Telia Server
Certificate Policy and Certification Practice Statement

CA name	Validation	OID
TeliaSonera Server CA v2 Telia Server CA v3	OV	2.23.140.1.2.2
Telia Extended Validation CA v3	EV	2.23.140.1.1
Telia Domain Validation SSL CA v1 Telia Domain Validation CA v2 Telia Domain Validation CA v3	DV	2.23.140.1.2.1
Telia Document Signing CA v3	Adobe, Web Trust	1.3.6.1.4.1.271.2.3.1.1.20

Revision Date: 23rd November 2020

Version: 2.9

Published by: Telia

Revision History

Version	Version date	Change	Author
1.0	11th June 2012	The first official version	TeliaSonera CA Policy Management Team
1.01	11th September 2012	Fixed minor errors in references	TeliaSonera CA Policy Management Team
1.02	21st 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	3rd 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	16th 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
1.4	16th November 2015	Clarifications mainly to EV processes, Revocation link added, CAA record handling	TeliaSonera CA Policy Management Team
1.5	4th January 2016	Clarifications mainly to EV processes based on EV pre-audit,	TeliaSonera CA Policy Management Team
1.6	1st December 2016	New company name “Telia”, New BR based OID values. LDAP references removed from CDP, new verification documentation, New ST value handling. Other improvements to CPS documentation.	Telia CA Policy Management Team

1.7	23rd March 2017	Telia Company -> Telia	Telia CA Policy Management Team
1.8	30th June 2017	New domain validation methods, validity of verified data to 27 months when reusing it.	Telia CA Policy Management Team
1.9	30th September 2017	CAA support (starting 8th September 2017), OCSP fully supports rfc6960, small clarifications, several new server names	Telia CA Policy Management Team
2.0	30th November 2017	DV added	Telia CA Policy Management Team
2.1	9th April 2018	Certificate Transparency included, max 2y validity for SSL, Enterprise signing certificate aka Telia Seal certificate, clearer audit requirements, small fixes in multiple chapters	Telia CA Policy Management Team
2.2	30th August 2018	New v2 issuers for DV and Document signing, E values are discarded from CSR, domain validation methods 3.2.2.4.1 and 3.2.2.4.5 are no more used, modified CAA chapter, improvements in domain validation chapter	Telia CA Policy Management Team
2.3	15th November 2018	New test certificate description, IP validation description, Telia Document Signing CA v1 removed (never used), Seal certificate process near to EV process, clarified certificate problem reporting description, old verification data valid max 825 days and not 27 months, OU validation description, list of supported Subject attributes, improved description of Seal certificates which provide Adobe trust, new technical support phone number	Telia CA Policy Management Team
2.4	15th March 2019	New BR compatible contact channel in chapter 1.5.1	Telia CA Policy Management Team
2.5	15th May 2019	BR 1.6.4 compatible domain validation. BR 1.6.5 compatible Subject value. Adobe AATL compatibility in 6.2.4.	Telia CA Policy Management Team

2.6	30th December 2019	-Seal certificate changes: a) EKU (7.1.2), b) Private key delivery (6.1.2, 6.2.6, 6.4.1), c) f2f in validation of authority (3.2.5); -v3 issuers added (1.2, 1.3, 2.1.2) -Updated audit scope (8.4); -Typographic corrections;	Telia CA Policy Management Team
2.7	30th March 2020	No stipulation replaced by a comment; Test certificate OID removed; Sections exactly like in RFC3647; More detailed re-key and modification chapters; support for ECC P521 removed; request tokens not used in domain validation; IP and wildcard validation added.	Telia CA Policy Management Team
2.8	30th October 2020	BR 1.6.8 compatible new file validation method v2, 1.3.1 Certification authorities, 1.3.2 Registration authorities, 2.3 Time or frequency of publication, 3.1.1 Types of names, 3.2.2 Authentication of organization identity and/or domain name, 4.9 Certificate revocation and suspension, 4.9.1 Circumstances for revocation, 4.9.3 Procedure for revocation request, 4.10.1 Operational characteristics, 6.1.1 Key pair generation, 6.3.2 Certificate operational periods and key pair usage periods, 7.1 Certificate profile, 7.1.2 Certificate extensions, 7.1.3 Algorithm object identifiers, 7.1.5 Name constraints, 7.2 CRL profile, 7.3 OCSP profile	Telia CA Policy Management Team
2.9	23rd November 2020	Added 3.2.2.6 Wildcard Domain Validation, 3.2.2.7 Data Source Accuracy, revision on contact info and some minor language changes	Telia 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, Telia Domain Validation CA, Telia Document Signing CA and Telia Extended Validation CA with all their active versions 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 Telia Production CPS, which describes the premises, procedures and routines which apply for the Production of Telia 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.

All certificates containing the OID value 2.23.140.1.2.2 are so called Organization Validation (OV) SSL certificates. All certificates containing the OID value 2.23.140.1.2.1 are so called Domain Validated (DV) certificates. Both OV and DV certificates conform to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates 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.

All certificates containing the OID value 2.23.140.1.1 are so called Extended Validation (EV) certificates and conform to the current version of the Guidelines For The Issuance And Management Of Extended Validation Certificates 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.

Telia SSL DV, OV and EV certificates provide a mean for relaying parties to evaluate trust when relying on such certificates. In case of organization validated (OV) or extended validation (EV) certificates Telia CA has verified the name and some other details of the entity that controls the website from official registers.
Telia 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.

Telia 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 Telia CA verified that the business was legally organized, used domain names were owned or managed by the Subject and in EV case also that Applicant's physical existence (business presence at a physical address), and operational existence (business activity) were verified.

Telia DV (Domain Validated) Certificate is a certificate that contains one or more host domain names (FQDN) or wildcard names of the Subscriber that has been validated according to the issuer's disclosed practices, but that does not contain any information about any organization or person associated with the Subscriber.

