# Certificate Policy and Certification Practice Statement for Telia Client Certificates

Prepared by the Telia's Certification Authority Policy Management Team

Release: 3.8

Valid From: 2023-08-31

Classification: Public

# CONTENTS

# Revision History

| Version | Version date | Change | Author |
|---|---|---|---|
| 1.0 | 2012-06-11 | The first official version | TeliaSonera CA Policy Management Team |
| 1.01 | 2014-04-03 | Small fixes to text format | TeliaSonera CA Policy Management Team |
| 1.1 | 2015-04-16 | New SHA2 versions of each CA. Small other fixes. | TeliaSonera CA Policy Management Team |
| 1.2 | 2016-12-01 | New Company name, new improved documentation about validation of Customer authority in 3.2.5, few small corrections | Telia CA Policy Management Team |
| 1.3 | 2017-03-23 | Telia Company -> Telia | Telia CA Policy Management Team |
| 1.31 | 2019-09-30 | Changed number of persons needed for key recovery chapter 4.12.1 | Telia CA Policy Management Team |
| 1.4 | 2020-03-20 | No stipulation replaced by a comment; Fix CPS text that suspension hasn't be used; Fix CPS text regarding email domain validation in section 3.2.3; EKU is mandatory | Telia CA Policy Management Team |
| 1.5 | 2020-10-30 | Clarifications for 2.3 Time or frequency of publication, 4.9 Certificate revocation and suspension, 6.3.2 Certificate operational periods and key pair usage periods, 7.1.2 Certificate extensions, 7.1.3 Algorithm object identifiers, 7.2 CRL profile, 7.3 OCSP profile | Telia CA Policy Management Team |
| 1.6 | 2020-11-30 | Added information about issuing and usage of the short-lived personal certificates, removing the old SHA1 CA's, removing LDAP usage and suspended certificates, revision on the contact information | Telia CA Policy Management Team |
| 2.0 | 2021-02-17 | Merged with Telia root, production and customer CPSes | Telia CA Policy Management Team |
| 3.0 | 2021-06-11 | Removed Sonera Class2 CA, alignment with the new subscriber and relying party agreements, clarification on reporting key compromises, new CA hierarchy, clarifications on applicable law | Telia CA Policy Management Team |

| Version | Version date | Change | Author |
|---|---|---|---|
| 3.1 | 2021-07-15 | Added further explanation about the audit requirements according to ETSI, clarifications on definitions, clarifications on Mozilla root program requirements, other minor changes | Telia CA Policy Management Team |
| 3.2 | 2021-10-14 | ETSI compliance | Telia CA Policy Management Team |
| 3.3 | 2022-04-06 | Update section 5.1 to reflect current state of operations, specifically sections 5.1.2.1 and 5.1.2.2 respectively.<br><br>In section 1.3.1 incorrect SHA2 fingerprints for three (3) intermediate CAs corrected, Telia Class 1 CA v3, Telia Class 2 CA v2 and Telia Email CA v5 respectively<br><br>Minor typographic and spelling corrections throughout the document<br><br>Minor changes in the CA termination plan. | Telia CA Policy Management Team |
| 3.4 | 2022-06-07 | Ericsson NL Individual CA v4 created at 17th of May 2022, added to the CA hierarchy<br><br>As per [ETSI 319 401] REQ 6.3-9 and -10<br><br>“Information security policy;<br><br>The maximum interval between two checks shall be documented in the trust service practice statement”<br><br>Disclosure of maximum interval added to the section 9.12<br><br>Complete review and update of tables in the whole document describing CA details.<br><br>Problem reporting contact information added to the section 1.5.2 | Telia CA Policy Management Team |
| 3.5 | 2022-12-14 | Telia Sans font type face changed through the document to reflect Telia’s corporate document format policy. And minor typographic and grammatic changes made throughout the document<br><br>In section 4.4.3 language clarified to | Telia CA Policy Management Team |

| Version | Version date | Change | Author |
|---|---|---|---|
| | | express intended purpose<br><br>In section 1.5.4 disclosed PMT's CPS review policy<br><br>1.3.2.1 Updated the RA information for internal Telia Group email Certificate validation<br><br>1.3.2.2 Clarification of the purpose and role of the External RA<br><br>Annual full PMT review of the CP/CPS policy. | |
| 3.6 | 2023-03-21 | Changes identified by PMT's annual CP/CPS review in various sections of this CP/CPS | Telia CA Policy Management Team |
| 3.7 | 2023-06-13 | CP/CPS updates after PMT review of Telia CA's annual self-assessment to improve information provided in CP/CPS and to give explicit statements of current practice.<br><br>Detailed list of changes recorded by PMT in its meeting minutes. | Telia CA Policy Management Team |
| 3.8 | 2023-08-15 | CP/CPS update for CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates conformance | Telia CA Policy Management Team |

# 1 INTRODUCTION

## 1.1 Overview

This document is the Certificate Practice Statement (CPS) for client certificates, managed by Telia, or here after Telia Certification Authority (CA). It describes the Certificate Policy (CP), responsibility, operational, and technical procedures, and practices that Telia CA use in providing certificate services that include, but are not limited to, approving, issuing, using, revoking and managing certificates and operating a X.509 certificate based public key infrastructure (PKIX), including the management of a repository and informing the roles for parties involved such as Registration Authorities (RA), Subscribers or Relying Parties.

In summary following certificate types ("Services") are offered by Telia, equivalent to LCP, DVCP, OVCP, NCP and NCP+ as defined by ETSI 319 401 and ETSI 319 411-1:

Following client certificate types ("Services") are offered by Telia:

**(i)** **Telia DV certificate:** to authenticate servers and establishing secure TLS sessions with end clients. In this type of certificate, the domain name the server domain name is validated by Telia,

**(ii)** **Telia OV certificate:** to authenticate servers and establishing secure TLS sessions with end clients. In this type of certificate, domain name of the server, existence of the organisation and other attributes including name, type, status, and physical address is validated by Telia,

**(iii)** **Telia client certificate**: for identifying individual users, securing email communications and document signing, or

**(iv)** **Telia document signing (Seal) certificate:** for authenticating documents from Adobe PDF, Microsoft Office, OpenOffice, and LibreOffice.

Note! This CPS only discusses the practices and policies regarding the type (iii) of the list above.

This CPS conforms to the IETF PKIX Internet X.509 Public Key Infrastructure CP and CPS 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 the identification of the entity or entities that operate repositories; responsibility of a PKI participant to publish information regarding its practices, certificates, and the status; frequency of publication; and access control on the 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 an 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 concerning cryptographic key requirements.
- Section 7 - defines requirements for a 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.

## 1.2 Document name and identification

This CP/CPS is identified by the following information:

- **Name**: Certificate Policy and Certification Practice Statement for Telia Client Certificates
- **Release**: As stated on the cover page
- **OID**: 1.3.6.1.4.1.271.2.3.1.2.2
- **Location**: https://cps.trust.telia.com/

The certificates issued according to this CPS contain a CP OID corresponding to the applicable certificate type. The routines and roles resulting from this CPS apply only in connection with certificates referring to the following CP OIDs:

| CA | Type | CP OID |
|---|---|---|
| • TeliaSonera Root CA v1<br>• Telia Root CA v2 | Root CA | 1.3.6.1.4.1.271.2.3.1.1.2 |
| • TeliaSonera Class 1 CA v2 | User certificates for corporate Subscribers<br><br>(Finnish Registration Authority (RA)) | 1.3.6.1.4.1.271.2.3.1.1.11 |
| • Telia Class 1 CA v3 | User certificates for corporate Subscribers<br><br>(Finnish Registration Authority (RA)) | 1.3.6.1.4.1.271.2.3.1.1.11<br><br>2.23.140.1.5.1.1<br><br>2.23.140.1.5.3.1 |

| CA | Type | CP OID |
|---|---|---|
| • TeliaSonera Class 2 CA v2 | User certificates for corporate Customers<br>(Swedish RA) | 1.3.6.1.4.1.271.2.3.1.1.12 |
| • Telia Class 2 CA v3 | User certificates for corporate Customers<br>(Swedish RA) | 1.3.6.1.4.1.271.2.3.1.1.12<br>2.23.140.1.5.1.1<br>2.23.140.1.5.3.1 |
| • Telia Class 3 CA v1 | Short-lived personal certificates for individuals<br>(External RA) | 1.3.6.1.4.1.271.2.3.1.1.13 |
| • TeliaSonera Email CA v4<br>• Telia Email CA v5 | Email certificates for Telia Group | 1.3.6.1.4.1.271.2.3.1.1.14<br>2.23.140.1.5.1.1<br>2.23.140.1.5.3.1 |
| • Ericsson NL Individual CA v3 | User certificates for corporate Subscribers<br>(Swedish RA) | 1.3.6.1.4.1.271.2.3.1.1.18 |
| • Ericsson NL Individual CA v4 | User certificates for corporate Subscribers<br>(Swedish RA) | 1.3.6.1.4.1.271.2.3.1.1.18<br>2.23.140.1.5.1.1<br>2.23.140.1.5.3.1 |

## 1.3 PKI participants

Telia Root CAs (TeliaSonera Root CA v1 and Telia Root CA v2) issue Subordinate CA certificates to Telia and Subscribers hosting their CA at Telia.

A Subscriber that has agreed to and executed an Agreement with Telia and meets the requirements of this and other relevant CP/CPS can have a hosted CA at Telia CA.

Telia CA will issue certificates mainly to Subscribers of Telia but also to Telia employees or other clients. All the participating organisations shall undertake what is stated in this document.

### 1.3.1 Certification authorities

The CA operating in compliance with this CPS is Telia CA. The legal entity responsible of Telia CA is Finnish company “Telia Finland Oyj” (Business ID FI 1475607-9). Telia Finland Oyj is part of Swedish company “Telia Company AB” (Business ID SE 556103-4249).

The name of the CA in the “Issuer” field of the certificate is one of the issuing CA names listed in chapter 1.2.

As shown in Figure 1, Telia Root CA v2 is cross signed by TeliaSonera Root CA v1. Both versions of TeliaSonera Root CA v1 and Telia Root CA v2 certificates have the same key pairs and exist simultaneously (for validity check through self-signed or cross-signed path). Clients can use either one when doing PKI path validation.

In the hierarchy of subordinate CAs up to the root CAs (see Figure 1), Telia CA is responsible for ensuring the subordinate-CAs comply with the applicable policy requirements.

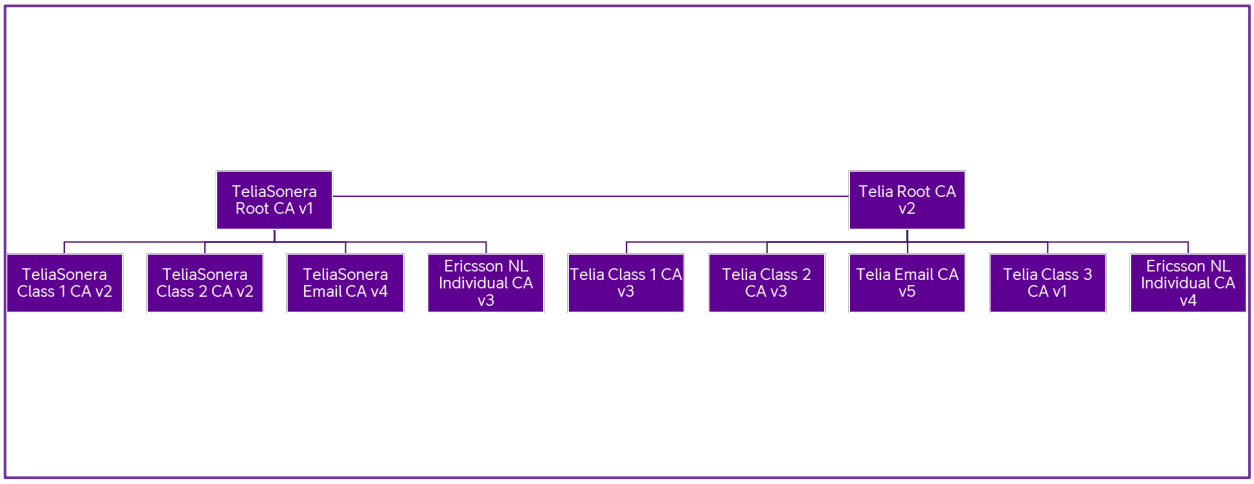


Figure 1, Telia CA Client Certificate PKI Hierarchy

The CAs 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

This CP/CPS governs all certificates issued and signed by the following CAs. Publicly Trusted S/MIME Certificates issued from the 1st of September 2023 onwards, Telia CA implements and supports only the **S/MIME Generation:Legacy, Mailbox-validated and Sponsor-validated certificate types** as defined in the Baseline Requirements for the Issuance and Management of Publicly Trusted S/MIME Certificates effective from the 1st of September 2023 and governed by this CP/CPS.

**Root CAs**

- **TeliaSonera Root CA v1**
  SHA2 Fingerprint:
  `DD6936FE21F8F077C123A1A521C12224F72255B73E03A7260693E8A24B0FA389`

- **Telia Root CA v2**
  SHA2 Fingerprint:
  `242B69742FCB1E5B2ABF98898B94572187544E5B4D9911786573621F6A74B82C`

**Cross-signed Root CAs**

- **Telia Root CA v2**
  SHA2 Fingerprint:
  `EF6F29F636F62BDD4753122F41F3419EE7C2877587BE4A9807ADF58946458E7F`

**Intermediate CA's**

- **TeliaSonera Class 1 CA v2**
  SHA2 Fingerprint:
  `F6E0D3006465585AA276E40861945102B2660708399879062FD53A2040EB5B31`

- **TeliaSonera Class 2 CA v2**
  SHA2 Fingerprint:
  `10D081A9541BF0B388818447A2A75465809AA5FB9A3DF375602472E873432AC1`

- **TeliaSonera Email CA v4**
  SHA2 Fingerprint:
  `77D82B83905D4465A3EB6B62E42081A7C273632F7D6CDA33A1E366987420AD12`

- **Ericsson NL Individual CA v3**
  SHA2 Fingerprint:
  `63ED95B17FFDCB7AE30FEAC6A874653099264E21B268D836D957966F0B04BE43`

- **Telia Class 1 CA v3**
  SHA2 Fingerprint:
  `E85BA26F89FEB670A2638E1E293054DE1A955DD1909A0AFD508B1F87F06104A9`

- **Telia Class 2 CA v3**
  SHA2 Fingerprint:
  `96FD4A9ED8E28B901D5E93E265992A9D411D49DC2280B5CF89398A862B7E26EC`

- **Telia Email CA v5**
  SHA2 Fingerprint:
  `E26BA792CDF9E21B6402044DD9A61E2E1537D5FFD22EE2478979408E3233310A`

- **Telia Class 3 CA v1**
  SHA2 Fingerprint:
  `E7340DC9475E87C4E5A4572C82604C5EFF9BF60B231C5486943173B26A4CAFCC`

- **Ericsson NL Individual CA v4**
  SHA2 Fingerprint:
  `EE0343093DF71E364606100164C62A4FB8C4A0F32B1EB47860FFD6C17E94CA54`

**Externally Operated Subordinate CAs**

- **None**

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
- Creating, storing, and recovering End-Entity confidential key pairs for organisations using the Telia key backup/restore service.

### 1.3.2 Registration authorities

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

Through those agreements, RAs are obliged to comply with this CPS for their part.

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

- Identification and authentication of certificate Subjects
- Initiating or pass along revocation requests for certificates
- Approving applications for new, renewal or re-keying certificates

Telia CA employs two RAs: Internal RA and External RA. Telia will not delegate domain validation to be performed by a third-party. The CA itself verifies email domain ownership or verifies that End-entity controls the email account.

#### 1.3.2.1 Internal Registration Authority

The Internal RA functions are executed as listed in the table below:

| Certificate type | Issuing CA | RA system and RA processes |
|---|---|---|
| User certificates for corporate Subscribers | TeliaSonera Class 1 CA v2<br><br>Telia Class 1 CA v3 | Finnish RA systems and RA processes |
| User certificates for corporate Subscribers | TeliaSonera Class 2 CA v2<br><br>Telia Class 2 CA v3<br><br>Ericsson NL Individual CA v3<br><br>Ericsson NL Individual CA v4 | Swedish RA systems and RA processes |
| Email certificates for Telia Group | TeliaSonera Email CA v4<br><br>Telia Email CA v5 | Swedish RA systems and respective RA processes as applicable in a given validation case |

The Registration Officer can be a physical person or an Application Programming Interface (API) to Telia's or Subscriber Organisation's system approved by Telia CA that is used to authenticate individual identity and submit the certificate request to the CA

system.

#### 1.3.2.2 External Registration Authority

The External RA functions are listed in the table below:

| Certificate type | Issuing CA | RA system and RA processes |
|---|---|---|
| Short-lived personal certificates for individuals | Telia Class 3 CA v1 | Delegated Third Party External RA contracted by Telia |

For this purpose, Telia ensures identity validation of individuals is done using substantial authentication methods (e.g. Swedish Bank ID) from trusted industry-wide identity provider sources.

