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". In general, following extension may be used in a Subscriber certificate:

Extension	Authority	Extension description and contents
Authority key identifier	CA	The identifier of the issuing CA public key is given in this extension. The identifier can be used to identify the public key that corresponds to the private key used for the signing of the certificate. SHA-1 hash algorithm is used to calculate the identifier.
Subject key Identifier	CA	The identifier of the Subject public key that is contained in the certificate is given in this extension. The identifier can be used to pick up those certificates that contain a given public key. SHA-1 hash algorithm is used to calculate the identifier.
Certificate policies	CA	This extension states the policies according to which the certificate has been issued. The relevant policy is identified based on an individual identifier (object identifier, OID) assigned to the policy document or certain certificate type. The identifiers covered by this CPS have been given in section 1.2.
CRL distribution points	CA	This extension gives the location where the CRL is available. The exact addresses of the CRLs corresponding to the different certificate classes are given in section 4.10.1.
Key usage	CA	The key usage purposes of the public key contained in the certificate are given in this extension. The CA is not responsible for use other than the given key usage purposes. The key usage extension is optional for TeliaSonera server certificates. Purposes KeyCertSign and cRLSign are never set.
Extended key usage	CA	This extension contains other key usage purposes of the public key except those contained in the "Key usage" extension. A key usage purpose given in this extension may be generally known or privately defined for a certain application. The extended key usage purposes of the public keys contained in the Subscriber certificates may include: <ul style="list-style-type: none"> a) Server authentication b) Server authentication and Client authentication
Subject alternative name	Subscriber	This extension should be used to relate identification information to the Subject. Subject alternative name information used in the Certificates is described in section 3.1.1.
Authority Info Access	CA	This extension may contain two values: <ul style="list-style-type: none"> a) The url to CA-certificate b) OCSP service address as defined by RFC2560 Typically all server certificates include both listed values.

Also some other extensions may be used if agreed with TeliaSonera or added to CSR and CA is aware of a reason for including the data in the certificate

7.1.3 Algorithm object identifiers

At least the following algorithms are supported for signing and verification:

```
sha1withRSAEncryption OBJECT IDENTIFIER ::= iso(1) member-body(2) us(840) rsadsi(113549)
pkcs(1) pkcs-1(1) 5; {1.2.840.113549.1.1.5}.
```

```
sha256withRSAEncryption OBJECT IDENTIFIER ::= iso(1) member-body(2) us(840) rsadsi(113549)
pkcs(1) pkcs-1(1) 11; {1.2.840.113549.1.1.11}
```

7.1.4 Name forms

Every DN will be in the form of an X.501 DirectoryString in accordance with section 3.1.1.

7.1.5 Name constraints

Subject and Issuer DNs comply with PKIX standards and are present in all certificates.

7.1.6 Certificate policy object identifier

The certificate policy object identifier will be present in issued certificates and will contain the OID of the policy according to which the certificate has been issued. The identifiers covered by this CPS have been given in section 1.2.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

The policy qualifier CPSuri may be used in the Subscriber certificates. The value of the CPSuri points to TeliaSonera CA Services repository website where this CPS is published.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL profile

The information contained in a Certificate Revocation List has been described below. The CRL is used to state which of the certificates, whose validity period has not yet expired have been revoked.

CRL basic fields are listed in the table below:

Field name	Field description and contents
Version	This field states which of the CRL versions defined in the X.509 standard the CRL conforms to. The CRLs conform to the version 2.
Signature algorithm	The CRLs are signed by using the same algorithm as is used for signing of the certificates. The algorithm used is sha1RSA or sha256RSA.
Issuer	This field states the name of the Issuer of the CRL. The CRL issuer name is always the same as the Issuer name (the CA's name) in the certificates listed on the CRL.
This update	Date and time of the CRL issuance.
Next update	Date and time by which the next CRL shall be issued. The next CRL may be issued at any time after the issuing of the previous CRL, however, it shall be issued before the time stated in the "Next update" field. The time difference between "This update" and "Next update" is defined in section 4.9.7.