All certificates containing the OID value 1.3.6.1.4.1.271.2.3.1.1.20 are so called Telia Enterprise Signing certificates aka Seal certificates and conform to the current version of the Adobe Approved Trust List Technical Requirements (AATL). Such certificates provide a mean for relaying parties to see PDF documents trusted when opened in Adobe Acrobat or Adobe Reader software. Organization value in Telia Enterprise Seal certificates is verified by Telia to be correct using almost same validation methods than SSL EV certificate validation utilizes. Note! Telia Seal certificates are client certificates in WebTrust/BR context.

1.2 Document name and identification

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

This CPS is also a Certificate Policy for Telia OV, EV, DV and Seal 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**
Organization validation (OV) certificates	TeliaSonera Server CA v2 Telia Server CA v3	2.23.140.1.2.2 (from 2016-12-01)
Extended validation (EV) certificates	Telia Extended Validation CA v3	2.23.140.1.1
Domain validation (DV) certificates	Telia Domain Validation SSL CA v1 Telia Domain Validation CA v2 Telia Domain Validation CA v3	2.23.140.1.2.1
Telia Enterprise Seal certificates	Telia Document Signing CA v3	1.3.6.1.4.1.271.2.3.1.1.20

This CPS also refers to the Telia Production CPS with the name {TELIA- PRODUCTION-CPS-2}.

1.3 PKI participants

Telia Seal, OV, EV and DV certificates are issued to devices (e.g. web servers) possessed by Customers of Telia or directly by Telia. All of the participating organisations shall undertake what's stated in this Certification Practice Statement.

1.3.1 Certification authorities

The Certification Authority (CA) operating in compliance with this Certification Practice Statement is Telia CA. The legal entity responsible of Telia CA is Finnish company "Telia Finland Oyj" (BusinessID 1475607-9). Telia Finland Oyj is part of Swedish company "Telia Company AB" (businessID 5561034249).
The name of the Certification Authority in the "Issuer" field of the certificate is one of the issuing CA names listed in chapter 1.2.

Issuers with version code "v1" or "v2" are subordinate CAs of TeliaSonera Root CA v1. Issuers with version code "v3" are subordinate CAs of Telia Root CA v2. Older TeliaSonera Root CA v1 has been cross-signed by Telia Root CA v2. Telia Root CA has its own CP and CPS describing the management of the certificate life cycle of subordinate CA certificates signed by those.

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

For the full hierarchy see chapter 1.3.2 of the Telia CA Root CPS.

1.3.2 Registration authorities

The CA's units authorised to perform registration functions, Customers acting as Customers of certification services and authorised by CA, or other organisations selected and authorised as Registration Authorities (RAs), with which the CA makes written agreements, can act as RAs. 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

All RA functions for the Telia CA listed in this CPS are performed internally by Telia.

1.3.3 Subscribers

The Subscriber is the legal entity that makes an agreement with the CA about issuance of a certificate to a Device in its possession. With both Seal, OV and EV certificates the Subscriber is typically also the Subject of a certificate.

1.3.4 Relying parties

Any natural person or Legal Entity that relies on a Valid Certificate.

1.3.5 Other participants

Telia has made agreements with Application Software Suppliers so that they may trust and display certificates issued by Telia as trusted when used via their software.

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

Telia server certificates can be used, for example, to identify servers and secure SSL/TLS sessions. Telia Seal certificates are used to sign documents on behalf of an organisation.

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 Organisation administering the document

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

Contact information:

Telia Finland Oyj (1475607-9)
FI-00510 Helsinki
Phone: +35820401
Internet: https://cps.trust.telia.com/CPS

1.5.2 Contact person

Contact point in matters related to this CPS:

Telia CA Policy Management Team
Email: cainfo@telia.fi
Phone: +358 (0) 20401
Internet: https://cps.trust.telia.com/CPS

Other contact information:

Customer Service:	+358 206 93693 (normal office hour Help Desk services)
CA Customer Service:	cainfo@telia.fi (PKI support issues)
Revocation Service:	+358 (0) 800 156677 (revocation requests or any urgent issues) https://support.trust.telia.com/certificate_revocation_request_en.html

Certificate problem reporting:

Subscribers, relying parties, application software vendors, and other third parties can use two optional methods to contact Telia CA:

1) cainfo@telia.fi Support channel. Not necessarily handled within 24 hours.
2) ca-problems@telia.fi Important reports. Always handled within 24 hours (BR compliant)

Use either of these channels to report complaints or suspected private key compromise, certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to certification. In urgent cases we recommend contacting Telia Company or revoking the certificate by calling and using the above contact phone numbers also.

1.5.3 Person determining CPS suitability for the policy

Telia 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

Telia 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 https://cps.trust.telia.com.

2.1.2 Revocation Information Repository

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

Certificate Revocation Lists (CRLs) are published on the Telia website:

Issuing CA	**CRL addresses**
TeliaSonera Server CA v2	*http://httpcrl.trust.telia.com/teliasoneraservercav2.crl*
Telia Server CA v3	*http://httpcrl.trust.telia.com/teliaservercav3.crl*
Telia Extended Validation CA v3	*http://httpcrl.trust.telia.com/teliaextendedvalidationcav3.crl*
Telia Domain Validation SSL CA v1	*http://httpcrl.trust.telia.com/teliadomainvalidationsslcav1.crl*
Telia Domain Validation CA v2	*http://httpcrl.trust.telia.com/teliadomainvalidationcav2.crl*
Telia Domain Validation CA v3	*http://httpcrl.trust.telia.com/teliadomainvalidationcav3.crl*
Telia Document Signing CA v3	*http://httpcrl.trust.telia.com/teliadocumentsigningcav3.crl*

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 Telia CA Service or agreed with a Customer. OV, EV and DV 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 Telia'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

Telia 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.

Telia 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

Telia CA CPS is reviewed and updated or modified versions are published at least once per year and in accordance with section 9.12 of this CPS.