### 1.3.3 Subscribers

A Subscriber may be a natural person or an organisation that is a Subscriber of Telia or an individual employed by Telia, requesting a Certificate through an account at Telia CA. Subscribers may allow Applicants to apply for a Certificate from the CAs listed in this CPS

The Subject for the short-lived personal certificates is a natural person that uses the issued certificate to sign a document, however not in possession of the private key that is managed by an External Telia Partner (e.g. External RA).

Telia considers a Subscriber as an Applicant for the services of Telia CA until issuance of the certificate, where its Subject is assigned to the Applicant. The Subscriber will be accountable for the proper usage of the Certificate regardless of the Applicant's responsibility.

### 1.3.4 Relying parties

Relying Parties use Telia CA services that are used to create Certificates and may rely on such Certificates and/or digital signature against the Public Key of the Subscriber's Certificate. Validity of a Certificate can be verified by a Relying Party through the CRL listed in the Certificate or through OCSP prior using the Certificate.

### 1.3.5 Other participants

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

Telia employs two group of partners to assist in providing the certificate services to Subscribers and Applicants: Certificate Manufacturer and External Partner.

#### 1.3.5.1 Certificate Manufacturer

Certificate Manufacturer is CA's subcontractor that is involved in the production of certification services in another role than that of RA. Also, when using Certificate Manufacturers as subcontractors, Telia CA is, however, ultimately responsible for the certification services.

#### 1.3.5.2 External Partner

External partnership with Telia provides the possibility of reselling Telia issued certificates by external companies that are trusted. Such companies are in charge of certificate lifecycle for their Subscribers. Telia considers such External Partners as External RAs or Enterprise RAs.

## 1.4 Certificate usage

### 1.4.1 Appropriate certificate uses

Certificates under this CPS are issued for the following applications:

- Root certificates: used to create Intermediate and Subordinate CAs
- S/MIME certificates: used to sign and encrypt emails
- Authentication certificates: used for subject authentication
- Signing certificates: short-lived certificates used for document signing

| CA | Appropriate usage |
|---|---|
| • TeliaSonera Root CA v1<br>• Telia Root CA v2 | These CAs issue certificates for Intermediate and Subordinate CAs. |
| • TeliaSonera Class 1 CA v2<br>• Telia Class 1 CA v3 | These certificates are issued for persons and devices within Subscribers and Telia. The certificates are intended for Subscriber's use in VPN, login, email, and other similar services. |
| • TeliaSonera Class 2 CA v2<br>• Telia Class 2 CA v3 | These certificates are issued for persons within Subscribers and Telia. The certificates are intended for securing email and other similar services. |
| • Ericsson NL Individual CA v3<br>• Ericsson NL Individual CA v4 | These certificates are issued for persons within Telefonaktiebolaget LM Ericsson. The certificates are intended for securing email and other similar services. |
| • TeliaSonera Email CA v4<br>• Telia Email CA v5 | These CA issues individual certificates to be used for signing and encrypting e-mails. Certificates are issued to Telia employees within the Telia Group and to individuals contracted by Telia. |
| Telia Class 3 CA v1 | Short-lived personal certificates for document signing by natural individuals. |

### 1.4.2 Prohibited certificate uses

Certificates under this CPS are not intended for servers or gateways. Thus "Extended Key Usage" purposes for "Server authentication", "Code signing" and "Time stamping" are prohibited.

Applications using certificates issued under this CPS shall consider the key usage

purpose stated in the “Key Usage” and “Extended Key Usage” extension field of the certificate.

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

It is not recommended to use certificates for encryption if the private key of the certificate is not backed up.

## 1.5 Policy administration

### 1.5.1 Organisation administering the document

The Telia CA Policy Management Team (PMT) is the responsible authority for reviewing and approving changes to this CP/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 PMT.

Contact information:

| |
|---|
| Telia Finland Oyj<br>Pasilan Asema-aukio 1<br>FI-00520 Helsinki, Finland<br>Phone: +358 (0) 20 401<br>Internet: https://cps.trust.telia.com/<br>Business ID: 1475607-9 |

### 1.5.2 Contact person

Contact person in matters related to this CPS:

| |
|---|
| Telia CA Policy Management Team (PMT)<br>Email: cainfo@telia.fi<br>Phone: +358 (0) 20 401<br>Internet: https://cps.trust.telia.com/ |

Other contact information:

| | |
|---|---|
| **Finland** | Customer Service: +358 20 693 693<br>Revocation Service: +358 800 156 677<br>Support: cainfo@telia.fi |
| **Sweden** | Customer Service and Revocation:<br>020 323 262, +46 771 323 262<br>kundtjanst-eid@teliacompany.com |
| **Certificate Problem report** | Problem reporting instructions, please see:<br><br>https://support.trust.telia.com/palvelinvarmenneturvallisuus_en.html |

### 1.5.3 Person determining CPS suitability for the policy

The PMT is the authority for determining this CPS suitability to the applicable policies.

### 1.5.4 CPS approval procedures

The PMT 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.

The PMT shall review whole CPS on annual basis. Such review is recorded in the CPS changelog as new CPS version and published according to Telia CA's CPS management policy.

## 1.6 Definitions and acronyms

### 1.6.1 Definitions

| | |
|---|---|
| **Affiliate** | A corporation, partnership, joint venture, or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity. |
| **Agent** | A person, contractor, service provider 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. |
| **Applicant** | The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Initial Certificate was created (initialization), the Applicant is referred to as the Subscriber. For Certificates issued to End-entities, the Subscriber (Certificate Applicant) is the entity that controls or operates/maintains the end-entity to which the Certificate is issued, even if the end-entity is sending the actual certificate request. |
| **Baseline Requirements** | Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates |
| **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 to sign certificates and where the public key is used to verify the same certificate. |
| **CA/Browser Forum** | A group of representatives from certificate authorities and browser vendors to discuss issues surrounding the existing market for server certificates, e.g., certificates used in authenticating TLS-enabled web sites and other servers (e.g., mail servers) to users. |
| **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." |
| **Certificate** | An electronic document issued by Telia to a person or entity mainly for verifying the identity of the sender/receiver of an electronic message, and/or for providing the means to encrypt/decrypt messages between sender and receiver (e.g., binding an entity to their public key). |
| **Certificate Policy (CP)** | 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. |

| | |
|---|---|
| **Certificate Request** | A process where a natural person (the Subscriber or someone employed by the Subscriber) or an authorised agent with the authority of representing the Subscriber that completes and submits a certificate request. |
| **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. |
| **Certification Authority (CA)** | CA is a trusted entity such as Telia that is authorised to create, sign, distribute, and revoke certificates. CA is also responsible for distributing certificate status information and providing a repository where certificates and certificate status information is stored. |
| **Certification Chain** | An ordered list of Certificates containing a Subscriber Certificate and CA Certificates, which terminates in a root Certificate. |
| **Certification Practice Statement (CPS)** | CPS is a document that defines the legal, commercial, and technical practices for approving, issuing, using, and managing Telia Server and Client certificates. It also outlines the roles and responsibilities of the parties involved in maintaining the Telia public key infrastructure. |
| **Client Certificate** | A digital certificate in which information about the organization and email of holding the certificate has been validated by Telia. |
| **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 electronic ID cards. |
| **Delegated Third Party** | A natural person or Legal Entity that is not the CA but is authorized by the CA, and whose activities are not within the scope of the appropriate CA audits, to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein. |
| **Digital Signature** | A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents. |
| **Distinguished Name (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. |
| **Document Signing (Seal) Certificate** | Used for authenticating documents from Adobe PDF (AATL), Microsoft Office, OpenOffice, and LibreOffice |
| **Domain Name** | The label assigned to a node in the Domain Name System (DNS). |
| **Domain Name Registrant** | Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar. |
| **Domain Name Registrar** | A person or entity that registers Domain Names under the auspices of or by agreement with: i. the Internet Corporation for Assigned Names and Numbers (ICANN), ii. a national Domain Name authority/registry, or iii. a Network Information Center (including their affiliates, contractors, delegates, successors, or assignees). |
| **Domain Namespace** | The set of all possible Domain Names that are subordinate to a single node in the Domain Name System. |
| **Domain Validated (DV) TLS Certificate** | A digital certificate for a web site or other server in which the information about the domain name has been validated by Telia. |

| | |
|---|---|
| **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 can access or utilize the materials, e.g., cryptographic key. |
| **End-Entity** | User of PKI certificates and/or end user system that is the subject of a certificate and cannot sign other certificates. |
| **Enterprise RA** | An employee or agent of an organisation unaffiliated with the CA who authorises issuance of Certificates to that organisation. |
| **Internal Server Name** | A Server Name (which may or may not include an Unregistered Domain Name) that is not resolvable using the public DNS. |
| **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 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. |
| **Legal Entity** | An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system. |
| **Object Identifier** | The unique alpha-numeric identifier registered under the ISO registration standard to reference a standard object or class. |
| **OCSP Responder** | An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol. |
| **Online Certificate Status Protocol** | An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder. |
| **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** | The community verification key for digital signature and the community encryption key for encrypting information to a specific Subscriber. |
| **Public Key Infrastructure (PKI)** | A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates. |
| **Publicly Trusted Certificate** | A Certificate that is trusted by virtue of the fact that its corresponding Root certificate is distributed as a trust anchor in widely available application software. |
| **Qualified Auditor** | A natural person or Legal Entity that meets the requirements of Section 8.2. |
| **Registered Domain Name** | A Domain Name that has been registered with a Domain Name Registrar. |
| **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-keying** | 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. |

| | |
|---|---|
| **Reliable Data Source** | An identification document or source of data used to verify Subject Identity Information that is generally recognised among commercial enterprises and governments as reliable, and which was created. |
| **Relying Party** | Anybody who relies on the certificates issued by Telia (including all end users and operating system vendors who trust Telia certificates). |
| **Repository** | An online database containing publicly disclosed Telia PKI governance documents, and certificate status information, either in the form of a CRL or an OCSP response. Currently at this link: https://cps.trust.telia.com. |
| **Revocation** | 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 CRL. |
| **Subject** | The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber. |
| **Subject Identity Information** | Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field. |
| **Subordinate CA** | A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA. |
| **Subscriber** | A person or entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement and Terms of Use. |
| **Subscriber Agreement** | An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties. |
| **Terms of Use** | Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with the CA/B Forum requirements when the Applicant/Subscriber is an Affiliate of the Telia CA or is the CA. |
| **TLS 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 TLS session (secure channel). There are different types of TLS certificates: single-domain, multi-domain and wild-card (SAN). |
| **Token** | Hardware devices, normally associated with a reader, used to store and/or generate encryption keys, such as smartcards and USB tokens. |
| **Trustworthy System** | Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. |
| **Unregistered Domain Name** | A Domain Name that is not a Registered Domain Name. |
| **Valid Certificate** | A Certificate that passes the validation procedure specified in RFC 5280. |
| **Validity Period** | From RFC 5280 (http://tools.ietf.org/html/rfc5280): "The period of time from notBefore through notAfter, inclusive." |
| **WHOIS** | Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website. |
| **Wildcard Certificate** | A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully Qualified Domain Names contained in the Certificate. |
| **Wildcard Domain Name** | A Domain Name consisting of a single asterisk character followed by a single full stop character ("*.") followed by a Fully Qualified Domain Name. |

### 1.6.2 Acronyms

| | |
|---|---|
| **AATL** | Adobe Approved Trust List |
| **BR** | Baseline Requirements for the Issuance and Management of Publicly Trusted S/MIME Certificates |
| **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 |
| **ETSI** | European Telecommunications Standards Institute |
| **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 |
| **NTP** | Network Time Protocol |
| **OCSP** | On-line Certificate Status Protocol |
| **OID** | Object Identifier |
| **PDF** | Portable Document Format |
| **PIN** | Personal Identification Number |
| **PKCS** | Public Key Cryptography Standards |
| **PKI** | Public Key Infrastructure |
| **PKIX** | Public Key Infrastructure X.509 (IETF Working Group) |
| **PMT** | Policy Management Team |
| **RA** | Registration Authority |
| **RFC** | Request for Comments |
| **RSA** | Rivest-Shamir-Adleman asymmetric encryption algorithm |
| **S/MIME** | Secure Multipurpose Internet Mail Extension |
| **SHA** | Secure Hash Algorithm |
| **TLS** | Transport Layer Security |
| **URI** | Uniform Resource Identifier |
| **URL** | Uniform Resource Locator |
| **VPN** | Virtua Private Network |

# 2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

## 2.1 Repositories

### 2.1.1 CPS Repository

A full text version of this CPS is published at the Repository https://cps.trust.telia.com/.

### 2.1.2 Revocation Information Repository

Following CRLs are published in the Telia's website:

| Issuing CA | CRL addresses |
|---|---|
| TeliaSonera Root CA v1 | http://httpcrl.trust.telia.com/teliasonerarootcav1.crl |
| Telia Root CA v2 | http://httpcrl.trust.telia.com/teliarootcav2.crl |
| TeliaSonera Class 1 CA v2 | http://httpcrl.trust.telia.com/teliasoneraclass1cav2.crl |
| TeliaSonera Class 2 CA v2 | http://httpcrl.trust.telia.com/teliasoneraclass2cav2.crl |
| TeliaSonera Email CA v4 | http://httpcrl.trust.telia.com/teliasoneraemailcav4.crl |
| Ericsson NL Individual CA v3 | http://crl.trust.telia.com/ericssonnlindividualcav3.crl |
| Telia Class 1 CA v3 | http://httpcrl.trust.telia.com/teliaclass1cav3.crl |
| Telia Class 2 CA v3 | http://httpcrl.trust.telia.com/teliaclass2cav3.crl |
| Telia Email CA v5 | http://httpcrl.trust.telia.com/teliaemailcav5.crl |
| Telia Class 3 CA v1 | http://httpcrl.trust.telia.com/teliaclass3cav1.crl |
| Ericsson NL Individual CA v4 | http://httpcrl.trust.telia.com/ericssonnlindividualcav4.crl |

OCSP is the recommended method to check certificate validity. Telia OCSP service is available at URL http://ocsp.trust.telia.com. OCSP requests may be signed or unsigned depending on the Subscriber Agreement and the payment method.

### 2.1.3 Certificate Repository

CA certificates are published in the 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 Subscriber.

The Repository will be available 24 hours per day, 7 days per week. If there will be a technical failure, that should not affect the availability of the services significantly more than 48 hours.

## 2.2 Publication of certification information

It is Telia's role to make the following information available:

a. This CPS
b. Certificate revocation lists of revoked certificates or revocation information via OCSP
c. Issued CA certificates and cross-certificates for cross-certified CAs

Telia may publish and supply certificate information under applicable legislation.

Each published 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.

Telia CA conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates published at https://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

## 2.3 Time or frequency of publication

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

## 2.4 Access controls on repositories

This CPS, CRLs and CA certificates are publicly available using read-only access. Only authorised CA personnel have access to information stored in the local database of the CA system.

# 3 3. IDENTIFICATION AND AUTHENTICATION

## 3.1 Naming

### 3.1.1 Types of names

An X.501 Distinguished Name (DN) is used as an unambiguous name of the Subject in the ”Subject” field of the certificate. The name always includes the following attributes except for the short-lived certificates that are not bound to an organisation (in such cases the issued certificate will not include O attribute)

#### 3.1.1.1 Root CA

The following attributes are used in the Subject field of the root CA certificates:

| **Attribute** | **Description of value (TeliaSonera Root CA v1)** | **Description of value (Telia Root CA v2)** |
|---|---|---|
| commonName (CN, OID 2.5.4.3.) | TeliaSonera Root CA v1 | Telia Root CA v2 |
| OrganizationName, (O, OID 2.5.4.10) | Telia | Telia Finland Oyj |
| Country (C, OID 2.5.4.6) | - | FI |

#### 3.1.1.2 Subordinate CAs

The following attributes are used in the Subject field of Subordinate CA certificates:

| **Attribute** | **Description of value** |
|---|---|
| commonName (CN, OID 2.5.4.3) | Name of the subordinate CA |
| OrganizationName (O, OID 2.5.4.10) | Name of the CA organisation. The name is either “Telia” or the legal name of Subscriber hosting CA at Telia. |
| Country (C, OID 2.5.4.6) | Country where the CA organisation is incorporated. |

#### 3.1.1.3 Subscriber Certificates

The subscriber certificates may include the following attributes in the Subject field:

| **Attribute** | **Description of value** |
|---|---|
| commonName (CN, OID 2.5.4.3) | Name of the Subject. |

| Attribute | Description of value |
|---|---|
| OrganizationName (O, OID 2.5.4.10) | Subscriber Organisation in relation to which the Subject is identified. |
| organizationIdentifier (OID 2.5.4.97) | The value is the NTR Registration Scheme identifier, where registrations are administrated at country level, a 2 character ISO 3166-2 identifier for the the nation in which the Registration Scheme is operated, preceded by a hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)) |
| Surname (S, OID 2.5.4.4) | Family name of the Subject |
| givenName (G, OID 2.5.4.42) | Subject's names, which are not family name |
| serialNumber (OID 2.5.4.5) | Character string that can be used to distinguish similar Subject names, e.g. personal ID number or username. |
| State or province (ST, OID 2.5.4.8) | Location of the Subscriber or the Subject |
| Locality (L, OID 2.5.4.7) | Location of the Subscriber or the Subject |
| Country (C, OID 2.5.4.6) | Location of the Subscriber or the Subject. Two letter country code e.g. "FI" or "SE" |
| domainComponent (DC, OID 0.9.2342.19200300.100.1.25) | Multiple values specifying the domain name of the Subject. |
| emailAddress (E, OID 1.2.840.113549.9.1) | Subject's email address. |

Subject name information may also be contained in the Subject Alternative Name X.509 version 3 extensions. Subject Alternative Name extension may contain following information:

| Attribute | Description of value |
|---|---|
| rfc822Name | E-mail address of the Subject |
| otherName | Other Name field can be used for Microsoft Windows user principal name (UPN) in the certificates issued to natural persons. |
| dNSName | dNSName field may contain one or more DNS domain names of the Device. |

| Attribute | Description of value |
|---|---|
| iPAddress | iPAddress field may contain one or more IP addresses of the Device. |

Distinguished Name (DN) and Subject Alternative Name attributes are verified by CA. None of the Subject attributes contains only metadata such as '.', '-', and ' ' (e.g. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

If subjectAltName: dNSName has international characters, then punycode 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

The commonName attribute can include the name, or a pseudonym, of the Subject.