Revoked certificates	This field states the serial numbers of revoked certificates, and for each revoked certificate the date and time of revocation and the reason for revocation.
----------------------	---

In general, following CRL extension may be used:

Extension	Extension description and contents
Authority key identifier	The identifier of the public key of the CRL Issuer is given in this field. The identifier can be used to identify the public key that corresponds to the private key used for the signing of the CRL. Within TeliaSonera PKI the SHA-1 hash algorithm is used to calculate the identifier.
CRL number	The CRL number is a number that indicates the position of the CRL in the sequence of issued CRLs. The numbering starts with 1, and it increases monotonically by one for each issued CRL. Based on the CRL number the user is able to determine if a certain CRL replaces another CRL.

7.2.1 Version number(s)

All issued CRL's are X.509 version 2 CRL's in accordance with the RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

7.2.2 CRL and CRL entry extensions

CRL extensions will be supported in accordance with RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

In general, the following entry extensions may be included in a CRL:

Extension	Extension description and contents
Reason Code of the CRL Entry	The reason for revocation can be one of the following: KeyCompromise, CACompromise, AffiliationChanged, Superseded, CessationOfOperation
Invalidity date	The invalidity date provides the date, on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid. This date may be earlier than the revocation date in the CRL entry, which is the date at which the CA processed the revocation.

7.3 OCSP profile

7.3.1 Version number(s)

TeliaSonera OCSP responders conform to version 1 of RFC 2560.

7.3.2 OCSP extensions

The OCSP Nonce extension should be used in OCSP requests.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 *Frequency or circumstances of assessment*

An annual Compliance Audit will be performed by an independent, qualified third party.

8.2 *Identity/qualifications of assessor*

The Compliance Auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the requirements which a CA service imposes on the issuance and management of certificates.

8.3 *Assessor's relationship to assessed entity*

The Compliance Auditor should not have any financial, legal or organizational relationship with the audited party. A person cannot be Compliance Auditor if he/she:

- a) is owner to or joint owner to TeliaSonera or another company within the same group.
- b) is a member of the TeliaSonera management or the management of any subsidiary, or assists with TeliaSonera's bookkeeping or management of means, or TeliaSonera's control of them, or managing the issues regarding information security.
- c) is employed by or in other aspects in subordinate or dependent relation to TeliaSonera or any other company referred to in a) and b) above,
- d) is married to or cohabiter with or is sibling or close relative to a person that is referred to in a) and b) above, or
- e) is in debt to TeliaSonera or any other company referred to in a) to c) above.

8.4 *Topics covered by assessment*

The purpose of the Compliance Audit is to verify that TeliaSonera and all engaged subcontractors are complying with the requirements of this CPS and TeliaSonera Production CPS. The Compliance Audit will cover all requirements that define the operation of a CA under these CPSes including:

- a. The CA production integrity (key and certificate life cycle management); and
- b. CA environmental controls.

8.5 *Actions taken as a result of deficiency*

Depending on the severity of the deficiency, the following actions may be taken:

- a) The Compliance Auditor may note the deficiency as part of the report;
- b) The Compliance Auditor may meet with TeliaSonera and determine if the deficiency can be remedied and an action plan should be developed and steps taken to remedy the deficiency. Such steps could be to change applied procedures and/or updating the CPS;
- c) The Compliance Auditor may report the deficiency and if the TeliaSonera CA Service deems the deficiency to have risk to the operation of the TeliaSonera or Customers CAs, the TeliaSonera CA Service operator may revoke the CA's certificate.

Should the CPS be updated in such a way that the new CPS is deemed to involve an amended degree of security; a new CPS with a new identity shall be drawn up (see section 1.2).

8.6 *Communication of results*

The Compliance Auditor shall provide the TeliaSonera CA Service management with a copy of the results of the Compliance Audit. The results will not be made public unless required by law.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Fees are defined in server certificate order site or in applicable Customer agreement.

9.1.1 Certificate issuance or renewal fees

See section 9.1.

9.1.2 Certificate access fees

See section 9.1.

9.1.3 Revocation or status information access fees

See section 9.1.

9.1.4 Fees for other services

See section 9.1.