2.4 Access controls on repositories

This CPS, CRLs and CA certificates are publicly available. Only authorised 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) together with Subject Alternative Name values are used as an unambiguous name of the Subscriber. The naming will conclude of the following attributes:

	Description – OV SSL	**Description – EV SSL**	**Description – DV SSL**	Description – Seal
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.	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). The CN value is always one of the values contained in the Certificate's subjectAltName extension.	A name of the service or server (FQDN) which is owned or controlled by the Subject Organization
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.	Not allowed.	Customer in relation to which the Subject is identified. Common variations or abbreviations may also be used provided that the named owner is unambiguous.
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.	Not allowed.	City name. A component of the address of the physical location of the Subject's Place of Business.
Country (C, 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.	Not allowed.	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.	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.	The same value that was used in CN. Often useless in Seal certificates.

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	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 applicable
jurisdictionCountry Name (OID: 1.3.6.1.4.1.311. 60.2.1.3)	May be used like in EV. Optional in normal OV certificates.	Two character country code of the country in which the subject is registered	Not allowed.	Optional. May be used like in EV.
businessCategory (OID: 2.5.4.15)	May be used like in EV. Optional in normal OV certificates.	One of the following strings: "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity" depending how the Subject qualifies in CA validation.	Not allowed.	Optional. May be used like in EV.
serialNumber (OID: 2.5.4.5)	May be used like in EV. Optional in normal OV certificates.	Registration Number (e.g. Business ID or organization number) assigned to the Subject by the Incorporating or Registration Agency.	Not allowed.	Optional. May be used like in EV.

Additionally, in case of Seal, OV and EV, the "Subject" field may include following attributes depending on the usage purpose of the certificate:

	Description – OV SSL, EV SSL, Seal
organizationalUnit Name (OU,OID:2.5.4.11)	Optional. 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.
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.

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. None of the Subject attributes contains only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

If subjectAltName: dNSName has international characters, then puny-code converted version of the string will be used.

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

Distinguished Names in Certificates are interpreted using X.500 standards and ASN.1 syntax.

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 organisations. However, the CA may issue several certificates to the same organisation, 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.

Telia 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 organisation identity and/or domain name

Telia CA or its authorised 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 SSL certificate service agreement (Full SSL agreement) or in web order form. 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.

In case of Seal, OV and EV certificates, Telia CA verifies the organisation name (O) of a new Customer by checking the existence of the company, its legal name, business identity code and other relevant organisation information from an official business register maintained by an applicable government agency (e.g. “ytj.fi” in Finland). The list of applicable trusted registries is maintained in CA internal instructions. Subject’s registration number and address components (street, postalcode, locality, 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. All attributes must have a successfully verified value. Certificates whose subjectAlternativeName extension or Subject commonName field contains a Reserved IP Address or Internal Name are not allowed, and there are internal checks to avoid issuing such certificates.

Telia CA issued certificates will not contain metadata such as ‘.’, ‘-’, and ’ ’ (i.e. space) characters, and/or any other indication that a value is absent, incomplete, or a field is not applicable. dNSName entries may not contain underscore characters (“_”).

Telia verifies domain name and IP address ownership or control by using these methods listed in Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (BR).

3.2.2.4.1 Validating the Applicant as a Domain Contact.

This method is no more used after 2018-08-01 and all domains using this method are revalidated using some other method listed here.

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact

Telia may use Email address from Registrant section of Domain Name Register to check if the Applicant has the right to use the domain. Email is sent to the address including a unique random value. The random value is valid for use for 30 days from its creation. If the receiver confirms the domain request and know the random value the domain is approved.

3.2.2.4.3 Phone Contact with Domain Contact

This method is no more used after 2019-05-15. Method 3.2.2.4.15 Phone Contact with Domain Contact

will be used instead.

3.2.2.4.4 Constructed Email to Domain Contact

Telia may use Email addresses listed in BR to check if the Applicant has the right to use the domain. Email message including a unique random value is sent to the address. If the receiver confirms the domain request and know the random value the domain is approved. Random values are valid for 30 days. Messages may be re-sent in its entirety.

3.2.2.4.5 Domain Authorization Document

This method is no more used after 2018-08-01 and all domains using this method are revalidated using some other method listed here.

3.2.2.4.6 Agreed-Upon Change to Website

This method is no more used after 2020-03-24. Method 3.2.2.4.18 Agreed-Upon Change to Website v2 or 3.2.2.4.19 Agreed-Upon Change to Website - ACME will be used instead.

3.2.2.4.7 DNS change

Telia may confirm the Applicant's control over FQDN by confirming the presence of a Random Value for either in a DNS CNAME, TXT or CAA record for either 1) an Authorization Domain Name; or 2) an Authorization Domain Name that is prefixed with a label that begins with an underscore character. The Random Value is valid for 30 days and is unique for each receiver.

3.2.2.4.8 IP Address

Telia may confirm the Applicant's control over FQDN by using IP address related to FQDN and IP validation methods described in BR chapter 3.2.2.5. Normal IP validation method is to verify that the applicant or its representative is the owner of the IP in valid IP registry using method 3.2.2.5.2. Email, Fax, SMS, or Postal Mail to IP Address Contact but also method 3.2.2.5.1. Agreed-Upon Change to Website or 3.2.2.5.5. Phone Contact with IP Address Contact may be used.

If CSR has IP address Telia is verifying that it isn't defined as private IP address and then validate it using methods above or using method 3.2.2.5.3. Reverse Address Lookup.

3.2.2.4.15 Phone Contact with Domain Contact

Telia may use phone number from Registrant section of Domain Name Register to check if the Applicant has the right to use the domain. In the event that someone other than a Domain Contact is reached, the CA will request to be transferred to the Domain Contact.

3.2.2.4.18 Agreed-Upon Change to Website v2

Telia may confirm the Applicant's control over FQDN using random value method described in chapter 3.2.2.4.18 of BR. Telia is using random codes that include 256 bits of entropy. The Random Value is valid for 30 days and is unique for each receiver and for request. The file containing the random value is retrieved using http or https protocol in ports 80 or 443 respectively. The URL used is containing server component using the Authorization Domain Name and URL containing " /.well-known/pki-validation/_telia_validation_data_file" e.g. http://telia.fi/.well-known/pki-validation/telia_validation_data_file_20200323.txt. Possible redirects must be initiated by HTTP return code 30x and must be redirected to resource URLs with either "http" or "https" scheme using ports 80 or 443 respectively.