Except within Telia Class 3 CA v1 certificates the organizationName attribute always contains a Subscriber Organisation's name that accurately identifies the Subscriber.

### 3.1.4 Rules for interpreting various name forms

The commonName (CN) attribute contains the name of the Subject in the following forms:

| | |
|---|---|
| **TeliaSonera Class 1 CA v2**<br><br>**Telia Class 1 CA v3** | For S/MIME Certificates issued by **Telia Class 1 CA v3**.<br><br>In accordance with section 3.1.4 of the S/MIME Baseline Requirements.<br><br>For other Certificates<br><br>The commonName is composed of the username or similar used by the Subscriber Organisation to identify users or devices in the VPN or other service that the certificates are used for. |
| **TeliaSonera Class 2 CA v2**<br><br>**Telia Class 2 CA v3**<br><br>**TeliaSonera Email CA v4**<br><br>**Telia Email CA v5** | For S/MIME Certificates issued by **Telia Class 2 CA v3, TeliaSonera Email CA v4 and Telia Email CA v5.**<br><br>In accordance with section 3.1.4 of the S/MIME Baseline Requirements.<br><br>For other Certificates<br><br>The commonName is composed of the given and surname of the Subject, and it can additionally contain other given names or initials.<br><br>If the certificate is issued to a group email account or similar, then the commonName should be the name of the related function or organisational unit. |
| **Telia Class 3 CA v1** | The commonName is composed of given name and surname obtained from trusted source such as Swedish BankID. |
| **Ericsson NL Individual CA v3** | For S/MIME Certificates<br><br>In accordance with section 3.1.4 of the S/MIME Baseline Requirements. |

| | |
|---|---|
| **Ericsson NL Individual CA v4** | For other Certificates<br><br>The commonName is composed of the given and surname of the Subject, and it can additionally contain other given names or initials.<br><br>If the certificate is issued to a group email account or similar, then the commonName should be the name of the related function or organisational unit. |

The Organization (O) attribute states the Subscriber Organisation in relation to which the Subject is identified. Normally Organization attribute contains the registered name of the Organisation with or without the abbreviation for the form of company incorporation. In some cases, the CA may also accept an Organization name attribute that is other than the official registered name of the Organization, if the name is commonly used or there is otherwise no risk of confusion.

### 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 entities. However, the CA may issue several certificates to the same entity, and in that case, the Subject names in those certificates may be the same.

Unambiguousness of the Subject names is secured in a two-phase procedure. A name contains both the name of the organisation and the name of the Subject. The CA system allows only unambiguous organisation names. The Subscriber Organisation is not able to change the organisation name that the CA has recorded for the organisation in the CA system. The Subscriber Organisations are responsible for the unambiguousness of the names of their own users and devices.

### 3.1.6 Recognition, authentication, and role of trademarks

The priority to entity names is given to registered trademark holders.
The use of a Domain Name is restricted to the authenticated legal owner of that Domain Name.
The use of an email address is restricted to the authenticated legal owner of that email address.

Telia does not otherwise check the right of the Subscriber Organisation to use the names it gives in its certificate applications except for the Organization Name as stated in section 3.2.2, nor does the CA participate in any name claim dispute resolution procedures concerning brand names, domain names, trademarks, or service names. 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

This section describes the Telia CA identification and authentication procedures for registration of subjects. Validation practice introduced in this section governs both Publicly Trusted S/MIME validation and other certificate types governed by this CP/CPS.

Separation between the two is clearly indicated in applicable subsections as seen necessary.

Telia CA implements **Legacy Generation** Publicly Trusted S/MIME Certificates for:

- Mailbox-validated and
- Sponsor-validated

profiles defined by the BR.

### 3.2.1 Method to prove possession of private key

All CA private keys are generated by Telia within the system and stored in a Hardware Security Module (HSM).

If the CA or RA does not generate the key pair of the Subject the CA or RA verifies:

a. The electronic signature included in the PKCS #10 Certificate Signing Request (CSR) to be corresponding to the public key of the signers in the CSR
b. Integrity of the signed data

### 3.2.2 Validation of authorization or control of domain and/or mailbox

Telia CA SHALL NOT delegate verification of domain and/or mailbox authorization or control. Telia CA SHALL verify Applicant's control or authorization (in case of Mailbox, only accepted authorization is for the email account holder) over domain and/or Mailbox fields referenced in the issued Certificates.

Telia CA employs validation methods allowed and described in the then current Telia Certificate Policy and Certification Practice Statement for Telia Server Certificates (section 3.2.2.4) valid and publicly disclosed in the Telia CA Public Repository (https://cps.trust.telia.com). Validation records document the method and the version number of TLS Baseline Requirements or S/MIME Baseline Requirements used to validate every domain or email address in issued Certificates.

Telia CA SHALL use only the approved methods in Section 3.2.2.4 of the TLS Baseline Requirements to perform this verification.

#### 3.2.2.1 Publicly Trusted S/MIME validating authority over mailbox via domain

Telia CA validates authority in accordance with the BR.

#### 3.2.2.2 Publicly Trusted S/MIME validating control over email

Telia CA validates authority in accordance with the BR.

#### 3.2.2.3 Publicly Trusted S/MIME validating applicant as operator of associated mail server(s)

NOT used by Telia CA.

#### 3.2.2.4 CAA records

No stipulation.

### 3.2.3 Authentication of organization identity

Telia verifies the organisation identity of the Applicant through a validation process.

#### 3.2.3.1 Publicly Trusted S/MIME attribute collection of organization identity

Applicable for S/MIME Certificates issued under Sponsor-validated profile.

Telia CA or RA SHALL collect and retain evidence supporting the following identity attributes for the Organization and to be included in the Certificate subject:organizationIdentifier:

1. Formal name of the Legal Entity
2. A registered Assumed Name for the Legal Entity (if included in the Subject)
3. An organizational unit of the Legal Entity (if included in the Subject)
4. An address of the Legal Entity (if included in the Subject)
5. Jurisdiction of Incorporation or Registration of the Legal Entity
6. Unique identifier and type of identifier for the Legal Entity

#### 3.2.3.2 Publicly Trusted S/MIME validation of organization identity

Applicable for S/MIME Certificates issued under Sponsor-validated profile.

##### 3.2.3.2.1 Verification of name, address, and unique identifier

Telia CA or RA verifies the information by one of the following methods:

1. Information verified from the Reliable Data Source disclosed in 3.2.3.3
2. From attestation verified and confirmed in accordance with 3.2.8

The same documentation or communication MAY be used to verify both the Applicant's identity and address.

##### 3.2.3.2.2 Verification of assumed name

Telia CA or RA verifies the validity of assumed name from the following sources:

1. Information verified from the Reliable Data Source disclosed in 3.2.3.3
2. From attestation verified and confirmed in accordance with 3.2.8

If option 1. is used, the assumed name's validity SHALL be verified.

#### 3.2.3.3 Disclosure of verification sources

Applicable for all certificate types governed by this CP/CPS. Telia CA or RA verify organizations unique identifier from the following Telia CA's verified and authorized sources maintained and/or authorized by relevant government agency:

- Bisnode Infotorg.se (SE)
  COM:infotorg.se  https://www.infotorg.se
  This registry is used to check Swedish company details; Account required. This is Web GUI to Bisnode data.
  Data and sources are same for Bisnode and Infotorg.
- Dun & Bradstreet REST API

In Telia countries is trusted based on data source description from Bisnode (BBC Suite – Data Sources) (FI)

Above list of data sources are considered by Telia CA as Reliable Data Sources as defined by the BR.

#### 3.2.3.4 Other certificate types

The Applicant legal name, business identity code, Fully Qualified Domain Name (FQDN), server name, IP address and other relevant organisation information are confirmed from an official business register maintained by an applicable government agency (e.g., ytj.fi in Finland) as disclosed in 3.2.3.3 or by using another trustworthy method. Common variations, tradenames, abbreviations, or suffixes for the name are allowed provided that the new name can be clearly associated with the Subscriber Organisation.

### 3.2.4 Authentication of individual identity

Accepted Individual Identity Attributes for Publicly Trusted S/MIME by Telia CA included in the issued certificates are:

1. Given name(s) and surname(s), which SHALL be current names of the Individual Applicant

#### 3.2.4.1 Publicly Trusted S/MIME attribute collection of individual identity

All identity attribute date is from Enterprise RA records provided by Enterprise RAs contracted by Telia CA and accepted as verified evidence of Individual Identities by Telia CA.

Enterprise RAs SHALL maintain records in accordance with the BR requirements and policies and practices required by section 1.3.2 and 8.8 of the respective documents.

#### 3.2.4.2 Publicly Trusted S/MIME validation of individual identity

All individual identity data is provided by Enterprise RA.

#### 3.2.4.3 Short-lived certificates

For the short-lived certificates the Delegated third party does not do the identity verification process because Subject's identity is verified by trusted national identity sources, currently Swedish BankID.

#### 3.2.4.4 Other certificate types

In scenarios where Subscriber acts as the role of Enterprise RA, the Subscriber shall comply with the following in addition to the Subscriber obligations, when registering, renewing or rekeying:

a. Verify the identity of the Subject for certificate application
b. Ensure that the Subject is authorized to apply for a certificate
c. Verify the authenticity of the information given for the certificate application Especially verify that common names, domain names, IP addresses and

organisation names and all other attributes used in certificate subjects are correct and belong to the subject

d. Ensure that the Subject is unique in the Subscriber's organisation
e. When the name of the Subject in the certificate is represented by a pseudonym, ensure that the genuine identity of the Subject is known at least throughout the validity period of the certificate
f. Submit the certificate request or the information for certificate application to the CA according to the instructions provided
g. When the Subject's key pair has been generated by the Subscriber or the Subject, ensure that the certificate request is signed by using the private key of the key pair where the public key is the one requested to be certified. Ensure that the key quality is adequate according to the applicable CP/CPS
h. Use the registration tools supplied by Telia only according to the instructions provided
i. Ensure that the private key and the related PIN code are securely delivered to the rightful Subjects and securely stored

The procedures to authenticate the identity of the Subject varies between the different Telia certificate services:

| | |
|---|---|
| **TeliaSonera Class 1 CA v2**<br><br>**Telia Class 1 CA v3** | Telia or Subscriber that acts as RA is responsible for authenticating the Subject data according to Organisation's internal policies. Subject authentication is typically based on a previously recorded ownership of the Customer's email address, device, or mobile phone number.<br><br>If Common Name or dnsName field of Subject Alternative Name includes domain names, Telia confirms Applicant's control over the domain either by using domain validation methods documented in Telia's Server Certificate CPS section 3.2.2 or Telia verifies that Applicant is able to receive and use random code delivered to the email address in the certificate.<br><br>Telia verifies the ownership of an email address by sending a one-time-password to the applied email-address. Then the Subject entity must use the password within a limited time frame to prove the access to the email-address. In Enterprise RA cases email address can be taken from a reliable internal source of the Subscriber without additional verification by one-time-password.<br><br>If CA API connection is used CA will pre-approve all allowed domain names and O values that can be used in Subscriber Subject data. |
| **TeliaSonera Class 2 CA v2**<br><br>**Telia Class 2 CA v3** | Telia Registration Officer or the Subscriber that acts as RA is responsible for authenticating the Subject. The Registration Officers are obliged to follow the policies and instructions given by the CA.<br><br>The Registration Officer should use Organisation's previously recorded directories, databases or other similar information on Organisation's employees, partners, or devices to verify the Subject information, Or the Registration Officer should verify the information by checking the Subject's identity card.<br><br>Registration Officer is responsible for validating the local-part of email address.<br><br>Telia CA validates domains used in email addresses. |

| | |
|---|---|
| **TeliaSonera Email CA v4**<br><br>**Telia Email CA v5** | Certificates are issued to employees within the Telia Group and individuals contracted by Telia. The Subscriber is authenticated using a username and password and information stored in Telia's directories or databases. |
| **Telia Class 3 CA v1** | External RAs that have partnership with Telia verify the following Subject information as described in section 3.2.3:<br>- givenName (G)<br>- surName (S)<br>- commonName (CN)<br>- Serial Number |
| **Ericsson NL Individual CA v3**<br><br>**Ericsson NL Individual CA v4** | Subscriber acts as the role of RA within the Subscriber Organisation and to register certificates for the persons or client devices related to the organisation.<br><br>The Subscriber is responsible for authenticating the Subject. The Registration Officers are obliged to follow the policies and instructions given by the CA.<br><br>The Subscriber should use Organisation's previously recorded directories, databases or other similar information on Organisation's employees, partners, or devices to verify the Subject information, or the Registration Officer should verify the information by checking the Subject's identity card.<br><br>Registration Officer is responsible for validating the local-part of email address.<br><br>Telia CA validates domains used in email addresses. |

## Telia verifies following Subject information:

| | |
|---|---|
| **TeliaSonera Class 1 CA v2**<br><br>**Telia Class 1 CA v3** | Telia verifies Organization Name (O), email address ownership and public domain name information as described in sections 3.2.2 and 3.2.3. The Subscriber that acts as RA role is responsible for verifying the other subject information according to the Subscriber's internal policy.<br><br>Telia does not verify other information within the certificate request. |
| **TeliaSonera Class 2 CA v2**<br><br>**Telia Class 2 CA v3** | Telia verifies Organization Name (O) information as described in section 3.2.2.<br><br>Telia Registration Officer or the Subscriber that acts RA is required to verify the following Subject information as described in section 3.2.3:<br>- commonName (CN)<br>If surName (S) and givenName (G) attributes are used, then the Registration Officer verifies those attributes.<br><br>If emailAddress (EA) attribute or Subject Alternative Name extension contain emailAddress then the Registration Officer verifies local-part of the emailAddress.<br><br>Telia CA validates domains used in email addresses.<br><br>Other information is not verified by Telia or Subscriber Organisation. |
| **TeliaSonera Email CA v4** | Telia verifies the following Subject information as described in section 3.2.3:<br>- commonName (CN) |

| | |
|---|---|
| **Telia Email CA v5** | - emailAddress (EA)<br>- serialNumber<br>- Organization Name (O)<br>Telia does not use other subscriber information within the certificate request. |
| **Telia Class 3 CA v1** | External RAs that have partnership with Telia verify the following Subject information as described in section 3.2.3:<br>- givenName (G)<br>- surName (S)<br>- commonName (CN)<br>- Serial Number |
| **Ericsson NL Individual CA v3**<br>**Ericsson NL Individual CA v4** | Telia verifies Organization Name (O) information as described in section 3.2.2.<br>The Subscriber that acts as RA is required to verify the following Subject information as described in section 3.2.3:<br>- commonName (CN)<br>If surName (S) and givenName (G) attributes are used, then the Subscriber RA verifies those attributes.<br>If emailAddress (EA) attribute or Subject Alternative Name extension contain emailAddress then the Subscriber RA verifies local-part of the emailAddress.<br>Telia CA validates domains used in email addresses.<br>Other information is not verified by Telia or Subscriber Organisation. |

### 3.2.5 Non-verified Subscriber information

For the issuance of Publicly Trusted S/MIME Certificates after the 1st of September 2023 by Telia CA, only the Subject information verified in accordance with the BR and this CP/CPS SHALL be included in the Certificate.