9.1.5 Refund policy

See section 9.1.

9.2 Financial responsibility

All stipulations regarding the section 9.2 Financial responsibility are specified in TeliaSonera Production CPS.

9.3 Confidentiality of business information

All stipulations regarding the section 9.3 Confidentiality of business information are specified in TeliaSonera Production CPS.

9.4 Privacy of personal information

All stipulations regarding the section 9.4 Privacy of personal information are specified in TeliaSonera Production CPS.

9.5 Intellectual property rights

The private signing key is the sole property of the legitimate holder of the corresponding public key identified in a certificate.

No part of this CPS (other than in accordance with the exceptions detailed below) may be reproduced, published in a database system or transmitted in any form (electronic, mechanical, photocopied, recorded or similar) without written permission from TeliaSonera.

However, permission generally applies for reproducing and disseminating this CPS in its entirety provided that this is at no charge and that no information in the document is added to, removed or changed.

Applications to reproduce and disseminate parts of this document in any other way may be made to TeliaSonera in accordance with section 1.5.2.

9.6 Representations and warranties

All stipulations regarding the section 9.6 Representations and warranties are specified in TeliaSonera Production CPS.

9.7 Disclaimers of warranties

All stipulations regarding the section 9.7 Disclaimers of warranties are specified in TeliaSonera Production CPS.

9.8 Limitations of liability

All stipulations regarding the section 9.8 Limitations of liability are specified in TeliaSonera Production CPS.

9.9 Indemnities

All stipulations regarding the section 9.9 Indemnities are specified in TeliaSonera Production CPS.

9.10 Term and termination

9.10.1 Term

This CPS remains in force until notice of the opposite is communicated by TeliaSonera on its web site in the TeliaSonera CA Service Repository (<https://repository.trust.teliasonera.com>).

9.10.2 Termination

Termination of this document will be upon publication of a newer version or replacement document, or upon termination of CA operations.

9.10.3 Effect of termination and survival

The conditions and effect resulting from termination of this document will be communicated, on TeliaSonera's web site in the TeliaSonera CA Service Repository (<https://repository.trust.teliasonera.com>), upon termination outlining the provisions that may survive termination of the document and remain in force.

9.11 Individual notices and communications with participants

TeliaSonera will define in any applicable agreement the appropriate provisions governing notices.

9.12 Amendments

TeliaSonera CA Policy Management Team is the responsible authority for reviewing and approving changes to this CPS. Written and signed comments on proposed changes shall be directed to the TeliaSonera CA Service contact as described in Section 1.5. Decisions with respect to the proposed changes are at the sole discretion of the TeliaSonera CA Policy Management Team.

9.12.1 Procedure for amendment

The only changes which can be carried out to this CPS without notification are linguistic amendments and rearrangements which do not affect the security level of the described procedures and regulations.

Changes which shall take place with notification can be made to this CPS 15 days after notification. The TeliaSonera CA Policy Management Team will post the notification at the CPS publishing point at (<https://repository.trust.teliasonera.com>). Changes affecting the terms of an agreement shall be notified in writing to the address given in the contact information of the signatory of the agreement.

TeliaSonera CA Policy Management Team decides which measures are taken in relation to the comments received. If comments received necessitate changes to the original change proposal which were not covered by the original notification, these changes may come into force no earlier than 15 days after publication of a new modified notification.

9.12.2 Notification mechanism and period

See 9.12.1

9.12.3 Circumstances under which OID must be changed

If TeliaSonera CA Policy Management Team determines that a new Object Identifier (OID) is required, TeliaSonera CA Policy Management Team will assign a new OID and required amendments will be made.

9.13 Dispute resolution provisions

All stipulations regarding the section 9.13 "Dispute resolution provisions" are specified in TeliaSonera Production CPS.

9.14 Governing law

All stipulations regarding the section 9.14 "Governing law" are specified in TeliaSonera Production CPS.

9.15 Compliance with applicable law

All stipulations regarding the section 9.15 "Compliance with applicable law" are specified in TeliaSonera Production CPS.