3.2.2.4.19 Agreed-Upon Change to Website - ACME

Telia ACME solution may confirm the Applicant's control over FQDN using method defined in section 8.3 of RFC 8555. Telia is using random token that include 256 bits of entropy. The Random token is valid for 30 days and is unique for request. The file containing the random code is retrieved using http protocol in port 80. Redirects are not supported so that response code must be 200.

Other allowed domain validation methods are used only in special circumstances and such usage must be authorised by supervising Telia Validation Board. Such special methods include:

- 3.2.2.4.12 Validating Applicant as a Domain Contact (if the CA is also the Domain Name Registrar)
    - 3.2.2.4.13 Email to DNS CAA Contact
- 3.2.2.4.14 Email to DNS TXT Contact
- 3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact
- 3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

These listed BR methods are not used:

- 3.2.2.4.1 Validating the Applicant as a Domain Contact
- 3.2.2.4.3 Phone Contact with Domain Contact
- 3.2.2.4.5 Domain Authorization Document
- 3.2.2.4.9 Test Certificate
- 3.2.2.4.10 TLS Using a Random Number
- 3.2.2.4.11 Any other method
- 3.2.2.4.20 TLS Using ALPN
- 3.2.2.5.4 Any Other Method

If the Subject field 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).

The subject value (OU) is verified each time separately. Telia verifies that it doesn't look like company name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity. If risk is identified Telia verify the value against applicable governmental company registry. Applicant must have a right to use the value. Empty pseudo values are technically rejected. In FullSSL service such manual verification can be done by the Customer Registration Officer and Telia regularly validates that all Registration Officers have used only correct values in all subject fields. If any incorrect values are found the Registration Officer is instructed to fix the incorrect values in further certificates and if the errors are significant the invalid certificates are immediately revoked.

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 OV and DV 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 Telia PKI board.

3.2.2.5 Authentication for an IP Address

For each IP Address listed in a Certificate, Telia confirms that, as of the date the Certificate was issued, the Applicant controlled the IP Address by:

- 3.2.2.5.1. Having the Applicant demonstrate practical control over the IP Address by confirming the presence of Random Value contained in the content of a file or webpage in the form of a meta tag under the "/.well-known/pki-validation" directory on the IP Address, performed in accordance with BR Section 3.2.2.5.1;

- 3.2.2.5.2. Confirming the Applicant's control over the IP Address by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value, performed in accordance with BR Section 3.2.2.5.2;

- 3.2.2.5.3. Performing a reverse-IP address lookup and then verifying control over the resulting Domain Name, as set forth above and in accordance with BR Section 3.2.2.5.3;

- 3.2.2.5.4. Telia will not perform IP Address validations using the any-other-method method of BR Section 3.2.2.5.4;

- 3.2.2.5.5. Confirming the Applicant's control over the IP Address by calling the IP Address Contact's phone number, as identified by the IP Address RA, and obtaining a response confirming the Applicant's request for validation of the IP Address, performed in accordance with BR Section 3.2.2.5.5

Telia CAs will not issue certificates with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name.

Entries in the dNSName MUST be in the "preferred name syntax", as specified in RFC 5280, and thus MUST NOT contain underscore characters ("_").

3.2.2.6 Wildcard domain validation

Before issuing a certificate with a wildcard character (*) in a CN or subjectAltName Telia confirms that, as of the date the Certificate was issued, the Applicant controlled the full domain. Telia prevents using just registry controlled public suffixes by utilizing domain suffix list from http://publicsuffix.org.

3.2.2.7 Data Source Accuracy

Telia CA ensures the reliability, integrity and authenticity of the data sources before issuing certificates according to the followings:

1. The age of the information provided by trusted third-parties and Telia internally,
2. The frequency of updates to the external and internal information source,
3. The data provider and purpose of the data collection,
4. The public accessibility of the data availability, and
5. The relative difficulty in falsifying or altering the data.

Telia CA only use trusted registers from government or reliable private company sources that are updated regularly to verify identity, address and any other information that might be required to issue a certificate.

3.2.3 Authentication of individual identity

Authentication of individual identity is done only as part of authorization verification described in 3.2.5.

3.2.4 Non-verified Subscriber information

Only subject attributes listed in chapter 3.1.1 are supported and thus verified. The Registration Officer is obliged to always review all included subject information and initiate additional checking routines if there are any unclear Subject values. Unknown extensions are accepted only if CA is aware of the reason for including the extension. Among others ST and E values are excluded from certificates and from verification because ST is useless in CA's current geographical scope and E is not supported.

3.2.5 Validation of authority

OV order via public web form or via using self-service software	Telia CA verifies that the administrative contact person defined in the certificate application is employed by the Customer. This is verified by calling the contact person via the Customer's PBX number or by making a phone call to other verified number(s) in the organisation, which is looked up from a directory maintained by a trusted party. Authorization of the administrative and technical contact persons may also be based on attorney letter or FullSSL agreement from the actual Customer. In that case CA will verify the origin of the authorization document by verification phone call. CA will always verify that the Customer's administrative contact person approves the subscriber agreement at least once including information about Customer responsibilities, Company details, authorised Certificate Approvers and all relevant subject or domain values allowed in the SSL certificates. In online service the agreement details are available to him/her online in the CA web pages so that the agreement can be modified at any time. In non-authenticated SSL web order all order details are verified each time by CA. In online mode the authenticated administrative contact person may be authorised by CA to approve further additions to the SSL contract (e.g. who can be Certificate Requester or Certificate Approver in the Company or if new domains are requested from CA). All authenticated and authorised contact persons are allowed to make SSL certificates but only in the limits of the pre-verified values and individual role. Data expiration time limits specified by CA/Browser Forum are utilized in all pre-verified values. Authentication is based on secure combination of client certificates, SMS-otp and weblinks with unique hash values. In internal Telia requests the authorization may be based on Employee register and authentication may be based on Telia email accounts. CA verifies that both technical and administrative contact persons are using approved Applicant company email addresses/domains and both persons are active employees of Telia Group according to the employee register and at least one representative is employee of Telia group and not an external worker.
EV order via public web form or via using self-service software	With the EV order the verification process is basically similar than above except that: 1) Customer's administrative contact person is verified to have Contract Signer role like specified in CA/Browser Forum EV specification 2) Two CA representatives will verify each component in EV order 3) Company verification process follow stricter rules like specified in CA/Browser Forum EV specification 4) Pre-verified data has shorter expiration time like specified in CA/Browser Forum EV specification 5) CA may use other verification rules to guarantee that EV order is properly verified and it is following all rules listed in CA/Browser Forum EV specification