### 3.2.6 Validation of authority

The Subscriber Organisation can agree with Telia to act as a Registration Authority (Enterprise RA) within the Subscriber Organisation and to register certificates for the persons or client devices related to the organisation and assign responsibilities to others to act in these roles for the organization.

The Subscriber Registration Officer is restricted to register certificates only within their own Organizations (O). Before authorizing the Enterprise RA, Telia CA verifies the organisation's identity as described in section 3.2.3.

Telia verifies that the Subscriber application for a hosted CA has been authorised.

| | |
|---|---|
| **TeliaSonera Class 1 CA v2**<br>**Telia Class 1 CA v3** | The Administrative Contact Person, who grants the necessary authorisations in the Subscriber Organisation, has been identified in the service agreement or order or in Appendix of them. In most cases, Telia validates the initial authority by calling the contact person via the verified Subscriber's PBX number or by making a call to some other verified number in the organisation, which is looked up from a directory |

| | |
|---|---|
| **TeliaSonera Class 2 CA v2**<br><br>**Telia Class 2 CA v3**<br><br>**Ericsson NL Individual CA v3**<br><br>**Ericsson NL Individual CA v4** | maintained by a trusted party. Role of Administrative Contact person can be re-validated later by Telia using the same method if the originally validated persons are unavailable or not known.<br><br>Initially authorised Administrative Contact Person may authorise new administrative contact persons or Registration Officers by delivering to Telia an authorisation in writing or by email. In certain services, he/she can do this by authenticating to the self-service tool provided by Telia and using it for authorisations. All authenticated administrative Contact persons can use the self-service tool or order process to check or modify authorisations within the Subscriber.<br><br>When registering Subjects, the identity and authority of the Registration Officer is verified by means of his certificate issued by Telia, or from his signature on the certificate order form, or using other comparable methods approved by the CA. |
| **TeliaSonera Email CA v4**<br><br>**Telia Email CA v5** | The registration system verifies from Telia's internal directories that the subscriber is a current employee within the Telia Group, or an individual contracted by Telia. |
| **Telia Class 3 CA v1** | Telia ensures verification of the identities using trusted identity sources (e.g. Swedish Bank ID). |

### 3.2.7 Criteria for interoperation

Telia CA has disclosed all Cross-Certified Subordinate CA Certificates in this CP/CPS and relevant public repositories and databases.

Telia CA shall not issue Cross-Certified Subordinate CA Certificates operated under this CP/CPS to external parties.

### 3.2.8 Reliability of verification sources

Telia CA verifies at least on annual basis the Reliable Data Sources validity. Validity is verified by Telia CA designated Trusted Role person by requesting and validating official written documentation of the data source(s) from the data source supplier.

Subject information MAY be verified by CA or RA with and official Attestation letter. Attestation letter (and any additional supporting documentation) supporting the fact to be attested is accepted from independent accountant and/or lawyer or from government official.

Attestation SHALL be accepted only in writing and SHALL be verified via Reliable Method of Communication for authenticity by contacting the sender for confirmation.

## 3.3 Identification and authentication for re-key requests

### 3.3.1 Identification and authentication for routine re-key

Re-keying requests can be automatically accepted without strong authentication if the subject information remains the same (e.g., one-time-password can be sent to the same mobile phone and/or email address again to re-new the subject's existing certificate).

If there are changes in the Subject or certificate delivery information the request will be validated in the same way as at initial registration.

### 3.3.2 Identification and authentication for re-key after revocation

In accordance with 3.3.1.

## 3.4 Identification and authentication for revocation request

### 3.4.1 Revocation by Subscriber Organisation

Subscriber's self-service revocation can be activated by the Subject or the Subscriber. The revocation request can be submitted to Telia by the Subject directly or via the Revocation Officer of the Subscriber Organisation. In the latter case The Revocation Officer is responsible for the verification of the authenticity and authorisation of the request. Telia verifies the identity of the Subject or the Revocation Officer with a certificate, one-time-password scheme or other reliable method.

In scenarios that Subscriber acts as RA, a revocation shall be done for the followings:

a. Upon suspected or known compromise of the private key
b. Upon suspected or known compromise of the media holding the private key
c. Subject or subscriber information is known to be invalid or re-verification fails
d. When there is an essential error in the certificate
e. When any information in the certificate changes
f. Upon termination of a Subject or when a Subject no longer needs certificates
g. When the certificate is redundant (for example, a duplicate certificate has been issued)
h. Subscriber's certificate contract with Telia has ended
i. Any other reason that makes the certificate obsolete or threats related keys

Revocation can be performed directly by the Subscriber or a notification for revocation may be given to Telia's Revocation Service.

### 3.4.2 Revocation by the Revocation Service of the CA

The Subject, or Subscriber, or Subscriber that acts as RA shall submit a request for certificate revocation to the Revocation Service by telephone or by e-mail. The source of the revocation request will be authenticated based on the S/MIME digital signature or the Revocation Service will make a call back to the Subscriber and asks certain detailed data. This data is compared with the information recorded about the Subject at registration, and if necessary, with information in the agreements made with the Subscriber or with the

Subscriber. If the data match the certificate will be revoked. The Revocation Service is responsible for the verification of the authenticity and authorisation of the request to revoke the certificate.

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 at the 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.

### 3.4.3 Revocation of CAs

The authorised CA personnel can request revocation of a CA certificate. Authorised Subscriber contact person can request revocation of that Subscriber's CA certificate. The Policy Management Team in the CA is responsible for the verification of the authenticity and authorisation of the request to revoke the certificate.

Subscriber contact person requesting revocation is authenticated by call-back to the Subscriber or by other means that the CA determines necessary to reliably authenticate the person requesting the revocation. The method and information that has been used for verification of the identity of the person requesting revocation, and the revocation request reception time, will be recorded.

Multi-factor authentication mechanisms are used to authenticate users to CA system. Multiple Trusted Roles of CA are required to gain access to revoke a CA certificate in the CA system.

### 3.4.4 Reinstatement of suspended certificate

Telia CA does not support suspension.

# 4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

## 4.1 Certificate Application

### 4.1.1 Who can submit a certificate application

#### 4.1.1.1 CAs

A CA certificate application can be submitted by an authorised Telia CA employee or an authorised representative of the Subscriber that has made an agreement to host their CA at Telia.

#### 4.1.1.2 Client Certificates

| | |
|---|---|
| **TeliaSonera Class 1 CA v2**<br>**Telia Class 1 CA v3**<br>**TeliaSonera Class 2 CA v2**<br>**Telia Class 2 CA v3**<br>**Ericsson NL Individual CA v3**<br>**Ericsson NL Individual CA v4** | When a certificate is requested for a person or Device, it is required that the ordering organisation is a Subscriber of Telia with which the Subject has a contractual relation.<br><br>Certificate request can be submitted by<br>a. A Subscriber that acts as RA<br>b. An employee or other individual contracted by a Customer Organisation (Subject)<br>c. An administrative contact person of a Subscriber Organisation |
| **TeliaSonera Email CA v4**<br>**Telia Email CA v5** | Certificate application can be submitted by an employee within the Telia Group, or an individual contracted by Telia. |
| **Telia Class 3 CA v1** | Anyone who is pre-registered in the External RA databases to use the certificate services. |

Authorised Telia personnel can also submit certificate applications.

### 4.1.2 Enrolment process and responsibilities

A Subscriber that has agreed to and executed an Agreement with Telia can have a hosted CA at the Telia CA. In the Agreement, the Subscriber is bound to this CPS, the CPS of the subordinate CA being enrolled and other terms and conditions.

During the enrolment process a new CPS is prepared for the subordinate CA unless the new CA can use an existing CPS, in which case the existing CPS is reviewed and required changes are made.

The certificate application is included in the CA hosting agreement. In all cases the final application is made and signed by an authorised Telia CA employee. Telia CA Installation Form document is used for the final application.

Multiple Trusted Roles of CA are required to enrol a new CA certificate based on the data in the final application. Actual enrolment process is documented in Telia CA Operational Documentation.

#### 4.1.2.1 CAs

The application is made and signed by an authorised Telia CA employee. Telia CA Installation Form document is used for such applications.

#### 4.1.2.2 Subscriber certificates

| | |
|---|---|
| **TeliaSonera Class 1 CA v2**<br><br>**Telia Class 1 CA v3**<br><br>**TeliaSonera Class 2 CA v2**<br><br>**Telia Class 2 CA v3**<br><br>**Ericsson NL Individual CA v3**<br><br>**Ericsson NL Individual CA v4** | Certificates can be applied for either through the RA office of the CA or directly from the CA system by using the tools supplied by the CA.<br><br>a. Subscriber that acts as RA pre-registers the Subject using self-service software provided by Telia and applies for a certificate to the Subject or the Subject can, after pre-registration, initiate the application for a certificate by using the one-time password sent to him/her. The Subject uses the one-time-password to authenticate to the registration tool. The Subscriber or the Subject generates the key pair and submits the certificate request to the CA system containing the certificate information defined by the Subscriber during the pre-registration and the public key.<br><br>b. The Subject initiates the enrolment process by submitting a certificate application using self-service software provided by Telia. The Subject generates the key pair and submits the certificate request containing the certificate information. The Subscriber verifies the information in the request and sends the Subject a link to pick up the issued certificate.<br><br>c. The self-service software provided by Telia is integrated with the existing authentication solution at the Subscriber site. The subject uses the user credentials in the Subscriber organisations authentication solution to enrol for a certificate (applicable to **Ericsson NL Individual CA v3 and Ericsson NL Individual CA v4**).<br><br>d. Certificate is applied for through the RA office of the CA. The Subscriber or Administrative contact person sends a manually or electronically signed order that contains the necessary information for the certificate there. At the RA office of the CA the signature is checked, the sufficiency of information given for the certificate is examined, and the Subject is pre-registered. The actual certificate request to the CA system can be initiated by the RA office of the CA, or alternatively the necessary instructions and one-time password for the certificate request can be delivered, according to the order, either directly to the Subject or to the Subscriber.<br><br>The Subscriber Organisation is bound to registration policies and Subscriber responsibilities through a certification service agreement with Telia. Subscriber Organisation's Registration Officers also accept Subscriber Responsibilities when they logon to Telia's self-service application first time. |
| **TeliaSonera Email CA v4**<br><br>**Telia Email CA v5** | The Subscriber fills the application form available in Telia's intranet. After a successful authentication, the registration system obtains Subject information from Telia directories and registers the certificate based on this information. |
| **Telia Class 3 CA v1** | 1. User will receive an email with a link from signing portal.<br>2. User will click on the link and will then have to be to be authenticated (e.g. Swedish Bank ID[1]).<br>3. User information will be sent for certificate request to Telia CA from the external partner using API including Subscriber information (givenName, surname, commonName) taken from a valid identity provider (e.g. Swedish Bank ID).<br>4. Telia will issue a certificate with short validity.<br>5. Issued certificate will be used in signing operation and it will be deleted immediately afterwards. |

[1] Swedish Bank ID: https://www.bankid.com/en/

## 4.2 Certificate application processing

### 4.2.1 Performing identification and authentication functions

Identification and authentication of Subject and Subscriber information is performed in accordance with the section 3.2.

#### 4.2.1.1 Reuse of completed validations for Publicly Trusted S/MIME issuance

Telia CA MAY reuse previously completed validations within following limits:

1. Validation of mailbox authorization or control
    a. 398 days from previous validation completed in accordance with 3.2.2.1 or 3.2.2.3
    b. Complete validation of control of a mailbox in accordance with 3.2.2.2 SHALL be obtained at earliest 30 days prior of issuance of the Certificate.
2. Authentication of organization identity
    a. Complete validation of organization identity in accordance with 3.2.3 SHALL be obtained at earliest 825 days prior of issuance of the Certificate.
    b. Validation of authority in accordance with 3.2.6 SHALL be obtained at earliest 825 days prior issuance of the Certificate or in accordance with agreed time limit in contract between Telia CA and the Applicant.
3. Authentication of individual identity
    a. Complete validation of Individual identity in accordance with 3.2.2.4 SHALL be obtained at earliest 825 days prior issuance of the Certificate.

Prior validation data and/or document SHALL NOT be used outside the said time limits in this section.

### 4.2.2 Approval or rejection of certificate applications

Telia will approve a certificate application if it meets the requirements of validation and identification. 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.

For CA's approvals, PMT approves or rejects CA applications.

### 4.2.3 Time to process certificate applications

Telia will process the applications for CAs within reasonable time frame.

When a certificate is applied for directly from the CA system by the tools provided by the CA, the certificate request is processed automatically by Telia's RA and CA systems immediately after the request is submitted.

When a certificate is applied for through the RA office of the CA, Telia process the applications within reasonable time frame. There are no specific requirements for the processing time unless otherwise agreed with the Subscriber.

## 4.3 Certificate issuance

### 4.3.1 CA actions during certificate issuance

If the certificate application is approved by the Registration Officer, the CA issues the certificate. The certificate is created by the CA according to the information contained in the certificate request. However, the CA may overwrite some certificate information using pre-defined certificate profile specific standard values.

### 4.3.2 Notification to Subscriber by the CA of issuance of certificate

#### 4.3.2.1 CA certificate issuance

If the certificate application is approved, the CA generates the root or subordinate CA key pair and issues the certificate. Two trusted Certification Authority Administrators together are required to execute the CA key generation and certificate issuance in the CA system.

The certificate is created by the CA according to the information contained in the final certificate application.

#### 4.3.2.2 Subscriber certificate issuance

| | |
|---|---|
| **TeliaSonera Class 1 CA v2**<br>**Telia Class 1 CA v3**<br>**TeliaSonera Class 2 CA v2**<br>**Telia Class 2 CA v3**<br>**Ericsson NL Individual CA v3**<br>**Ericsson NL Individual CA v4** | The certificate is available for the Subscriber acting as RA or for the Subject in the registration tool after the issuance. |
| **TeliaSonera Email CA v4**<br>**Telia Email CA v5** | The certificate is made available for download in PKCS#12 format by the Subject during the registration process after it has been issued by the CA. |
| **Telia Class 3 CA v1** | Subscribers will not receive any notification about issuance of the certificates. They will receive a link from the External RA to sign a document. |

## 4.4 Certificate acceptance

By accepting a certificate, the Subscriber:

I. Agrees with the continuing responsibilities, obligations and duties required by Telia CA,
II. Agrees to the Telia CA Subscriber Agreement and Terms of Use,
III. Represents and warrants that no unauthorised access to the private key associated with the certificate is allowed,
IV. Represents and warrants that the provided information during the registration

process is truthful and accurate, and

V. Review and verify the certificate contents for accuracy, completeness and the certificate is not damaged or corrupted.

Note: When a certificate is inaccurate, damaged, or corrupted (violation of item V above), the Subscriber should inform the CA.

### 4.4.1 Conduct constituting certificate acceptance

The Subscriber is considered to have accepted the certificate when:

- The Subscriber start using the certificate's key pair, or
- One calendar month is passed from the certificate issuance date.

### 4.4.2 Publication of the certificate by the CA

CA certificates are published in the CA repository in accordance with the section 2.1.3.

Telia will not publish subscriber certificates to a publicly available repository if not agreed upon with the Subscriber Organisation.

### 4.4.3 Notification of certificate issuance by the CA to other entities

All publicly trusted CA certificates are published to CCADB database at https://ccadb.force.com prior CA certificate is used for issuance of certificates.

There are no external notifications related to the issuance process of End-Entity certificates.

## 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. If the private key is compromised the Subscriber shall discontinue the use of the Subject private key immediately and permanently and request for the revocation of the certificate.

### 4.5.2 Relying party public key and certificate usage

Prior to accepting a Telia 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, e.g., verify the validity dates and the validity of the certificate and issuance signatures

c. Verify from a valid CRL or other certificate status service provided by the CA that the certificate has not been revoked or suspended. If certificate status cannot be verified due to system failure or similar, the certificates shall not be accepted

## 4.6 Certificate renewal

Certificate renewal is the re-issuance of a certificate with a new validity date using the same public key corresponding to the same private key. Normally a new key pair is generated when a certificate is renewed and Telia prefers that the certificates are re-keyed instead of renewing them using the existing key pair. However, it is possible that Subscriber uses existing key pairs instead of generating new public and private keys.

Certificate renewal requests are processed as certificate re-keys as described in section 4.7.

Telia CA will not renew short-lived personal certificates. Subordinate CA certificates may be renewed if the validity time of the Subordinate CA certificate does not exceed the expiration date of the root CA.

## 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 as before.

### 4.7.1 Circumstance for certificate re-key

When the validity time of a certificate is about to end, the certificate can be re-keyed. Also, technical problems in certificate installation or in certificate storage may trigger re-keying.

The short-lived personal certificates will be issued per request by the External RA and will not be re-keyed.

### 4.7.2 Who may request certification of a new public key

Re-key may be requested by the same persons as the initial certificate application as described in section 4.1.1. If the Subject has technical problems with the certificate or he/she has lost the certificate, the Subject may also request a new certificate from Telia's Subscriber Service.