9.16 Miscellaneous provisions

All stipulations regarding the section 9.16 "Miscellaneous provisions" are specified in TeliaSonera Production CPS.

9.17 Other provisions

All stipulations regarding the section 9.17 "Other provisions" are specified in TeliaSonera Production CPS.

ACRONYMS

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DER	Distinguished Encoding Rules
DN	Distinguished Name
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
EID	Electronic Identification
EV	Extended Validation
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest 5
OCSP	On-line Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509 (IETF Working Group)
RA	Registration Authority
RFC	Request for Comments
RSA	Rivest-Shamir-Adleman asymmetric encryption algorithm
SEIS	Secure Electronic Information in Society
SHA –1	Secure Hash Algorithm
S/MIME	Secure Multipurpose Internet Mail Extension
SSL	Secure Sockets Layer
TTP	Trusted Third Party
UPS	Uninterruptible Power Supply
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

DEFINITIONS

Access control:

The granting or denial of use or entry.

Activation Data:

Activation data, in the context of certificate enrollment, consists of a one-time secret communicated to the enrolling user (Subscriber) out of band. This shared secret permits the user to complete of the enrollment process.

Administrator:

A Trusted Person within the organization of a Processing Center, Service Center, Managed PKI Customer, or Gateway Customer that performs validation and other CA or RA functions.

Administrator Certificate:

A Certificate issued to an Administrator that may only be used to perform CA or RA functions.

Agent:

A person, contractor, service provider, etc. that is providing a service to an organization under contract and are subject to the same corporate policies as if they were an employee of the organization.

Application Server:

An application service that is provided to an organizational or one of its partners and may own a certificate issued under the organizational PKI. Examples are Web SSL servers, VPN servers (IPSec), object signer services, Domain Controllers, etc.

Authentication:

Checking the identity provided, e.g. when logging in, in the event of communication between two systems or when exchanging messages between users. General: strengthening of authenticity.

Authorization:

The granting of permissions of use.

Authorized representative:

An employee of the commissioner who has the authority to order and revoke certificates at the CA.

Asymmetric encryption algorithm:

An encryption technique which uses two related transformation algorithms: a public transformation, with the use of a public key, and a private transformation with the use of a private key. The two transformations are such that if the public transformation is known, it is mathematically impossible to derive the private transformation from this.

Base certificate:

See primary certificate.

Business process:

A set of one or more linked procedures or activities which collectively realize a business objective or policy goal, normally within the context of an organizational structure defining functional roles and relationships.

CA certificate:

Certificate which certifies that a particular public key is the public key for a specific CA.

CA key:

Key pair where the private key is used by the CA in order to sign certificates and where the public key is used to verify the same certificate.

Certificate:

The public key of a user, together with related information, digitally signed with the private key of the Certification Authority that issued it. The certificate format is in accordance with ITU-T Recommendation X.509.

Certificate extensions:

Sections of certificate content defined by standard X.509 version 3.

Certificate level:

Certificates exist at two levels: primary certificates and secondary certificates.

Certification Authority (CA):

An authority trusted by one or more users to manage X.509 certificates and CRLs.

Certification Chain:

An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.

Certificate Policy:

Named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements. It is the principal statement of certificate policy governing the organizational PKI. The CP is a high-level document that describes the requirements, terms and conditions, and policy for issuing, utilizing and managing certificates issued by a CA.

Certification Practice Statement (CPS):

A statement of the practices, which a Certification Authority employs in issuing certificates. It is a comprehensive description of such details as the precise implementation of service offerings and detailed procedures of certificate life-cycle management and will be more detailed than the certificate policies supported by the CA.

Certificate Revocation List (CRL):

A periodically 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. CRL can be used to check the status of certificates.

Confidential:

A security classification used to describe information which if disclosed could result in personal loss or minor financial loss. Personal information and tactical information would be deemed confidential.

Confidentiality:

Information that has an identifiable value associated with it such that if disclosed might cause damage to an entity.

Cross Certification:

The process describing the establishing of trust between two or more CAs. Usually involves the exchange and signing of CA certificates and involves the verification of assurance levels.