DV order via public web form or via using self-service software.	Telia verifies host domain name/IP address ownership or control of those by using methods listed in Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.
Seal order via web form	Telia 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 by making a call to some other verified number in the organisation, which is looked up from a directory maintained by a trusted party. Authorization of the administrative and technical contact persons may also be based on attorney letter or FullSSL agreement from the actual Customer. In that case CA will verify the origin of the authorization document by verification phone call. In addition Applicant representative identity is verified using a strong identity proofing, based on a face-to-face meeting with the representative of the Applicant, or on a procedure that provides an equivalent assurance (e.g. by means of a secure video communication or using nationally accepted authentication (e.g. Telia Tunnistus identification) where face-to-face authentication has been a prerequisite or using trusted partner to do the same on behalf of Telia). CA will always verify that the Customer's administrative contact person approves the subscriber agreement at least once including information about Customer responsibilities, private key storage solution and Company details. In Seal certificate web order all order details are verified each time by CA.

For Seal, OV and EV orders both contact persons as well as Subscriber company are always checked against EU blacklist and only non-listed persons or companies are approved.

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 Telia 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 as specified in chapter 3.2.2.

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 as specified in chapter 3.2.2.

3.4 Identification and authentication for revocation request

Revocation by Customer

In cases where a Customer can issue SSL certificates using Telia's self-service software, the Subscriber shall submit a request for certificate revocation to the Registration Officer of its own organisation, 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 or another strong authentication method.

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, via web form or via online channel. The revocation service checks that the origin of the request is the Customer who owns or control the certificate. 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 authorised 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

Seal, OV or EV order via public web form	Manually processed Certificate application can be submitted by a representative of the Organisation, which possesses or will possess the Device or service to which the certificate is applied. If the application is submitted by a different organisation from the organisation that owns the service, domain name or the IP address (e.g. by an IT service provider), the application must be authorised by the organisation owning the service, domain name or IP address.
DV order via public web form	Like OV and EV but also host domain name/IP address ownership or control of those is verified by using methods listed in Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and any device or person having ownership or control of the server/domain can submit a valid DV application
DV, OV or EV order using Telia's self-service software	Automatically processed Certificate application can be submitted by an authorised Certificate Requester that has successfully authenticated to Telia's self-service software. The authorization must become from the organisation owning/controlling the domain and subject values and authorization and authentication must be approved by CA as described above in chapter "Validation of authority".

Telia CA will issue server certificates only to organisations that are registered in Finland, Sweden, Norway, Denmark, Lithuania, Estonia. Telia CA may refuse to issue certificates to organisations registered in countries where Telia cannot reliably validate information on the certificate application.

4.1.2 Enrolment process and responsibilities

Seal, DV, OV or EV order via public web form	A certificate to a Device (an EV, OV or DV server certificate) is applied by filling in a form that is publicly available at Telia'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 Telia's RA office where the sufficiency of the application is checked. Before the application can be submitted, the Subscriber has to accept the Subscriber responsibilities and terms and conditions of the service.

DV, OV or EV order using Telia's self-service software	A Certificate Requester in a Customer applies for certificates to Devices (OV or EV server certificates) directly from the CA system by using the self-service application provided by Telia. The application will print all relevant certificate request values on screen for final review. If accepted by the Certificate Requester and by the CA configuration the request is processed automatically. It may contain only pre-defined values like Domain Names and Organization Names (for EV or OV) that have been pre-validated by CA to this Customer. If the order includes new values or order is originated from a new person the customer's administrative contact must approve the new values or persons to be added to Customer's SSL contract. Then CA will verify that the Customer is allowed to use the new values before the certificate is created and the new values get pre-approved status for further orders. If the EV order includes components that are not pre-approved by two Registration Officers by CA or the values require special EV treatment the CA will verify the order even if it would be directly approved according to OV rules. Only Telia Registration Officers may add new allowed Domain Name or Organization Name values for Customers. New values are always verified according to 3.2.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

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

In addition to functions listed in section 3.2 Telia CA uses a second Registration Officer to verify all validations regarding EV certificate orders. The second Registration Officer will verify that the EV checks done by the first Registration Officer are correctly done and valid. If needed he/she will return the EV order to the first Registration Officer to fix the verification documentation.

Telia may use its previously documented verification data. Old verification data will expire in 825 days in OV and DV verification and in thirteen months in EV verification or earlier. Old verification data including organisation name, address components, Parent/Subsidiary/name change relationships, authorisation documents and domain/IP ownership are stored related to organisation's registration number if available.

4.2.2 Approval or rejection of certificate applications

Telia 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

Seal, DV, OV or EV order via public web form	Telia process the applications within reasonable time frame and usually within one work-day.
DV, OV or EV order using Telia's self service software	The certificate request is processed automatically by Telia's RA and CA systems immediately after the request is submitted. If automatic approval isn't possible CA will manually verify the order within reasonable time frame and usually within one workday.

4.2.4 Certificate Authority Authorization (CAA)

During validation Telia checks the DNS for the existence of a CAA record. If a CAA record exists that has issue, issuewild or iodef property tags and does not list Telia as an authorised CA, Telia won't issue the certificate.

Telia is using these domain names to authorise Telia as valid CAA issuer: "telia.com", "telia.fi", "telia.se".

Telia CA checks for a CAA record for each dNSName in the subjectAltName extension of the Certificate to be issued, according to the procedure in RFC 6844, following the processing instructions set down in RFC 6844 for any records found.