### 4.7.3 Processing certificate re-keying requests

| | |
|---|---|
| **TeliaSonera Class 1 CA v2**<br>**Telia Class 1 CA v3**<br>**TeliaSonera Class 2 CA v2**<br>**Telia Class 2 CA v3**<br>**Ericsson NL Individual CA v3**<br>**Ericsson NL Individual CA v4** | If the certificate re-key is started by the acting as the RA role, it is his/her responsibility to ensure that there are no obstacles to the re-key. If there are changes in the Subject information or in the certificate delivery information those shall be checked in the same way as at initial registration. A re-keyed certificate is issued and delivered in the same way as the initial certificate as described in section 4.1 – 4.4.<br><br>If the certificate re-key is processed by the Customer Service of the CA or other authorised CA personnel, they ensure that the original usage purpose for the certificate still exists. Then they use the information from the initial certificate request authorised by the Registration Officer and deliver the one-time password to the Subject using the existing contact information stored in the registration system. The Subject can then use the one-time password to initiate the application for a certificate. |
| **TeliaSonera Email CA v4**<br>**Telia Email CA v5** | Re-key is processed in the same way as the initial certificate application as described in section 4.1 – 4.4. |

| | |
|---|---|
| **Telia Class 3 CA v1** | |

### 4.7.4 Notification of new certificate issuance to subscriber
Subscriber is notified in the same ways when the certificate is issued first time as described in section 4.3.2.

### 4.7.5 Conduct constituting acceptance of a re-keyed certificate
Conduct constituting acceptance of a re-keyed certificate is described in section 4.4.1.

### 4.7.6 Publication of the re-keyed certificate by the CA
Re-keyed certificates are published like initial certificates 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). Certificate modification requests are processed as initial certificate requests as described in sections 4.1 – 4.4.

Certificate subject or extension modification is possible within certificate renewal process which is covered in section 4.6.

## 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 is updated, and operational period of that Certificate is immediately considered terminated.

### 4.9.1 Circumstances for revocation
Telia CA will revoke a Subordinate CA certificate within seven (7) days if one or more of the following occurs:

1. The Subordinate CA requests revocation by trustworthy means of communication (written request, phone call etc.)
2. The Subordinate CA notifies the Telia CA that the original certificate request was not authorised and does not retroactively grant authorisation
3. The Telia CA obtains evidence that the Subordinate CA's private key corresponding to the public key in the certificate suffered a key compromise or no longer complies with the Baseline Requirements of Sections 6.1.5 and 6.1.6
4. Telia CA obtains evidence that the certificate was misused
5. Telia CA is made aware that the certificate was not issued in accordance with, or that Subordinate CA has not complied with this document or the applicable CPS
6. Telia CA determines that any of the information appearing in the certificate is inaccurate or misleading

7. Telia CA or Subordinate CA ceases operations for any reason and has not made arrangements with another CA to provide revocation support for the certificate
8. Telia CA's or Subordinate CA's right to issue certificates under the Baseline Requirements expires or is revoked or terminated, unless the Telia CA has made arrangements with another CA to continue maintaining the CRL/OCSP Repository
9. Revocation is required by the Telia CA's CPS

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 authorisation
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 authorisation or control for any Fully Qualified Domain Name (FQDN) or IP address in the Certificate should not be relied upon
5. 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

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

1. The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;
2. The CA obtains evidence that the Certificate was misused;
3. The 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. The CA is made aware of any circumstance indicating that use of a Fully Qualified Domain Name 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. The CA is made aware of a material change in the information contained in the Certificate;
6. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the applicable CP/CPS;
7. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate;
8. The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by the applicable CP/CPS; or
10. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise 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 Subject whose name the certificate is issued under
2. A Subscriber or Subscriber that acts as RA that has made an application for a certificate on behalf of an organisation, device or application
3. Personnel of Telia CA
4. An authorised representative of the Subscriber hosting their CA at Telia

### 4.9.3 Procedure for revocation request

For CA revocation, Telia CA identifies and authenticates the originator of a revocation request according to section 3.4. The PMT approves revocation requests. The certificate is permanently revoked after the approval.

The Subject, and where applicable the Subscriber, of a revoked certificate, where possible, will be informed of the change of status of the certificate. If the request cannot be confirmed within 24 hours then the status will not be changed.

When making a revocation request as above, Telia's CA system checks that the digital signature on the revocation request is valid and that the person signing the revocation request is authorised to do so. If both these criteria are met, the certificate in question is revoked.

A revocation request may be received by Telia in one of the following ways:

a. Subscriber acting as RA makes the revocation request using the administration interface

b. The Subject makes the revocation request using a self-administration or re-enrolment interface

c. Revocation may be requested by contacting Telia CA's Revocation Service by telephone or via online channel (see 1.5.2)

If the revocation request cannot be carried out in accordance with a. or b., the Subscriber acting as RA, or the Subject may contact Telia Revocation Service by telephone or email and make a revocation request. Authorised Telia revocation staff, then authenticates the identity of the originator of a revocation request according to section 3.4 and makes the revocation request using Telia's CA system.

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.

### 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 Subject or Subscriber shall as soon as possible inform the Revocation Service directly or the Subscriber that acts as the RA. Also, the Registration Officer shall revoke the certificate using the

administration interface or inform Telia's Revocation Service as soon as possible, when a reason for the revocation of a certificate comes to his/her 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 CRL according to the principles given in this CPS.

### 4.9.5 Time within which CA must process the revocation request

Telia process revocation requests within reasonable time frame. There are no specific requirements for the processing time unless otherwise agreed with the Subscriber.

### 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 against the current CRL's or on-line OCSP. 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 him-/herself of the authenticity and integrity of the CRLs or on-line certificate status 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 and OCSP response in order to make sure that the information in the CRL or OCSP response 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 CRL Revocation Status Service is implemented by publishing CRLs that are digitally signed by the CA and publicly available. The following rules are enforced:

For the CA's

a. A new CRL is published at intervals of not more than twelve months
b. A new CRL is published within 24 hours after revoking a Subordinate CA Certificate
c. The validity time of every CRL is one year

For client certificates:

a. A new CRL is published at intervals of not more than two (2) hours
b. The validity time of a CRL is forty-eight (48) hours
c. The publishing intervals and validity time may also be agreed upon with Telia's Subscriber

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

No stipulation.

### 4.9.9 On-line revocation/status checking availability

Telia may provide on-line revocation status checking via the OCSP protocol.

### 4.9.10 On-line revocation checking requirements

All OCSP responses 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).

The validity interval of an OCSP response is the difference in time between the thisUpdate and nextUpdate field, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day, ignoring leap-seconds.

#### 4.9.10.1Status of Subscriber Certificates

For the status of subscriber certificates following applies:

- OCSP responses have validity interval greater than or equal to eight hours.
- OCSP responses have validity interval less than or equal to ten days.
- For OCSP responses with validity intervals less than sixteen hours, the information provided via an Online Certificate Status Protocol, will be one-half of the validity period before the nextUpdate.
- For OCSP responses with validity intervals greater than or equal to sixteen hours, the information provided via an Online Certificate Status Protocol, shall be at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.

#### 4.9.10.2 Status of Subordinate CA Certificates

For the status of subordinate CA certificates following applies:

- The CA SHALL update information provided via an Online Certificate Status Protocol
    - At least every twelve months.
    - Within 24 hours after revoking a Subordinate CA Certificate.

#### 4.9.10.3 Other information

OCSP responder will respond with an "unknown" status for certificate status request for a certificate serial number that is “unused”, thus do not exist in the CA database.

For Telia CA OCSP service, a certificate serial number within an OCSP request is one of the following three options:

1. “assigned” if a Certificate with that serial number has been issued by the Issuing CA, using any current or previous key associated with that CA subject.

2. “reserved” if a Precertificate [RFC6962] with that serial number has been issued by the Issuing CA.

“unused” if neither of the previous conditions are met.

### 4.9.11 Other forms of revocation advertisements available

Not applicable.

### 4.9.12 Special requirements regarding key compromise

In case of CA private key compromise, the procedures defined in section 5.7.3 are followed.

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.

For short-lived personal certificate’s key compromise, External RA will notify immediately the potential Relying Parties, CA and Subscribers.

The key compromise cases shall be reported to Telia CA instantly by Subscriber or any other parties or participants. The report shall include supporting information such as the CSR that was signed by the compromised private key, the actual private key or a valid email address that can be used for further communication regarding the revocation of the corresponding certificate compromised key.

### 4.9.13 Circumstances for suspension

Telia CA does not support suspension.

### 4.9.14 Who can request suspension

Telia CA does not support suspension.

### 4.9.15 Procedure for suspension request

Telia CA does not support suspension.

### 4.9.16 Limits on suspension period

Telia CA does not support suspension.

## 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. Telia CA ensures integrity and authenticity of the status information using strong security mechanisms. CRLs are digitally signed using the CA's private key. OCSP response is digitally signed by the OCSP response 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.

## 4.11 End of subscription

The end of a subscription because of no longer requiring the service, compromise or breach of contract result in the termination of the CA as described in section 5.8.

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

## 4.12Key escrow and recovery

### 4.12.1Key escrow and recovery policy and practices

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

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

A Subscriber's confidentiality private keys will not be escrowed but Telia may keep a backup of the keys if agreed between Telia and the Subscriber. The keys are protected in an encrypted form and are protected at a level no lower than stipulated for the primary versions of the keys. The decryption key used to decrypt the key backups is stored in an HSM and the key backups are saved for a period that is agreed with the Subscriber.

A private key may be recovered for two separate reasons:

a. The hard disc, the Smart Card or equivalent that holds the Subscriber's private key is corrupted and the Subscriber needs to make a recovery of his key. The process of authenticating the Subscriber is the same as at the initial certificate issuance. When a private key has recovered the certificate for the corresponding public key is automatically revoked, a new key pair is created, and a new certificate is issued
b. The Subscriber is for some reason prevented from using his private key (the Subscriber may, for instance, be deceased, injured or has left the organisation) and Subscriber's Organisation needs to decrypt data encrypted by the Subscriber. The process of such key recovery involves at least two (2) persons from the Subscribers' organisation or at least two (2) persons from the CA organisation where all are authenticated by certificates. When a private key has recovered the certificate for the corresponding public key is automatically revoked

For short-lived personal certificates there will be no key-escrow or recovery.

### 4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

# 5 FACILITIES, MANAGEMENT, AND OPERATIONAL CONTROLS

Telia CA has implemented continuously maintained Security Program in accordance with Telia Company policies, processes, and procedures including built-in Risk Assessment program.

Telia CA's Security Program is designed to address (but not necessarily limited to):

- Protection of the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes.
- Protection against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes.
- Protection against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes.
- Protection against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes
- Compliance with all other security requirements applicable to the CA by law.
- Risk assessment program
    - to identify foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes.
    - to assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes
    - to assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

Based on the Risk Assessment, Telia CA develop, implement, and maintain a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes.

The security plan includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes.

Within the security plan Telia CA considers and take account of then-available technology and the cost of implementing the specific measures and implement a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

Telia CA incorporates the CA/Browser Forum's Network and Certificate System Security Requirements by reference as if fully set forth herein.

## 5.1 Physical controls

### 5.1.1 Site location and construction

Telia's CA and RA operations are conducted within Telia's premises in Finland and Sweden.

All Telia CA and RA operations are conducted within a physically protected environment designed to deter, prevent, and detect covert or overt penetration.

#### 5.1.1.1 CA Site location and construction

The premises where central CA functions take place are physically located in a highly secure server rooms dedicated for CA operations. The physical protection of which corresponds at least with the requirements for "priority 1 premises" defined in the regulation on priority rating, redundancy, power supply and physical protection of communications networks and services (TRAFICOM/54045/03.04.05.00/2020) issued by TRAFICOM (Finnish Transport and Communications Agency). Within these server rooms, key components are locked in separate, freestanding security cabinets.

Telia CA operates two distinct sites in Finland. In addition to what is said above, one (1) of the facilities is meeting structural specifications of KATAKRI Level III for Secure Areas.

The server rooms, which are locked and alarmed, are in secure buildings, which are also locked and alarmed. These are protected jointly by using active monitoring.

#### 5.1.1.2 RA Site location and construction

The premises where central RA functions take place are physically located in highly secure server rooms.

Within these server rooms, key components are locked in separate, freestanding security cabinets. The server rooms, which are locked and alarmed, are in secure buildings, which are also locked and alarmed. These are protected jointly by using active monitoring.

Certain RA functions comprising roles in accordance with section 5.2.1 may be carried out outside the physical environment of the protected premises detailed above. These are:

a. Identification on application of key holders who are present in person
b. Issuing keys and codes
c. Identifying key holders and ownership of the correct private key on electronic application
d. Electronic registration of key holders
e. Revocation service for revoking certificates

Functions in accordance with a) do not involve any access to the central RA system. This environment therefore has no specific security provisions in terms of physical security.

Functions in accordance with b) to e) are carried out in well controlled office environments where access is restricted to authorised personnel.

In the case where the CA is a Subscriber's CA, the stipulations above for physical protection of the locality for RA functions may not be followed.

### 5.1.2 Physical access

For security reasons, detailed information on security procedures for physical access to the premises is not publicly available but is described in the Telia Operational Documentation. The security procedures are described in separate documentations belonging to the Telia CA Services.

The physical locations, sites and premises are under 24/7 surveillance and monitoring by on call site security.

Authorized Trusted Role personnel may access CA and RA sites and servers unescorted based on pre-approved and authorized access lists. Unauthorized visitors will be escorted by authorized personnel and supervised during their work.

Site access is logged and monitored. Access logs are inspected at least quarterly by qualified personnel. The inspection documentation is retained for at least a one-year period to support audit requirements.

Access control and monitoring systems are secured by uninterruptible power supply systems (UPS).

UPS system undergoes annual inspection and disaster recovery testing by site operator, and the inspection documentation is retained for at least a one-year period.

#### 5.1.2.1 CA Site Physical access

Telia CA facilities are protected at least five (5) tiers of distinctive physical security layers where the CA systems and other important CA devices have been placed in a security vault. Protection and controls are progressively restrictive from tier to tier.

The detailed implementation of controls and mechanisms applied for access control and monitoring is classified as confidential information and documented in separate Telia CA documentation and made available on need-to-know basis only.

#### 5.1.2.2 RA Site Physical access

The Telia RA systems are protected at least four (4) tiers of distinctive physical security layers. Protection and controls are progressively restrictive from tier to tier. The detailed implementation of controls and mechanisms applied for access control and monitoring is classified as confidential information and documented in separate Telia CA documentation and made available on need-to-know basis only.

### 5.1.3 Power and air conditioning

Telia locations are equipped with required establishments as expressed in section 5.1.1.1 for structural site requirement specification.

### 5.1.4 Water exposures

Telia locations are equipped with required establishments as expressed in section 5.1.1.1 for structural site requirement specification

.

### 5.1.5 Fire prevention and protection

Telia locations are equipped with required establishments as expressed in section 5.1.1.1 for structural site requirement specification.

### 5.1.6 Media storage

All media containing production software and data, audit, archive, or backup information is stored within the Telia facilities or in a secure off-site storage premises with appropriate physical and logical access controls designed to limit access to authorised personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic).

### 5.1.7 Waste disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or erased in accordance with Telia CA's guideline for secure material decommission. Other waste is disposed of in accordance with Telia's normal waste disposal requirements.

### 5.1.8 Off-site backup

Telia performs daily routine backups of critical system data, audit log data, and other sensitive information. The backups are either daily transported over a secure channel or periodically moved physically to an off-site storage facility.

## 5.2 Procedural controls

Telia is responsible for all procedures and circumstances defined in this section. This includes everything from production and logistics to the administration of the entire process.

Critical CA and RA operations is prohibited from being performed at distance over networks and must be performed locally at the CA and RA sites.

### 5.2.1 Trusted roles

Trusted Roles include all employees, contractors, and consultants that have access to or control authentication, cryptographic operations and information that may materially affect:

a. The administration of CA private keys and RA system private keys
b. Configurations of the CA and central RA systems
c. The validation of information in Certificate Applications
d. The acceptance, rejection, or other processing of Certificate Applications, revocation requests, or renewal requests, or enrolment information
e. The issuance, or revocation of Certificates
f. The handling of Subscriber information or requests

Trusted Roles include, but are not limited to:

a. Subscriber service personnel
b. Cryptographic business operations personnel
c. Security personnel
d. System administration personnel
e. Designated engineering personnel
f. Executives that are designated to manage infrastructural trustworthiness

Telia considers the categories of personnel identified in this section as Trusted Roles

having a Trusted Role. Persons appointed to Trusted Roles by appropriate management authorization, person adopting the Trusted Role must successfully complete the screening requirements of section 5.3 before the Trusted Role is assigned to the person.

Examples of roles defined for CA and RA operations and maintenance are:

#### 5.2.1.1 Certification Authority Administrator (CAA): Administrative production/operational staff for the CA and RA systems.