Cryptographic Module:

A unit in which encryption keys are stored together with a processor which can carry out critical cryptographic algorithms. Examples of cryptographic modules include EID cards.

Decryption:

The process of changing encrypted (coded) information into decrypted (legible) information. See also encryption.

Distinguished Encoding Rules (DER):

The Distinguished Encoding Rules for ASN.1, abbreviated DER, gives exactly one way to represent any ASN.1 value as an octet string. DER is intended for applications in which a unique octet string encoding is needed, as is the case when a digital signature is computed on an ASN.1 value.

Digital Signature:

The result of the transformation of a message by means of a cryptographic system using keys such that a person who has the initial message can determine that the key that corresponds to the signer's key created the transformation and the message was not altered.

Directory Service:

Database service which in this document relates to a database structure in accordance with standard X.500 or LDAP.

Distinguished Name (DN):

Every entry in a X.500 or LDAP directory has a Distinguished Name, or DN. It is a unique entry identifier through out the complete directory. No two Entries can have the same DN within the same directory. A DN is used in certificates to uniquely identify a certificate-owner.

Dual Control:

A process utilizing two or more separate entities (usually persons), operating in concert, to protect sensitive functions or information, whereby no single entity is able to access or utilize the materials, e.g., cryptographic key.

EID card:

Electronic ID card in the form of an active card containing certificates and keys while the front of the card can be used as a visual ID document.

Electronic identity check:

Identity check which can be carried out without the persons whose identity is being checked being present in person.

Electronic signature:

General signature designation created using IT. Digital equivalent to traditional signature. See also digital signature.

Encryption:

The process of changing information which can be interpreted (clear text) into encrypted information. The aim of the encrypted information is that it shall not be interpretable by anyone who does not hold exactly the right key (in symmetrical encryption) or exactly the right private key (in asymmetrical encryption) required to correctly decrypting the information.

E-mail Certificates:

Certificates utilized for encrypting and verifying digital signatures. Normally two separate certificate: one for encryption, the other for signature verification.

Entity:

Any autonomous element or component within the Public Key Infrastructure that participate is one form or another, such managing certificates or utilizing certificates. An Entity can be a CA, RA, Subscriber, Relying Party, etc.

Extended Validation Certificates (EV certificates)

Extended Validation ("EV") Certificates are intended to provide enhanced assurance of the identity of the legal entity that controls a website, including the entity's name, address of Place of Business, Jurisdiction of Incorporation or Registration, and Registration Number. EV Certificates may be issued to Private Organizations, Government Entities, International Organization Entities, and Business Entities.

FIPS 140-2:

Federal Information Processing Standard 140-2(FIPS 140-2) is a standard that describes US Federal

government requirements that IT products shall meet for Sensitive, but Unclassified (SBU) use. The standard was published by the National Institute of Standards and Technology (NIST), has been adopted by the Canadian government's Communication Security Establishment (CSE), and is likely to be adopted by the financial community through the American National Standards Institute (ANSI). The different levels (1 to 4) within the standard provide different levels of security and in the higher levels, have different documentation requirements.

FIPS 180-1:

Standard specifying a Secure Hash Algorithm, SHA-1, for computing a condensed representation of a message or a data files.

Integrity:

Ensuring consistency of an object or information. Within security systems, integrity is the principle of ensuring that a piece of data has not been modified maliciously or accidentally.

Internal Server Name:

A Server Name (which may or may not include an Unregistered Domain Name) that is not resolvable using the public DNS.

ISO 11568-5:

Basic principles and requirements for Key lifecycle for public key cryptosystems, provides instructions to financial institutions in the development, implementation and/or the operation of systems and procedures throughout Key's lifecycle

Key:

When used in the context of cryptography, it is a secret value, a sequence of characters that is used to encrypt and decrypt data. A key is a unique, generated electronic string of bits used for encrypting, decrypting, e-signing or validating digital signatures.

Key holder:

In this context, a person, an organisation, an organisational unit or a function which has exclusive control of the private key, the public equivalent of which is certified in a certificate. See also Subscriber.