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 with the exception of DV. 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

Seal, DV, OV or EV order via public web form	Subscriber is informed of the acceptance or rejection of the certificate request. Telia's RA office delivers a web link to the contact person for fetching of the certificate.
DV, OV or EV order using Telia'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

All OV, EV and DV certificates will 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

DV,OV and EV certificates are distributed to external directories as required by Certificate Transparency specification at http://www.certificate-transparency.org/. There are no external notifications related to the issuance process.

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 Telia. 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 unauthorised 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 Telia 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. 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

Seal, DV, OV 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 as specified in chapter 3.2.2.
DV, OV or EV order using Telia's self-service software	Customer Certificate Requester has an option to renew certificates using the tools provided by the CA which may use the old CSR file to renew the certificate. Customer Certificate Requester is responsible to ensure that the certificate information is still valid and that there are no other obstacles to the renewal. CA will verify the renewal request like it were a new request. Even if all values were approved previously some pre-approvals or algorithms may have been expired or authorization may have been changed so the renewal request may now fail.

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

DV, EV and OV certificates are 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 but same subject

and SAN values than before.

4.7.1 Circumstance for certificate re-key

When old certificate is about to expire the subscriber has to renew the certificate. 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, Telia recommends that the Subscriber creates new key pair when renewing the certificate.

4.7.2 Who may request certification of a new public key

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

4.7.3 Processing certificate re-keying requests

Certificate re-key requests are processed as initial certificate requests as described in sections 4.1 – 4.4. CA may use the stored data of previous validations if available and such data is not expired.

4.7.4 Notification of new certificate issuance to subscriber

Certificate re-key notifications are generated like initial certificate notifications as described in section 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Certificate re-key acceptance is done like initial certificate acceptance as described in section 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

Certificate publication is done like initial certificate publication as described in section 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

Certificate re-key notifications are generated like initial certificate notifications as described in section 4.4.3.

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).

4.8.1 Circumstance for certificate modification

When old certificate needs any kind of update a modification is required. Currently Telia system requires that CSR is re-entered to CA system like in initial creation by the Subscriber. Certificate modification is not technically supported except in billing system which may count the new certificate as modification of the old one so that no extra billing is generated.

4.8.2 Who may request certificate modification

Certificate modification is not technically supported.

4.8.3 Processing certificate modification requests

Certificate modification is not technically supported.

4.8.4 Notification of new certificate issuance to subscriber

Certificate modification is not technically supported.

4.8.5 Conduct constituting acceptance of modified certificate

Certificate modification is not technically supported.

4.8.6 Publication of the modified certificate by the CA

Certificate modification is not technically supported.

4.8.7 Notification of certificate issuance by the CA to other entities

Certificate modification is not technically supported.

4.9 Certificate revocation and suspension

Telia CA supports certificate revocation. Certificate suspension is not used.

When a certificate is revoked, it is marked as revoked by having its serial number added to the CRL to indicate its status as revoked. In addition, the OCSP database will be updated and operational period of that certificate is immediately considered terminated.

4.9.1 Circumstances for revocation

Telia CA will revoke a Subscriber certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that Telia CA revoke the Certificate;
2. The Subscriber notifies Telia CA that the original certificate request was not authorised and does not retroactively grant authorization;
3. Telia CA obtains evidence that the Subscriber's private key corresponding to the public key in the certificate suffered a key compromise;
4. Telia CA obtains evidence that the validation of domain authorization or control for any Fully Qualified Domain Name (FQDN) or IP address in the Certificate should not be relied upon.

Telia CA will revoke within 5 days if one or more of the following occurs:

1. The Certificate no longer complies with the Baseline Requirements of Sections 6.1.5 and 6.1.6;
2. Telia CA obtains evidence that the certificate was misused;
3. Telia CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
4. Telia CA is made aware of any circumstance indicating that use of a FQDN or IP address in the certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
5. Telia CA is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subordinate FQDN;
6. Telia CA is made aware of a material change in the information contained in the certificate;
7. Telia CA is made aware that the certificate was not issued in accordance with the Baseline Requirements or the applicable CSP.
8. Telia CA determines or is made aware that any of the information appearing in the certificate is inaccurate;
    a. Telia CA's right to issue certificates under the Baseline Requirements expires or is revoked or terminated, unless Telia CA has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by Telia CA' applicable CPS; or
10. Telia CA is made aware of a demonstrated or proven method that exposes the Subscriber's private key to compromise, methods have been developed that can easily calculate it based on the public key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the private key was flawed.

4.9.2 Who can request revocation

The revocation of a certificate can be requested by:

1. A Subscriber or Certificate Requester from the Customer who has made an application for a certificate on behalf of an organisation, device or application; or
2. Personnel of Telia.
3. Owner of the server or device that possesses the certificate

4.9.3 Procedure for revocation request

Subscriber or Applicant may contact Telia Revocation Service by telephone, use an URL or via online channel and make a revocation request (look 1.5.2). Authorised Telia revocation staff then authenticates the identity of the originator of a revocation request according to section 3.4 and processes the revocation request using Telia's revocation system.

In case of SSL Service where the Customer can issue SSL certificates using Telia'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, Telia's system checks that the person making revocation request is authorised to do so and after that the certificate in question is revoked.

Revocation of certificates using ACME is also available.

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 Telia's self-service software, the Registration Officer shall revoke the certificate using the self-service software or inform Telia'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

Telia processes revocation requests within reasonable time frame or at least within 24 hours.

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 **two (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

Normally latency will be a matter of seconds.

4.9.9 On-line revocation/status checking availability

Telia is providing on-line revocation status checking via the OCSP protocol. The OCSP service address is added to certificate extension as defined by RFC6960.

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 near-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

Not applicable.

4.9.12 Special requirements regarding key compromise

Telia CA uses commercially reasonable efforts to notify potential Relying Parties if it discovers or suspects the compromise of a Private Key. Revocation reason code “key compromise” is used in such case.

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

Revocation information on a CRL or OCSP Response are not removed until after the expiry date of revoked certificates.