Typical duties which may be administered by the CAA include:

a. Creating CA certificates
b. Personalising cards
c. Generating CA and central RA keys
d. Configuration of CA and RA applications
e. Generating revocation lists
f. Checking the certificate issue log

#### 5.2.1.2 System Administrator (SA): Technical production/operational staff for the CA and RA systems.

Typical duties which may be administered by the SA include:

a. Installations of hardware and software
b. System maintenance
c. Changing of backup media

#### 5.2.1.3 Security Manager: Overall responsibility for the security of the Telia CA Service.

#### 5.2.1.4 Registration Officer: RA Office and Subscriber Service staff of the CA.

Subscriber RA's Registration Officers are not Trusted Roles. Typical duties of the Registration Officer include processing and approving certificate applications and submitting certificate requests to the CA system that issues and signs the certificates. Registration Officers also create new Subscriber accounts, privileges, and values to enable Telia's self-service software for the Subscriber. More detailed obligations and responsibilities of the Subscriber acting as RA are as below.

a. Authentication of Registration Officers. When the Subscriber is using an application programming interface (API) or Certificate Application supplied by Telia for registration, the Subscriber is responsible for verification of the identity of the Registration Officer using this interface or application. Authentication to registration systems must be done with Multi Factor Authentication (MFA) every time the Certificate Application is used for registration. Systems accessing Telia CA services via API, must use authentication key provided by Telia CA.
b. Security. The Subscriber shall ensure that he manages securely his part of the certificate registration process. The Registration Officer workstations shall be in premises secured with physical access control. Each registration Officer shall use

his securely stored personal credentials. The Subscriber shall ensure that unauthorized persons cannot use the registration privileges.

c. Recording and filing. The Subscriber is responsible for recording and filing the relevant actions, data and documents associated with the certificate application process, and for storing them for as long as the Subscriber acts as a RA and uses certificates issued by Telia CA.
d. Chained responsibilities. The entitled Subscriber's Administrative Contact person shall appoint a Registration Officer for the Subscriber's organisation. The Administrative Contact Person is entitled to appoint new Registration Officers and cancel their rights in the organisation as necessary. All Registration Officers have the right, delegated by the Administrative Contact Person, to make the necessary entries and configurations into the data systems to authorize new Registration Officers. The Administrative Contact Person is obligated to ensure that Registration Officers will be familiarised with their responsibilities and obligations and instructed in their duties as described in this CPS and other related documents and agreements applicable.
e. Confidentiality. The terms concerning confidentiality in Telia´s general delivery terms for business shall apply. The Subscriber shall commit himself to follow the legislation concerning personal data protection in registration as data Processor or Subscriber's personal data in Certificate Application.
f. Inspection rights. Telia is entitled to verify by inspection that the Subscriber fulfils the requirements concerning registration.

### 5.2.2 Number of persons required per task

Telia maintains a policy and rigorous control procedures to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA and central RA cryptographic modules and associated key material, require presence of and/or actions by multiple authorized Trusted Role individuals (Dual Control).

These internal control procedures are designed to ensure that at a minimum, two individuals are required to have either physical or logical access to the device. Access to CA and central RA cryptographic hardware is enforced by Dual Control throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls are invoked to maintain segregation of duties and/or Dual Control over both physical and logical access to the device. Requirements for CA private key activation data is specified in section 6.2.2.

Physical and operational system access to the central CA and RA servers require the participation of at least 2 Trusted Roles that works in conjunction. Either persons work physically together, or the other Trusted Roles is involved via following security controls:

a. Each administrative login or physical access to critical servers or environments is causing alarm to be inspected by security supervisors. If alarm is caused by a

security supervisor only another security supervisor can inspect and accept the alarm
b. Each operation and command entered by operator is logged on the separate log server.
c. All operational remote access to critical systems is done only via secure management hosts.
d. Root/admin privilege of log and management hosts are guarded by persons who have no root access to CA servers. If maintenance to log/maintenance server is required, the normal system operators may get temporary root access from the root guards
e. Critical files and directories are monitored by checksum tests, so they are not modified during operational access. Security supervisors get alarm if modifications are done. If alarm is caused by a security supervisor only another security supervisor can inspect and accept the alarm
f. Segregation of duties separates the role to install new CA and RA software from the role to activate CA and RA keys and vice versa. CAA role may have both rights but there are several compensating processes such as regular log comparison and configuration check and login alarm to verify that there doesn't exist any non-controlled processes or certificates

Other requirements in terms of the presence of people when carrying out other tasks involving CA and RA operations are detailed in the Telia CA Operational Documentation.

The Trusted roles in section 5.2.1 are fulfilled by at least one person each. Those working in the role of CA System Administrator or Registration Officer do not simultaneously work in any of the other roles involving the system.

### 5.2.3 Identification and authentication for each role

Person appointed and authorized to a Trusted Role by Telia CA and appropriate manager, person's identity is verified during the recruitment process by in presence verification of the person and corresponding legally acceptable identity certificate (e.g., passport, national identity card or equivalent) by the recruiter. List of nationally acceptable identity certificates is verified by the recruiter.

In addition to above identity verification, each person is further cleared by background checking procedures described in section 5.3.1 before any of the following may be granted.

a. Included in the access list for the CA and RA sites
b. Included in the access list for physical access to the CA and RA system
c. Given a certificate for the performance of their CA or RA role
d. Given a user account on the CA or RA system

Each of these certificates and accounts shall be:

a. Personal and directly attributable to the Trusted Role
b. Restricted to actions authorised by the Trusted Role in use of CA and RA software, servers and operating systems, physical access, and procedural

controls

Identification of roles in the CA and RA systems takes place as follows:

Identification of SA roles take place within the operating system in the CA and RA systems. Identification of the CAA roles (where applicable) take place within the CA system applications and is based on strong authentication using personal operator smart cards.

Identification of the RA roles takes place within the CA and RA system applications, and it is based on strong authentication either using personal operator cards or other two factor authentication mechanisms depending on the policy requirements of the applicable CA..

### 5.2.4 Roles requiring separation of duties

Telia maintains a policy and rigorous control procedures to ensure a separation of duties for critical CA and RA functions to prevent one person from maliciously using the CA or RA system without detection. Complete documentation of all roles and what roles are allowed for a single person can be found from Telia CA Operational Documentation.

## 5.3 Personnel controls

### 5.3.1 Qualifications, experience, and clearance requirements

Persons selected and designated to any of the Trusted Roles defined in section 5.2.1 shall meet set qualifications for the position as seen required by Telia. Qualifications include (but are not limited to) prior work experience, educational qualifications and general trustworthiness of the candidate in relation to the position. Same selection criterion applies to internal employees, contingent workers and external resources.

Qualifications and selection criterion may vary on country by country basis in Telia's geographical footprint. All qualifications are evaluated and verified in accordance of the local laws applicable to the candidate selection process.

Segregation of Duties (SoD) is applied over Trusted Roles by separately documented SoD rules defined in Telia CA's internal policies and guidelines. Primary objective is that segregation adheres to "least privilege" and "approver and executor are distinct roles or dual control must be applied".

In addition to above, all persons designated to any Trusted Role must be cleared by national background check and security clearance performed by designated government office or agency and described in section 5.3.2.

Telia HR may request for applicable certification documentation to be presented by the person being considered to a Trusted Role as deemed necessary by Telia HR on case by case basis.

### 5.3.2 Background check procedures

Telia conducts background checks for each Trusted Role candidate as described in this

section. Background check and security clearance shall be performed by designated government office or agency in accordance with national laws and in relation to requirements specific to the Trusted Role.
Information considered in the background check and security clearance is dependent on the national regulations and may vary between the countries where Telia CA operates.

Background clearance may include one or more of the following (additional checks and verifications may be included from time to time as seen necessary by Telia) verifications:

- Confirmation of previous employment
- Check of professional reference
- Search of criminal records (local, state, or provincial, and national)
- Check of credit/financial records
- Search of driver's license records
- National security clearance check

Background checks are repeated periodically for Trusted Role personnel, in accordance with national laws and Telia's corporate policies.

The outcome of background check is considered on grounds for accepting or rejecting candidate for a Trusted Role, generally including the following (but not necessarily limted to):

- Misrepresentations made by the candidate or Trusted Role
- Highly unfavourable or unreliable personal references
- Possible criminal background
- Indications of a lack of financial responsibility

Outcome and reports are evaluated by human resources and security personnel, who determine the appropriate course of action considering the full impact uncovered by the background check.

Any personal data and personally identifiable information (PII) disclosed by the background check is subject to the applicable federal, state, and local laws and considered as confidential information on as need to know basis.

### 5.3.3 Training requirements

Telia provides its personnel with courses and training needed for personnel to perform their job responsibilities competently and satisfactorily. Telia periodically reviews and enhances its training programs as deemed necessary.

Training programs consist of general trainings and tailored trainings on role and responsibility basis, including but not limited to the following:

- Basic PKI concepts
- Telia CA's operational requirements and policies (e.g. CP/CPS, internal guidelines and instructions)

- Telia security and operational policies and procedures
- Use and operation of deployed hardware and software
- Incident and Compromise reporting and handling
- Common security and vulnerability awareness trainings and updates
- Global PKI community updates and trainings (e.g. CA/Browser forum updates)
- Role and occupation dependent training (e.g. Registration Officer)
- Individually tailored training programs

### 5.3.4 Retraining frequency and requirements

Telia provides refresher training and updates to its personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

### 5.3.5 Job rotation frequency and sequence

Not applicable.

### 5.3.6 Sanctions for unauthorised actions

All employees and external resources working for Telia are informed about their obligation to report details immediately to superior, Group Security, Corporate Internal Audit on suspected security events, criminal activity, or fraud acts. Appropriate disciplinary actions are taken for unauthorised actions or other violations of Telia policies and procedures. Disciplinary actions may include warning, role change or termination of employment and are dependent on the frequency and severity of the unauthorised actions.

### 5.3.7 Independent contractor requirements

Independent contractors or external consultants may be designated to a Trusted Role. External persons are subject to the same qualifications and background controls as Telia employed personnel prior designation to a Trusted Role.

Independent contractors and consultants who have not completed the background check procedures specified in section 5.3.2 may only access Telia's secure facilities escorted and directly supervised by authorized person in applicable Trusted Role.

### 5.3.8 Documentation supplied to personnel

Telia personnel involved in the operation of Telia CA Services will be provided with required documentation needed to perform their duties.

## 5.4 Audit logging procedures

Telia CA and its Delegated Third Parties deploy auditing, monitoring, and logging system that continuously monitors, detects, and alerts designated personnel of any modification to Certificate Systems, Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems.

If deployed system cannot automatically detect and record an event, manual procedures are implemented to ensure required events are recorded.

### 5.4.1 Types of events recorded

Telia manually or automatically logs at least the following events relating to the CA and RA systems:

1. CA and RA certificate and key lifecycle events, including
    1. Key generation, backup, storage, recovery, archival, and destruction
    2. Certificate requests, renewal, and re-key requests, and revocation
    3. Approval and rejection of certificate requests
    4. Cryptographic device lifecycle management events
    5. Generation of Certificate Revocation Lists
    6. Signing of OCSP Responses (as described in Section 4.9 and Section 4.10)
    7. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles

2. Subscriber Certificate lifecycle management events, including
    1. Certificate requests, renewal, and re-key requests, and revocation
    2. All verification activities stipulated in these Requirements and the CA's Certification Practice Statement
    3. Approval and rejection of certificate requests
    4. Issuance of Certificates
    5. Generation of Certificate Revocation Lists
    6. Signing of OCSP Responses (as described in Section 4.9 and Section 4.10)
    7.Date, time, phone number used, persons spoken to, and end results of verification telephone calls
    8. The type(s) of identification document(s) presented by the Certificate Applicant
    9. Storage location of copies of applications and identification documents
    10. Identity of entity accepting the application
    11. Method used to validate organisation and individual identity and authority
    12. Information concerning the person requesting revocation
    13. Method of verifying the identity of the person requesting revocation
    14. Revocation request reception time
    15. Information concerning the certificate to be revoked

3. Security events, including
    1. Successful and unsuccessful PKI system access attempts
    2. PKI and security system actions performed
    3. Security profile changes
    4. Installation, update, and removal of software on a Certificate System
    5. System crashes, hardware failures, and other anomalies
    6. Firewall and router activities
    7. Entries to and exits from the CA facility

4. All Log entries include the following elements:
    1. Date and time of event

2. Identity of the person making the journal record
3. Description of the event

All records are made available for external auditing performed by qualified auditors as proof of Telia's adherence to applicable requirements, policies, and practices attributable to Telia.

### 5.4.2 Frequency of processing log

In the CA system the audit logs are reviewed at least monthly to check for any unauthorised activity. Audit log reviews include a verification that the log has not been tampered with, a brief inspection of all log entries, and a more thorough investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews are also documented.

In the RA systems the audit logs are automatically and continuously analysed, or logs are reviewed monthly to check for any unauthorised activity. The audit logs are also manually reviewed to search for any alerts or irregularities that for any reason have been missed by the automatic reviews. If such an irregularity is found the application for the automatic reviews will be updated to handle future irregularities of that type.

Telia also reviews its audit logs for suspicious or unusual activity in response to alerts generated based on irregularities and incidents within Telia CA and RA systems.

### 5.4.3 Retention period for audit log

Audit logs in accordance with section 5.4.1 are retained for at least seven (7) years from the date the entry is created or longer if required by law for audit and compliance purposes.

### 5.4.4 Protection of audit log

Logs are protected against improper alteration through the logical protection mechanism of the operating system and through the system itself not being physically or logically accessible other than by authorised personnel. Logging servers are protected from normal CA operators.

### 5.4.5 Audit log backup procedures

Audit logs are transferred online to at least two logging servers. Back-up copies of the system audit logs are made regularly according to defined schedules using offline storage media. Copies of the audit log and summaries of the inspection of audit logs are stored in physically secure locations in two physically separate places.

The logs are stored in such a way that they can, in the event of serious suspicion of irregularities, be produced and made legible for auditing during the stated storage time.

### 5.4.6 Audit collection system (internal vs. external)

Automated audit data is generated and recorded at the application, network, and

operating system level.

Manually generated audit data is recorded by Telia personnel.

### 5.4.7 Notification to event-causing subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organisation, device, or application that caused the event.

### 5.4.8 Vulnerability assessments

The CA assesses the vulnerability of its critical systems regularly. The CA address any critical vulnerability not previously addressed by the Telia CA, within a period of 48 hours after its discovery. On the basis of the assessment results the configurations of firewalls and other systems are updated, and operation policies and practices are revised, if necessary.

## 5.5 Records archival

Telia CA archives relevant materials which affect the operation of the CA service. Procedures and prerequisites for this archiving are detailed in the following subsection.

### 5.5.1 Types of records archived

The following information is archived on an ongoing basis:

a. Transactions containing signed requests for certificate production and revocation of certificates from authorised operators
b. Certificate application documentation signed by applicant commissioners and by persons responsible for receiving and accepting applications
c. Signed receipt confirmations when issuing keys and codes
d. Issued certificates and related catalogue updates
e. History of previous CA keys, key identifiers and cross certificates between different CA key generations
f. Revocation, suspension and re-instatement requests and related information received by the revocation service
g. CRL creation times and CRL catalogue updates
h. Results of reviewing Telia compliance with this CPS and other audits.
i. Applicable terms and conditions and contracts (in all versions applied)
j. All CP and CPS versions published by the CA

In cases where the archived information constitutes a digitally signed volume of information, the necessary information required for verifying the signature during the stated archiving time is also archived.

### 5.5.2 Retention period for archive

Telia CA will retain all documentation relating to certificate requests and the verification thereof, and all certificates and revocation thereof, for at least seven (7) years from the date the entry is created, or longer if required by law, after any certificate based on that documentation ceases to be valid.

### 5.5.3 Protection of archive

The archives are stored also in locations other than the CA and RA sites. The archives are stored under such conditions that the archived material is protected from unauthorised viewing, modification, or deletion by physical protection and in some cases combined with cryptographic protection.

Archived material which is classified as confidential in accordance with section 9.3 is not accessible to external parties in its entirety other than as required by law and court orders.

Individual pieces of information relating to a specific key holder or transaction may be released after individual investigations.

The archive is stored under such conditions that it remains legible for auditing during the stated storage time.

However, the parties are made aware that technology for storing archived material may be changed and, in such an event, the CA is not obliged to retain functioning equipment for interpreting old, archived material if this is more than five years old. In such an event, the CA is however instead obliged to be prepared to set up the necessary equipment on payment of a charge corresponding to the costs of Telia.

In the event that changes in procedures for access to archived material have been caused by Telia ceasing its operations, information on procedures for continued access to archived material shall be supplied by Telia through the notification procedures in accordance with section 5.8.

### 5.5.4 Archive backup procedures

Information to be archived is collected continuously from the places of origin and transferred to several online archives. Online archives are backed up regularly to offline archives.