Key Pair:

Often referred to as public/private key pair. One key is used for encrypting and the other key used for decrypting. Although related, the keys are sufficiently different that knowing one does not allow derivation or computation of the other. This means that one key can be made publicly available without reducing security, provided the other key remains private.

Log:

A sequential and unbroken list of events in a system or a process. A typical log contains log entries for individual events, each containing information on the event, who initiated it, when it occurred, what it resulted in, etc.

MD5:

A Message Digest Algorithm.

Non-repudiation:

Protection against the denial of the transaction or service or activity occurrence.

Non-repudiation services:

Service which aim to hold a key holder responsible for signed messages in such a way that they can be verified by a third party at a later point in time.

Object Identifier:

The unique alpha-numeric identifier registered under the ISO registration standard to reference a standard object or class.

Operator:

Employee of a CA.

Out of band process:

Communications which occur outside of a previously established communication method or channel.

PKCS #1:

Standard that provides recommendations for the implementation of public-key cryptography based on the RSA algorithm, covering the following aspects: cryptographic primitives; encryption schemes; signature schemes, etc.

PKCS #7:

A cryptographic message format or syntax managed and edited by RSA Laboratories. A standard describing general syntax for data that may have cryptography applied to it, such as digital signatures and digital envelopes.

PKCS #10:

A certificate request format or syntax managed and edited by RSA Laboratories. It is a standard describing syntax for a request for certification of a public key, a name, and possibly a set of attributes.

PKIX:

The Public Key Infrastructure (X.509) or PKIX is an IETF Working Group established with the intent of developing Internet standards needed to support an X.509-based PKI. The scope of PKIX extends to also develop new standards for use of X.509-based PKIs in the Internet.

PKI personnel:

Persons, generally employees, associated with the operation, administration and management of a CA or RA.

Policy:

The set of laws, rules and practices that regulates how an organization manages its business. Specifically, security policy would be the set of laws, rules and practices that regulates how an organization manages, protects and distributes sensitive information.

Primary certificate:

A certificate which is issued on the basis of identifying key holders other than by the key holder producing another certificate. Identification then normally takes place through the key holder instead producing an identity document.

PrintableString:

String format for representing names, such as Common Name (CN), in X.509 certificates. The encoding of a value in this syntax is the string value itself.

Private Key:

The private key is one of the keys in a public/private key pair. This is the key that is kept secret as opposed to the other key that is publicly available. Private keys are utilized for digitally signing documents, uniquely authenticating an individual, or decrypting data that was encrypted with the corresponding public key.

Public Key Infrastructure:

A set of policies, procedures, technology, audit and control mechanisms used for the purpose of managing certificates and keys.

Public:

A security classification for information that if disclosed would not result in any personal damage or financial loss.

Public Key:

The community verification key for digital signature and the community encryption key for encrypting information to a specific Subscriber.

RA policy:

A named set of rules for the RA's role in producing, issuing and revoking certificates and which regulates the applicability of certificates within a specific area of application.

Registration Authority (RA):

An entity that performs registration services on behalf of a CA. RAs work with a particular CA to vet requests for certificates that will then be issued by the CA.

Re-key:

The process of replacing or updating the key(s). The expiration of the crypto period involves the replacement of the public key in the certificate and therefore the generation of a new certificate.

Relative Distinguished Name (RDN):

A Distinguished Name is made up of a sequence of Relative Distinguished Names, or RDNs. The sequences of RDNs are separated by commas (,) or semi-colons (;). There can be more than one identical RDN in a directory, but they must be in different bases, or branches, of the directory.

Relying Party:

A person or entity that uses a certificate signed by the CA to authenticate a digital signature or encrypt communications to a certificate Subject. The relying party relies on the certificate as a result of the certificate being signed by a CA, which is trusted. A relying party normally is but does not have to be a Subscriber of the PKI.

Repository:

A place or container where objects are stored. A data repository is technology where data is stored logically. In PKI terms, a repository accepts certificates and CRLs from one or more CAs and makes them available to entities that need them for implementing security services.

Revocation:

In PKI, revocation is the action associated with revoking a certificate. Revoking a certificate is to make the certificate invalid before its normal expiration. The Certification Authority that issued the certificate is the entity that revokes a certificate. The revoked status is normally published on a certificate revocation list (CRL).