4.10.2 Service availability

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

4.10.3 Optional features

Relying parties may decide if they are using OCSP or CRL to verify certificate status. Telia recommends using OCSP as primary method and CRL as secondary method.

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

Not applicable.

5 FACILITIES, MANAGEMENT, AND OPERATIONAL CONTROLS

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

6 TECHNICAL SECURITY CONTROLS

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

The sections below are additions to the texts in the corresponding sections of the "Telia 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.
In case of Seal certificates, the keys are directly generated by and stored in such a secure cryptographic hardware device that complies with AATL technical requirements (FIPS 140-2 level2 or equivalent)

Requests for Subscriber Certificates are rejected if the Public Key does not meet the Baseline Requirements or the applicable CPS.

6.1.2 Private key delivery to Subscriber

Within DV, OV and EV certificates Telia never creates private keys.
In case of Seal certificates Customer typically creates and manages private key according to Subscriber agreement that list relevant AATL requirements. In case when Telia has initiated key generation and delivered such hardware token to Subscriber the activation code (PIN code) delivery is protected in a cryptographically secure manner so that only Subscriber can get it.

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 Telia Production CPS.

6.1.5 Key sizes

The CA requires that the Subscribers generate at least 2048 bit RSA keys or ECC curve NIST P256 or P384 keys.

6.1.6 Public key parameters generation and quality checking

Telia refuses 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 labelling 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

All stipulations regarding the section "6.2.2 Private key (n out of m) multi-person control" are specified in Telia Production CPS.

6.2.3 Private key escrow

Telia does not escrow Subscriber private keys.

6.2.4 Private key backup

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

Within Seal certificates the keys may be generated on HSM device that allow key backup only if a third party is managing the secure cryptographic hardware device on behalf of the signer. In that case device possessing the keys belongs to legal person. The Subscriber is responsible that no duplication of the private key is allowed, except for duly documented service availability purpose, and the duplicated key must abide at least the same security measures as the original. If the secure cryptographic hardware device is controlled directly by the signer, then the device must prevent exportation or duplication of the private key.

6.2.5 Private key archival

Telia does not archive Subscriber private keys.

6.2.6 Private key transfer into or from a cryptographic module

Within Seal certificates the private keys must be installed only on valid Hardware device defined by Adobe AATL Technical specifications. If Telia is not providing the hardware, Subscriber is responsible to follow this requirement and Subscriber must accept this requirement explicitly when ordering Telia Seal certificates. Telia or Adobe has right to verify the Customer installation or HSM implementation if there are any arguments about it.

6.2.7 Private key storage on cryptographic module

Check 6.2.6.

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.

Within Seal certificates if third party is managing the secure cryptographic hardware device on behalf of the Subscriber the key activation must rely on at least a 2-factor authentication (2FA) process. Telia or Adobe has right to verify the Customer installation or HSM implementation.

6.2.9 Method of deactivating private key

Subscribers should deactivate their Private Keys via logout and removal procedures when not in use.

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.

Within Seal certificates private keys must be stored in a secure cryptographic hardware device according to Adobe AATL Technical requirements. That means that HSM is certified according to:

I. FIPS 140-2 Level 2; or

II. Common Criteria (ISO 15408 & ISO 18045) - Protection Profiles CEN prEN 14169 (all parts applicable to the device type) or standards such as CEN EN 419 241 series or equivalent, for remotely managed devices; or

III. by an EU Member State as a Qualified Signature Creation Device (QSCD) after 1 July 2016, or that was recognized as a Secure Signature Creation Device (SSCD) by an EU Member State designated body before 1 July 2016.

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 Telia Production CPS.

6.3.2 Certificate operational periods and key pair usage periods

The usage period of the Subscriber Seal certificate shall not be longer than 3 years. The usage period of the Subscriber OV, EV and DV certificate is described below.

Certificates issued on or after 1 September 2020 don't have a validity period greater than 397 days.

Certificates issued after 1 March 2018, but prior to 1 September 2020, do not have a validity period greater than 825 days.

Certificates issued after 1 July 2016 but prior to 1 March 2018 do not have a validity period greater than 39 months.

6.4 Activation data

The Subscriber uses his private keys with the help of activation data. Check 6.2.8.

6.4.1 Activation data generation and installation

If Telia is not providing the hardware and activation data, 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. Check also 6.2.8 regarding Seal certificates.

Within Seal certificates Telia may generate and store the activation data. It is generated automatically using secure random method. It is protected into self-service system using cryptographically secure method so that only authorised Subscriber can read the codes.

6.4.2 Activation data protection

The Subscriber is recommended to keep his activation data appropriately protected from unauthorised access. Check also 6.2.8 regarding Seal certificates.

6.4.3 Other aspects of activation data

Not applicable.

6.5 Computer security controls

Check "Telia Production CPS".

6.6 Life cycle security controls

Check "Telia Production CPS".

6.7 Network security controls

Check "Telia Production CPS".

6.8 Time-stamping

Check "Telia Production CPS".

7 CERTIFICATE, CRL, AND OCSP PROFILE

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 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. Every DN will be in the form of an X.501 DirectoryString and Issuer DN is same than Subject DN of the Issuing CA in certificates.
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 Backdating of certificates in order to avoid some deadline or code-enforced restriction is not used by Telia CA.
Subject	This field identifies the Subscriber under whose possession the server possessing the certificate is. 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. This extension is mandatory in Telia SSL certificates. Telia asserts the compliance with the applicable CA Browser Forum standard as described in section 1.1.
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 2.1.2.
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 Telia server certificates. Purposes KeyCertSign and cRLSign are never set. The key usage purposes of the public keys contained in the OV, DV and EV certificates typically include: Digital Signature, Key Encipherment, Data Encipherment The key usage purposes of the public keys contained in the Seal certificates typically includes: nonRepudiation, Digital Signature
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 OV, DV and EV certificates include: Server authentication and Client authentication The extended key usage purposes of the public keys contained in the Seal certificates includes: 1.3.6.1.4.1.311.10.3.12 (Microsoft Doc. signing) 1.2.840.113583.1.1.5 (Adobe Authentic Documents Trust)

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: a) The url to CA-certificate b) OCSP service address Typically all server certificates include both listed values.