### 5.5.5 Requirements for timestamping of records

All documents archived pursuant to this section will be marked with the date of their creation or execution.
The date and time information in the CA system and certain other system logs is synchronized with an external coordinated universal time source (UTC). The time used for the provision of revocation services is synchronized with UTC at least once every 24 hours.

### 5.5.6 Archive collection system (internal or external)

Telia is using internal archive systems and servers to collect archived information.

### 5.5.7 Procedures to obtain and verify archive information

Telia will verify the integrity of the backups at least once every 12 months to ensure usability of these backups. Material stored off-site will be periodically verified for data integrity.

## 5.6 Key changeover

Telia CA key pairs are retired from service at the end of their respective maximum lifetimes as defined in section 6.3.2. CA certificates may be renewed if the cumulative certified lifetime of the CA key pair does not exceed the maximum CA key pair lifetime. New CA key pairs will be generated as necessary, for example to replace CA key pairs that are being retired, to supplement existing, active key pairs and to support new services in accordance with section 6.1.

A new set of CA key pairs is created at least three months before the point when the existing CA keys ceases to be used for issuing of new certificates.

### 5.6.1 Self-Signed CA

Changing of CA keys for a self-signed CA will be done, using the following procedure:

a. A new CA key pair is created
b. A new self-signed certificate is issued for the new public CA key
c. A cross certificate is issued where the new public CA key is signed using the old private CA key, and the certificates in accordance with b) to c) is published in the relevant directory
d. New Subscriber certificates are signed with the new private CA key
e. The old CA private key is used to issue CRLs until the expiration date of the last certificate issued using the old key pair has been reached

### 5.6.2 CA Hierarchies

Changing of CA key pairs for a subordinate CA will be done using the following procedures:

a. A new subordinate CA key pair is created
b. A new subordinate CA certificate is issued for the new public CA key by the superior CA on the next level of the hierarchy
c. The certificate in accordance with b. is published in the relevant directory
d. New subordinate CA certificates or Subscriber certificates issued by the new subordinate CA are signed with the new private subordinate CA key
e. the old subordinate CA private key is used to issue CRLs until the expiration date of the last certificate issued using the old key pair has been reached

A superior CA ceases to issue new subordinate CA certificates no later than three months before the point in time where the remaining lifetime of the superior CA key pair equals the approved certificate Validity Period for the specific type of certificates issued by subordinate CAs in the superior CA's hierarchy.

## 5.7 Compromise and disaster recovery

Telia has implemented a robust combination of physical, logical, and procedural controls to minimize the risk and potential impact of a key compromise or disaster. Telia has implemented disaster recovery procedures and key compromise response procedures described in this CPS. Telia's compromise and disaster recovery procedures have been developed to minimize the potential impact of such an occurrence and restore Telia's operations within a commercially reasonable period.

### 5.7.1 Incident and compromise handling procedures

Telia has implemented detailed change and incident management procedures to allow for controlled and accountable handling of incidents and recovery from system and application disasters. Regarding disaster recovery at the site level Telia has implemented disaster recovery plans.

Detailed instructions are provided in the Telia Operation Procedures with a Disaster Recovery Plan outlining the steps to be taken in the event of an incident and the incident reporting caused by such an incident.

### 5.7.2 Computing resources, software, and/or data are corrupted

In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to Telia Security staff and Telia's incident handling procedures are initiated. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, Telia's key compromise or disaster recovery procedures will be initiated.

### 5.7.3 Entity private key compromise procedures

Upon the suspected or known compromise of a Telia CA private key, Subscriber CA private key or the Telia infrastructure, Telia's Key Compromise Response procedures are followed. Detailed instructions are provided in the Telia Operation Procedures.

Telia undertakes, on suspicion that Telia no longer has full and exclusive control of a CA's private key, to take the following action:

a. Revoke the CA certificate associated to the compromised CA private key if the CA is a part of a CA hierarchy and make the updated ARL (ARL is CRL for CA certificates) publicly available
b. Cease all revocation checking services relating to certificates issued using the compromised key and all revocation checking services signed using the comprised key or keys certified using the compromised key. This means that all associated revocation lists are removed from their assigned locations
c. Inform all key holders and all parties with which Telia has a relationship that the CA's private key has been compromised and how new CA certificates can be obtained
d. In the event that Telia has cross certified the compromised CA key with another operational CA key, revoke any such cross certificates

Subscriber key holders will be informed that they should immediately cease using private keys which are associated with certificates issued using the compromised CA's private key.

Key holders are furthermore informed how they should proceed in order to obtain replacement certificates and any new private keys, and the circumstances under which old private keys can be used in connection with other certificates which have not been issued using the compromised CA key.

Information will be made available to relying parties, who are clearly informed that the

use of the affected certificates and the CA's issuer certificate has been revoked.

The action of relying parties is outside Telia's influence. Through Telia's revocation information process, they will receive the necessary information to be able to take the correct action.

### 5.7.4 Business continuity capabilities after a disaster

Telia will provide business continuity procedures in a Disaster Recovery Plan that outline the steps to be taken in the event of corruption or loss of computing resources, software and/or data. Telia has implemented mission critical components of its CA infrastructure in redundant configurations. This applies both to hardware and software components. The main CA system components have been implemented in two data canters located in different cities.

Telia maintains offsite backup of important CA information for CAs issued at the Telia's premises. Such information includes but is not limited to: Backups of CA key pairs, application logs, certificate application data, audit data and database records for all certificates issued. In addition, CA private keys are backed up and maintained for disaster recovery purposes.

## 5.8 CA or RA termination

If it is necessary for a Telia CA to cease operation, Telia makes a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination.

Unless otherwise addressed in an applicable agreement between Telia and a Subscriber, Telia may:

a. Ensure that any disruption caused by the termination of an Issuing CA is minimized as much as possible
b. Provision of notice to parties affected by the termination, such as Subscribers Relying Parties, and Supervisory bodies and informing them of the status of the CA
c. Make public announcement in the CA repository at least three months in advance that operations will cease for the CA
d. Revoke all active Certificates before the end of the three months' notice period
e. Destroy private keys, including backup copies, in a manner such that the private keys cannot be retrieved
f. Cease all revocation checking services relating to certificates issued using the CA keys of which use will cease. This means that all associated revocation lists are removed from their assigned locations and that no new revocation lists are issued to replace those that are removed
g. Terminate all rights for subcontractors to act in the name of the CA which will cease to operate
h. Ensure that all archive records of the issuing CA are retained
i. Prior terminating the CA services - if applicable depending on the agreed contracts, Telia may transfer provision of the CA services for its existing

Subscribers to another CA successor entity

j. Notify relevant parties such as auditors, CA root programs and CCADB

Telia has made arrangement to cover the costs to fulfil these minimum requirements in case the CA becomes bankrupt or for other reasons is unable to cover the costs by itself, as far as possible within the constraints of applicable legislation regarding bankruptcy.

# 6 TECHNICAL SECURITY CONTROLS

## 6.1 Key pair generation and installation

### 6.1.1 Key pair generation

The CA key pairs are generated in FIPS 140-2[2] level 3 or higher validated cryptographic hardware modules designated for Telia CA.

CA Key Pairs are generated by multiple trusted individuals acting in trusted roles and using dedicated cryptographic hardware device as part of scripted key generation ceremony in the environments described in section 5.1 and logged in accordance with section 5.4.

Activation of the hardware requires the presence of two (2) authorized Trusted Role personnel. Telia produces auditable evidence during the key generation process to prove that the CPS was followed, and role separation was enforced during the key generation process.

Generation of key pairs for publicly trusted CA hierarchy requires that an external auditor witness the generation of any CA keys intended to be used for publicly trusted Root CA or publicly trusted Subordinate CA creation.

CA key pair generation ceremony script must be approved and signed by Telia CA Security Board. CA Key Pairs are generated by multiple trusted individuals acting in trusted roles and using dedicated cryptographic hardware device as part of scripted key generation ceremony in the environments described in section 5.1 and logged in accordance with section 5.4. The authorized trusted roles shall sign and document record of the key generation ceremony, as allowed by applicable policy.

RA keys used by Registration Officers are encrypted are securely used and kept secret privately by each Registration Officer.

Root CA keys are stored in offline state. They are activated only when needed. Two (2) duly authorized Trusted Role persons are required to activate offline key.

The Subscriber key pair may be generated by the Subscriber, or the Subscriber may use the registration tool provided by the CA to generate the key pair (PKCS#12 files). The Subscriber may also generate the key pair on a Smart Card or USB token. It is also possible use Smart Cards that have the key pair generated by the Card Manufacturer.

If the key pair is generated by the Subscriber in a Subscriber Organisation, External RA or External Partner (for short-lived personal certificates) such parties themselves are responsible for the secure generation of the key pair and the confidentiality of the private key.

If the key pair is provided by the CA, the generation will be carried out according to the

secure procedures defined by the CA.

### 6.1.2 Private key delivery to Subscriber

The CA delivers the Subscriber's private key on a Smart Card, on a USB token, or in a file to the Registration Officer in Subscriber Organisation or to the Subject.

When the Subject generates his key pair, the private key will be recorded on the Subjects workstation, Smart Card or USB token, a separate delivery of the key is not needed.

Telia CA does not generate or deliver private keys to Subscribers for short-lived personal certificates. Export of the private key for short-lived personal certificate is not possible.

Software certificates

If the key pair is generated using the self-service software provided by the CA, the private key is delivered to the Subscriber in a password protected PKCS#12 file. The Subscriber Registration Officer can download the PKCS#12 file directly from the application. Alternatively, Subscriber Registration Officer may generate a one-time password for the Subject to access the self-service software. Subject generates the key pair and downloads the PKCS#12 file.

Smart Cards and USB tokens

If the key pair is generated by the Card Manufacturer, the Card Manufacturer delivers the Smart Card that contains the private key to the address specified in the card order, which is normally the address of the Registration Officer of the Subscriber Organisation. The Registration Officer will deliver the card to the Subject.

### 6.1.3 Public key delivery to certificate issuer

Subscribers and RAs submit their public key to Telia for certificate signing in a PKCS#10 CSR, certificate request syntax, or other digitally signed package in a session secured by TLS.

### 6.1.4 CA public key delivery to relying parties

CA public key is made available in the form of signed X.509 certificate in Telia CA public repository (https://cps.trust.telia.com/). Certificate will be available in both Privacy Enhanced Mail (PEM) and Distinguished Encoding Rules (DER) format.

Telia CA's publicly trusted Root CA and Subordinate CA public keys are made available to the relying parties as uploaded certificates in the Common CA Database (CCADB, https:/ccadb.force.com/)

Subscriber CA may be made available as described above, if approved by the Subscriber.

### 6.1.5 Key sizes

Permitted key sizes and algorithms accepted by Telia CA are defined in the following

sections.

No other key sizes or algorithms are permitted.

#### 6.1.5.1 CA key pairs

Allowed key sizes and algorithms for CA key pairs are:

- RSA algorithm (rsaEncryption (OID: 1.2.840.113549.1.1.1) with a minimum key length of 4096 bits.
- ECDSA algorithm, NIST P-384, namedCurve secp384r1 (OID: 1.3.132.0.34)

#### 6.1.5.2 Subscriber key pairs

Allowed key sizes and algorithms for Subscriber key pairs are:

- RSA algorithm (rsaEncryption (OID: 1.2.840.113549.1.1.1)
  - Minimum key length of 2048 bits.
- ECDSA algorithm (id-ecPublicKey (OID: 1.2.840.10045.2.1)
  - P-256, namedCurve secp256r1 (OID: 1.2.840.10045.3.1.7)
  - P-384, namedCurve secp384r1 (OID: 1.3.132.0.34)

### 6.1.6 Public key parameters generation and quality checking

Telia uses a HSM device that conforms to FIPS 186-2 and provides random number generation and on-board generation of up to 8192 bit RSA Public Keys and a wide range of ECC curves.

CA keys are protected by a secure cryptographic hardware module rated at least FIPS 140-2, Level 3.

Telia verifies the quality of keys before accepting the certificate request in accordance with the requirements set forth in Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates section 6.1.6.

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

Issued certificates contain information that 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. The area of application labelling takes place in accordance with X.509 and chapter 7.

End-Entity certificates issued according to this CPS include the following areas of application (smart cards are not in use for all certificate types):

#### 6.1.7.1 Non-S/MIME End-Entity Certificates

Certificate stored on a Smart Card, signing key:

NonRepudiation

Certificate stored in a Smart Card, authentication/encryption key:

DigitalSignature, KeyEncipherment, DataEncipherment

Short-lived personal certificates:

DigitalSignature and/or NonRepudation

Other certificates:

All the purposes mentioned on the list are not contained in all certificates, and in certain certificates there is no key usage purpose given: DigitalSignature, NonRepudiation, KeyEncipherment, DataEncipherment, KeyAgreement.

#### 6.1.7.2 S/MIME End-Entity Certificates

Publicly Trusted S/MIME Certificates issued in accordance with this CP/CPS and adhering to the BR SHALL use keyUsage-extension in supported S/MIME profiles.

| S/MIME Profile | keyUsage per public key type |
|---|---|
| Legacy | **RSA**<br>For signing only, bit positions SHALL be set for digitalSignature and MAY be set for nonRepudiation.For key management only, bit positions SHALL be set for keyEncipherment and MAY be set for dataEncipherment.For dual use, bit positions SHALL be set for digitalSignature and keyEncipherment and MAY be set for nonRepudiation and dataEncipherment.<br><br>**EC**<br>For signing only, bit positions SHALL be set for digitalSignature and MAY be set for nonRepudiation.For key management only, bit positions SHALL be set for keyAgreement and MAY be set for encipherOnly or decipherOnly.For dual use, bit positions SHALL be set for digitalSignature and keyAgreement and MAY be set for nonrepudiation and for encipherOnly or decipherOnly (only if keyAgreement is set). |

#### 6.1.7.3 Special considerations on Root CA private key use to sign certificates.

Telia CA uses Root CA Private keys only to sign certificates in following cases:

- Signing of self-signed Certificate to represent the Root CA itself

- Signing of subordinate CA certificates and Cross Certificates by the Root CA
- Signing of OCSP response verification certificates

## 6.2 Private key protection and cryptographic module engineering controls

Telia CA has implemented a combination of physical, logical, and procedural controls to ensure the security of Telia and Subscribers CA private keys. Logical and procedural controls are described here in section 6.2. Physical access controls are described in section 5.1.2. Subscribers are required by contract to take necessary precautions to prevent the loss, disclosure, modification, or unauthorised use of private keys.

The Subscriber is required to protect its private key from disclosure according to the requirements as defined by the issuing CA. The Subscriber is responsible for its private keys.

### 6.2.1 Cryptographic module standards and controls

All CA Digital Signature key generation, CA Digital Signature key storage and certificate signing operations will be performed in a hardware cryptographic module validated to at least FIPS 140-2 Level 3. The cryptographic module is physically protected within the protected environment defined in section 5.1.

All other CA cryptographic operations, such as certificates and keys used for administering the CA, will be performed with hardware based cryptographic module.

End entity private keys can be enclosed and protected in two different ways:

a. Hardware protected private keys which are created and stored in smart cards or equivalent chip-based hardware.
b. Software protected private keys generated by the CA or by the Subscriber

Software protected keys shall be stored in encrypted form with a security level which makes it unfeasible to crack the encryption protection through logical attacks. For this reason, key holders shall use methods and tools approved by the CA. However, for locally generated software-protected keys, it is the key holder (and the key holder's organisation) who takes sole responsibility for satisfactory security being achieved in the user's local environment.

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

Telia has implemented technical and procedural mechanisms that require the participation of multiple Trusted Role individuals to perform CA cryptographic operations.

Telia uses "Secret Sharing" to split the recovery data needed to make use of a CA private key into separate parts called "Secret Shares". A threshold number of Secret Shares (n) out of the total number of Secret Shares created and distributed for a particular hardware cryptographic module (m) is required to recover a CA private key

stored on the cryptographic module.

### 6.2.3 Private key escrow
Telia CA does not escrow private keys.

### 6.2.4 Private key backup
Telia CA backup copies of CA and RA private keys for recovery purposes. Backup retrieval requires same access protection controls which apply to the original keys. At least two authorized Trusted Role persons are required to manage CA private key backups.

Telia backup subscriber private keys, if separately agreed between Telia and the Subscriber. The backup keys are copied and stored in encrypted form and protected at a level no lower than of the keys in use.

No backups are made of the subscriber's private non-repudiation keys.

See section 4.12. for a more detailed description.

### 6.2.5 Private key archival
RA or CA private keys will be archived by Telia CA for recovery purposes.

Telia CA do not archive subscriber private keys.

### 6.2.6 Private key transfer into or from a cryptographic module
Telia CA generates CA key pairs on the hardware cryptographic modules in which the keys will be used. When CA key pairs are transferred to another hardware cryptographic module, key pairs are transported between modules by secure methodology supported by the cryptographic module.