RSA:

A public key cryptographic algorithm invented by Rivest, Shamir, and Adelman.

Secondary certificate:

A certificate issued on the basis of another certificate, the primary certificate. This means that the issuing CA relies on the CA which issued the primary certificate, i.e. accepts the public key's certification of the key holder, which in turn requires reliance on the identification of the key holder when issuing the primary certificate being correct.

Sensitive:

Used to describe the security classification of information where the information if disclosed would result in serious financial loss, serious loss in confidence or could result in personal harm or death.

Signature Verification Certificate:

Often referred to as simply a Signature Certificate. It is the certificate containing the public key used to verify a digital signature that was signed by the corresponding private key.

Split Knowledge

A condition under which two or more parties separately and confidentially have custody of components of a single key that, individually, convey no knowledge of the resultant cryptographic key. The resultant key exists only within secure cryptographic devices.

SSL Client Certificate:

Certificate utilized to verify the authentication of an end user to a server when a connection is being established via a SSL session (secure channel).

SSL Server Certificate:

Certificate utilized to verify the authentication of a web or application server to the end user (client) when a connection is being established via a SSL session (secure channel).

Storage module:

In this document relates to cryptographic module.

Subject:

Entity identified in a certificate as the holder of the private key associated with the public key given in the certificate. [ETSI TS 101 456 v1.2.1] Subject can also be a device (a data network component or software, hereafter referred to as "Device").

Subscriber:

Entity subscribing with a Certification Authority on behalf of one or more Subjects. The Subject may be a Subscriber acting on its own behalf. [ETSI TS 101 456 v1.2.1]

Surveillance Camera:

A surveillance camera is a video recording device used for detection and identification of unauthorized physical entry to a secured area. A camera used for recording a signing ceremony for auditing purposes is not considered a surveillance camera.

Symmetric encryption:

Encryption system characterized by both the sender and the recipient of encrypted information using the same secret key for both encryption and decryption.

Threat:

A danger to an asset in terms of that asset's confidentiality, integrity, availability or legitimate use.

Token:

Hardware devices, normally associated with a reader, used to store and/or generate encryption keys, such as smartcards and USB tokens.

Trusted Third Party (TTP):

A party on which two or more collaborative parties rely. A TTP carries out services for the collaborative parties, such as time-stamping, certificate issuing, etc.

Trusting party:

A recipient of a certificate which trusts this certificate on authentication, verification of digital signatures and/or encryption of information. See also Relying Party.

Unambiguous identity:

An identity comprising a set of attributes which relate unambiguously to a specific person or entity. The unambiguous connection between the identity and the person may be dependant on the context within which the identity term is used. Certain contexts may require assistance from the current registrar of various attributes.

URI

Universal Resource Indicator - an address on the Internet.

UTF8String

UTF-8 is a type of Unicode, which is a character set supported across many commonly used software applications and operating systems. UTF-8 is a multi-byte encoding in which each character can be encoded in as little as one byte and as many as four bytes. Most Western European languages require less than two bytes per character. Greek, Arabic, Hebrew, and Russian require an average of 1.7 bytes. Japanese, Korean, and Chinese typically require three bytes per character. Such Unicode is important to ensure that universal /foreign characters are supported.

Verification:

The process of ensuring that an assumption is correct. This term relates primarily to the process of ensuring that a digital signature represents the party which the signed information details as its issuer.

Vettor:

A person who verifies information provided by a person applying for a certificate.

Vulnerability:

Weaknesses in a safeguard or the absence of a safeguard.

Written:

Where this CPS specifies that information shall be written, this requirement is generally also met by digital data provided that the information it contains is accessible in such a way that it is useable by the parties involved.

X.500

Specification of the directory service required to support X.400 e-mail initially but common used by other applications as well.

X501 PrintableString:

String format for representing names, such as Common Name (CN), in X.509 certificates. The encoding of a value in this syntax is the string value itself; an arbitrary string of printable characters.

X.509:

ITU standard that describes the basic format for digital certificates.