Also some other extensions may be used if agreed with Telia or added to CSR and CA is aware of a reason for including the data in the certificate. If Basic Constraints extension is used it doesn't allow CA flag to be true.

Application of RFC 5280

For purposes of clarification, a Pre-certificate, as described in RFC 6962 - Certificate Transparency, shall not be considered to be a "certificate" subject to the requirements of RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile under these Baseline Requirements.

7.1.3 Algorithm object identifiers

SHA-1 functionality was discontinued in 2014 except that old TeliaSonera Root certificates still use SHA-1.

Telia CA certificates are signed using one of the following algorithms:

1. sha256WithRSAEncryption OBJECT IDENTIFIER::={ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
2. ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2}
3. ecdsa-with-SHA384 OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3}

Telia CA only uses NIST "Suite B" curves for EDCSA.

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

Not applicable.

7.1.8 Policy qualifiers syntax and semantics

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

7.1.9 Processing semantics for the critical Certificate Policies extension

Not applicable.

7.2 CRL profile

Telia CAs issue CRLs that are compliant with RFC 5280.

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

Telia CA supports OCSP and their responders conform to the RFC 6960.

7.3.1 Version number(s)

Telia OCSP responders conform to RFC6960.

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. Audits are divided into an unbroken sequence of audit periods. An audit period must not exceed one year in duration.

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.
The auditor conducting audits listed in chapter 8.4 must be a licensed Practitioner for such audits.

8.3 Assessor's relationship to assessed entity

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

a) is owner to or joint owner to Telia or another company within the same group.
b) is a member of the Telia management or the management of any subsidiary, or assists with Telia's bookkeeping or management of means, or Telia'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 Telia 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 Telia 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 Telia and all engaged subcontractors are complying with the requirements of this CPS and Telia 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.

The audit for all certificates covered by this CPS is done in accordance with the WebTrust v.2.2 principles as documented here: http://www.webtrust.org. In addition all OV and DV certificates are audited also in accordance with WebTrust SSL Baseline with Network Security v1.4 as documented here:. EV certificates are audited in accordance with WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.6.2 as documented here http://www.webtrust.org.

In addition, Compliance Audit verifies that Seal certificates are compatible with requirements in Adobe AATL technical specification v2.0 and DV, OV and EV certificates are compatible with requirements in Mozilla Root Store Policy v 2.7.

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 Telia 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 Telia CA Service deems the deficiency to have risk to the operation of the Telia or Customers CAs, the Telia 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 Telia CA Service management with a copy of the results of the Compliance Audit. The results will not be made public unless required by law. Audit reports are published on Telia CA Web page https://cps.trust.telia.com and are informed to vendors that have root agreement with Telia. Detailed findings are stored by Telia CA and are not published.

8.7 Self-audits

Telia CA performs regular self-audits and audits of Registration Authorities in accordance with Section 8.7 of the Baseline Requirements.

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 Telia Production CPS.

9.3 Confidentiality of business information

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

9.4 Privacy of personal information

All stipulations regarding the section 9.4 Privacy of personal information are specified in Telia 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 Telia.

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 Telia 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 Telia Production CPS.

9.7 Disclaimers of warranties

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

9.8 Limitations of liability

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

9.9 Indemnities

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

9.10 Term and termination

9.10.1 Term

This CPS remains in force until notice of the opposite is communicated by Telia on its web site in the Telia CA Service Repository (https://cps.trust.telia.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 Telia's web site in the Telia CA Service Repository (https://cps.trust.telia.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

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

9.12 Amendments

Telia 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 Telia CA Service contact as described in Section 1.5. Decisions with respect to the proposed changes are at the sole discretion of the Telia 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 Telia CA Policy Management Team will post the notification at the CPS publishing point at (https://cps.trust.telia.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.

Telia 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 Telia CA Policy Management Team determines that a new Object Identifier (OID) is required, Telia 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 Telia Production CPS.

9.14 Governing law

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

9.15 Compliance with applicable law

All stipulations regarding the section 9.15 “Compliance with applicable law” are specified in Telia Production CPS.

9.16 Miscellaneous provisions

All stipulations regarding the section 9.16 “Miscellaneous provisions” are specified in Telia Production CPS.

9.17 Other provisions

All stipulations regarding the section 9.17 “Other provisions” are specified in Telia 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
DV	Domain Validation
EAL	Evaluation Assurance Level
EID	Electronic Identification
EV	Extended Validation
FIPS	Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
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 enrolment, 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 enrolment process.

Administrator:

A Trusted Person within the organisation of a Processing Centre, Service Centre, 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 organisation under contract and are subject to the same corporate policies as if they were an employee of the organisation.

Application Server:

An application service that is provided to an organisational or one of its partners and may own a certificate issued under the organisational 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.

Authorisation:

The granting of permissions of use.

Authorised 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 organisational structure defining functional roles and relationships.

CAA

From RFC 6844 (http:tools.ietf.org/html/rfc6844): “The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify the Certification Authorities (CAs) authorised to issue certificates for that domain. Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate mis-issue.”

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 organisational 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 throughout 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 certificates: 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 organisation manages its business. Specifically, security policy would be the set of laws, rules and practices that regulates how an organisation 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 a 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 sign 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 form 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.

Seal certificate:

All certificates containing the OID value 1.3.6.1.4.1.271.2.3.1.1.20 are so called Telia Enterprise Signing certificates aka Seal certificates and conform to the current version of the Adobe Approved Trust List Technical Requirements (AATL). Such certificates provide a mean for relaying parties to see PDF documents trusted when opened in Adobe Acrobat or Adobe Reader software. Organization value in Telia Enterprise Seal certificates is verified by Telia to be correct using almost same validation methods than SSL EV certificate validation utilizes. Note! Telia Seal certificates are client certificates in WebTrust/BR context.

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 is 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 an 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 an 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 unauthorised 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 dependent 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 commonly 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.