### 6.2.7 Private key storage on cryptographic module
CA private digital signature key is kept in a secure cryptographic hardware module rated to at least FIPS 140-2 Level 3.

### 6.2.8 Method of activating private key
CA keys:

The activation of the CA private key is done by person serving in authorized trusted role of the CA and authenticated with a two-factor authentication to activate the private key. The key remains active in the CA system for a single process until it is deactivated.

Essential information exchange between a RA and the CA is protected. All CA and RA operators are authenticated in CA or RA system in accordance with section 5.2.3 and transactions affecting the use of a CA's private issuer keys are authenticated by the CA system based on a digital signature. Activation of the private key of the Telia RA requires the use of activation data as described in section 6.4.

Subscribers are solely responsible for protecting their Private Keys in a manner commensurate with the Certificate type. Subscribers should use a strong password or

equivalent authentication method to prevent unauthorized access or use of the Subscriber's Private Key. Subscribers should also take commercially reasonable measures for the physical protection of their workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization. When deactivated, private keys shall be kept in encrypted form only and secured. At a minimum, Subscribers are required to authenticate themselves to the cryptographic module before activating their Private Keys.

Telia recommends that Subscribers and Subscriber Registration Officers take as protective measure to store their private keys in encrypted form and protected by the use of a hardware token and/or strong passphrase. The use of two factor authentication mechanisms (e.g., token and passphrase or biometric and token) is encouraged.

Software keys:

The CA recommends that the Subscriber Organisations use passwords for private key activation as described in section 6.4 and take appropriate measures for the physical protection of the workstations or other devices used to store private keys.

Smart Cards and USB tokens:

Activation of the Subject's private requires the use of activation data as described in section 6.4.

### 6.2.9 Method of deactivating private key

CA keys:

Telia's CA private keys are deactivated via logout procedures on the applicable HSM device when not in use.

Telia never leaves its HSM devices in an active unlocked or unattended state.

Software keys:

Deactivation of software keys should be performed according to software manufacturer's instructions and recommendations. Software keys should be deactivated at all times when not attended.

Smart Cards and USB tokens:

The private key on a Smart Card or USB token will be locked if the activation data related to it is inserted falsely too many times in succession. The lock-out threshold depends on the Smart Card or USB token type used and can be, for example, 3 or 5 failed attempts. A locked key can be returned into use with the help of a PUK code (PUK = PIN Unblocking Key) or equivalent technology (e.g. challenge/response).

### 6.2.10 Method of destroying private key

For operational keys which are stored on the issuer system's hard disk or other media in encrypted form, the following applies:

a. If the equipment is to be used further in the same protected environment, erasing is carried out in such a way that these keys cannot be recovered at least without physical access to the media. Old or broken CA key storage media may be temporarily stored in the protected CA environment
b. If the media that has contained CA key material will permanently leave the protected CA environment, it will be destroyed. Physical destruction is used when destroying the media

The Subscriber private confidentiality keys that are stored by the CA for backup purposes are securely destroyed at the end of service.

The short-lived certificates private keys that are used for document signing will be destroyed immediately by the operating External RA after signing documents. The private keys of short-lived certificates will not be permanently stored on any device (e.g., USB token, smart card or hard disk). Key is temporarily created in document signing server's random-access memory.

#### 6.2.11Cryptographic module rating

See section 6.2.1.

## 6.3 Other aspects of key pair management

### 6.3.1 Public key archival

Telia CA retain archives of public keys for the period of at least seven years after the expiration of the last Subscriber certificate that has been issued by the CA.

### 6.3.2 Certificate operational periods and key pair usage periods

Telia CA operational periods for key pairs and certificates as depicted in below table.

| Certificate type | Key pair usage period | Certificate term |
|---|---|---|
| Publicly Trusted Root CA | 25 years | Maximum 25 years |
| Publicly Trusted Cross CA | 25 years | Maximum 25 years |
| Publicly Trusted Subordinate CA | 25 years | Maximum 25 years |
| Subscriber certificates | 3 years | Maximum 3 years |
| S/MIME Subscriber certificates issued under Legacy profile | Maximum 1185 days | Maximum 1185 days |

Certificate term is limited by the time of creation or issuance and notAfter is set to a date earlier or the same as expiration date of the key pair used for the Certificate.

Telia CA discourages reuse of key pairs over certificate's lifetime.

The usage period of the public and private keys shall not exceed beyond the time the applied cryptographic algorithms and their pertinent parameters remain cryptographically secure or otherwise suitable.

For calculations, a day is measured as 86,400 seconds. Any amount of time greater than

this, including fractional seconds and/or leap seconds, represents an additional day. For purposes of calculating time periods in this document, increments are rounded down subject to the imposed maximum requirements.

## 6.4 Activation data

Telia CA activates the cryptographic module containing its CA Private Keys according to the specifications of the hardware manufacturer. For roots and public issuing CAs, this method has been evaluated as meeting at least the requirements of FIPS 140-2 Level 3. The cryptographic hardware is maintained under two-person control as explained in this CPS.

Activation data is transmitted via an appropriately protected channel and at a time and place that is distinct from the delivery of the associated cryptographic module.

Telia CA and RA operators are either using PIN protected private keys on smart cards or have private keys stored on personal computer hard disk. If the keys are stored on personal computer hard disk, private keys shall be protected by strong passwords meeting the criterion set forth in CA/Browser Forum Network and Certificate System Security Requirements.

Telia encourages Subscribers and Subscriber Registration Officers choose activation data that meet the requirements described above. Telia also recommends the use of two factor authentication mechanisms (e.g., token and pass phrase or biometric and token) for private key activation.

### 6.4.1 Activation data generation and installation

Publicly trusted Root CA and Subordinate CA keys:

Activation data (Secret Shares) used to protect Telia CA, and Subscribers CA private keys is generated in accordance with the requirements of section 6.2.2.

Software keys:

When the Subject or subscriber Registration Officer generates a key pair, password or passphrase should be created as activation data, where applicable according to Subscriber Organisation policy.

When Telia CA generates the key pair on behalf of the subscriber, the activation data will be generated using enough characters to be secure.

Smart Cards and USB tokens:

The Card Manufacturer, Subscriber Organisation or RA system generates the activation data in pursuance of key pair generation.

### 6.4.2 Activation data protection

All activation data will be protected from unauthorised use by a combination of cryptographic and physical access control mechanisms as explained in this CPS.

Activation data (Secret Shares) used to protect Telia CA private keys is stored in secure locations where at least two trusted individuals are required to access them. Telia CA and RA operators are required to store their Administrator private keys on smart cards or in encrypted form using password protection.

Telia CA personnel (internal or external), Subscribers and, Subscriber Registration Officers shall protect the activation data for their private keys against loss, disclosure, modification, or unauthorised use. Any activation data should be memorized and not to be written down in any form or disclosed to other individuals. Subscribers shall instruct their Subjects protect activation data in similar manner.

When the Card Manufacturer generates the key pairs, the activation data is generated at the same time and delivered securely to the Subject.

Secure delivery may be, but not limited to, achieved by:

- Concealed under a protective surface layer or enclosed in a sealed envelope
- Or other similar secure method

When Telia CA generates the key pair, the activation data and the private key are delivered separately to the Subscriber.

When subscriber Registration Officer generates the key pairs, the organisation is responsible for the secure delivery of the activation data to the Subject.

.

### 6.4.3 Other aspects of activation data

Not applicable.

## 6.5 Computer security controls

### 6.5.1 Specific computer security technical requirements

The entire CA system is built in such a way that individual roles as per section 5.2 can be separated. The access control systems used is built in such a way that every operator is identified at an individual level and authenticated in accordance with the section 5.2.3.

The above shall apply regardless of whether an operator acts directly within the CAs central premises or whether the operator is in an external RA function.

### 6.5.2 Computer security rating

No stipulation.

## 6.6 Life cycle security controls

### 6.6.1 System development controls

Two-phase testing is used in the development of the CA and RA production systems. The changes that have emerged because of development work will be first tested in a separate development system. After a successful testing the changes are taken into the test system that is like the production system. The acceptance test is performed in the

test system before the changes are taken into production.

All the changes in the system, which are to be taken into production, are properly documented.

### 6.6.2 Security management controls

Telia's Group Security Policy applies to the Telia CA. Furthermore, the CA follows the security instructions and guidelines, applicable CP/CPS governing the CA operations. The auditing of the operation has been described in chapter 8.

Evaluation of business risks and establishment of reaction and recovery models for potential risks belong to the management of the Business Continuity Plan drawn up by the CA. The reporting of abnormal events and of detected or suspected weaknesses in security is carried out according to the procedures defined by the CA.

The CA ensures by contractual arrangements that the level of security is preserved also when the outsourced functions are concerned, and that the defined policies and practices are followed also when subcontractors are involved.

Operational documentation has been drawn up which documents in detail how roles and authorisation are applied and maintained.

### 6.6.3 Life cycle security controls

Telia has prevented developers to access production systems. Versions and releases are separated from each other using software management tools designed to this purpose. Each update to production is approved and documented.

## 6.7 Network security controls

Telia CA services are secured by two-factor authentication through VPN to protect data and systems from unauthorised personnel. Suspicious login attempts or activities will be monitored and alerted by the intrusion detection system. Industry best practices are followed for securing the CA networks, for example by conforming to the CA/B Forum Network Security Guidelines[3].

Firewalls have been implemented to restrict access to the Telia CA equipment. Only specified traffic allowed through network boundary controls such as protocols and ports required by Telia CA's operations.

Essential information exchange between the RA and Telia CA is encrypted and transactions affecting the use of the CA's private issuer keys are individually signed. All communication ports in the CA system which are not needed are deactivated and associated software routines which are not used are blocked.

Telia CA services are secured by two-factor authentication through VPN to protect data and systems from unauthorised personnel. Suspicious login attempts or activities will be

[3] Network and Certificate System Security Requirements, https://cabforum.org/network-security-requirements/

monitored and alerted by the intrusion detection system.

## 6.8 Timestamping

The system time on Telia CA computers is updated using the Network Time Protocol (NTP) to synchronize system clocks. The used Telia NTP servers are using time where quality is on level Stratum-3.

# 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 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 random 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 guaranteeing non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.. |
| 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 one of the following sha256RSA/ECDSA, sha384RSA/ECDSA or sha512RSA. |
| Issuer | This field states the name of the Issuer of the certificate. The Issuer name in the certificates of each CA has been described in section 1.3.1. |
| Validity | The validity of the certificate is that period during which the CA guarantees that it maintains status information of the certificate, in other words about the possible revocation of the certificate. This field states the date and time when the certificate comes into force, and the date and time after which the certificate is no more valid. The certificate can be trusted during its validity period if the certificate has not been published on the CRL. |
| Subject | This field identifies the person or Device under whose possession the private key is, that corresponds to the public key contained in the certificate. The field includes the unambiguous name of the Subject. The contents of the field have been described in section 3.1. |

| Field name | Field description and contents |
|---|---|
| Subject public key info | This field gives the algorithm under which the public key of the Subject shall be used.<br><br>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 CRL Profile".

In general, following extension may be used in a CA certificate:

| Extension | Criticality | Extension description and contents | In Root CA |
|---|---|---|---|
| Authority key identifier | non-critical | 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. | Yes |
| Subject key Identifier | non-critical | 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. | Yes |
| Certificate policies | non-critical | 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. | No |
| CRL distribution points | non-critical | 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. | No |
| Key usage | critical | The key usage purposes of the public key contained in the certificate are given in this extension.<br><br>Within Telia PKI the key usage purposes of the public key of the CA are:<br><br>- Certificate signing (KeyCertSign)<br><br>- CRL signing (CRLSign) | Yes |

| Extension | Criticality | Extension description and contents | In Root CA |
|---|---|---|---|
| Basic constraints | critical | This extension expresses if the certificate is a CA certificate, e.g., the Subject is the CA. In CA certificates the CA field is set to "True".<br><br>The extension path field "pathLenConstraint" defines the maximum number of CA certificates that may follow this certificate in a certification path. Root CA certificates have a "pathLenConstraint" field set to a value of "none" e.g., there is no restrictions for length subordinate CA path length. Subordinate CAs that may only issue end-user certificates have a "pathLenConstraint" set to a value of "0". | Yes |
| Authority information access | non-critical | This extension may contain two values:<br>a. The URL to CA-certificate<br>b. OCSP service address as defined by RFC6960<br>Typically, all subordinate CA certificates include both listed values. | No |
| Name constraints | critical | Defines the permitted subtree(s) for the CA to issue Subscriber certificates | No |
| Extended key usage | non-critical | For S/MIME capable CAs:<br>SHALL contain, id-kp-emailProtection<br>MAY contain, id-kp-clientAuth<br><br>For other CAs<br>SHALL contain, id-kp-clientAuth<br><br>MAY contain, 1.2.840.113583.1.1.5 and/or 1.3.6.1.4.1.311.10.3.12 | No |

## Certificate extensions in Publicly Trusted S/MIME certificates

| Extension | Criticality | Extension description and contents |
|---|---|---|
| Extended key usage | non-critical | S/MIME **Strict** profile in S/MIME capable CAs:<br>SHALL contain, id-kp-emailProtection<br>Other values SHALL NOT be present.<br><br>S/MIME **Legacy** profile in S/MIME capable CAs:<br>SHALL contain, id-kp-emailProtection<br>MAY contain, id-kp-clientAuth |

In general, the following extensions may be used in a certificate. In the table "Authority" means who verifies the content of the extension:

| Extension | Authority | Extension description and contents |
|---|---|---|
| Authority key identifier | CA | The identifier of the issuing CA public key is given in this extension. The identifier can be used to identify the public key that corresponds to the private key used for the signing of the certificate. SHA-1 hash algorithm is used to calculate the identifier. |
| Subject key Identifier | CA | The identifier of the Subject public key that is contained in the certificate is given in this extension. The identifier can be used to pick up those certificates that contain a given public key. SHA-1 hash algorithm is used to calculate the identifier. |
| Certificate policies | CA | This extension states the policies according to which the certificate has been issued. The relevant policy is identified based on an individual identifier (object identifier, OID) assigned to the policy document or certain certificate type. The identifiers covered by this CPS have been given in section 1.2. |
| CRL distribution points | CA | This extension gives the location where the CRL is available. The exact addresses of the CRLs corresponding to the different certificate classes are given in section 4.10.1. |
| Key usage | CA | The key usage purposes of the public key contained in the certificate are given in this extension. The key usage purposes of the public keys contained in the certificates are listed in section 6.1.7. |
| Extended key usage | CA | This extension is mandatory in Telia certificates.<br><br>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.<br><br>E.g. the following key usage purposes may be given in a Certificate: ClientAuthentication, WindowsLogon, S/MIME |
| Basic constraints | CA | This extension may be used to express explicitly, if the certificate is a CA certificate (e.g., the Subject of the certificate is a CA) or not. Certain End-Entity certificates state that the certificate in question is not a CA certificate. |
| Subject alternative name | Subscriber | This extension can be used to relate alternative identification information to the Subject. Subject alternative name information used in the Certificates is described in section 3.1.1. |
| Authority Info Access | CA | The URL to the OCSP service or CA-certificate may be given in this field. |

| Extension | Authority | Extension description and contents |
|---|---|---|
| Smartcard serial number | Subscriber | Certificate stored on a Smart Card:<br><br>The serial number of the Smart Card of the Subject is given in this field. The serial number is used to relate the Subject to the cryptographic device used by the Subject. An individual number together with a checksum is used as a serial number. The number belongs to the number space reserved for the Smart Cards of the CA and it is stored on the Smart Card.<br><br>Certificate stored in a USB token:<br><br>The field can be utilized also in connection with other cryptographic devices to indicate the type of the Device in question. The field is used also in certificates stored in USB tokens and its contents are a character string defined by the CA. |

Also, other extensions may be used.

### 7.1.3 Algorithm object identifiers

#### 7.1.3.1 SubjectPublicKeyInfo

Telia CA uses following algorithms and algorithm identifiers in issued certificates in accordance with the Baseline Requirements.

- RSA,
  - rsaEncryption (OID: 1.2.840.113549.1.1.1)
- ECDSA namedCurve
  - P-256 keys, secp256r1 (OID: 1.2.840.10045.3.1.7)
  - P-384 keys, secp384r1 (OID: 1.3.132.0.34)

No other encodings are permitted.

#### 7.1.3.2 SignatureAlgorithmIdentifier

Telia CA uses following signature algorithms and algorithm identifiers when signing objects with CA Private Key in accordance with the Baseline Requirements.

- RSA
  - RSASSA-PKCS1-v1_5 with SHA-256, AlgorithmIdentifier: `300d06092a864886f70d01010b0500`
  - RSASSA-PKCS1-v1_5 with SHA-384 AlgorithmIdentifier: `300d06092a864886f70d01010c0500`
  - RSASSA-PKCS1-v1_5 with SHA-512 AlgorithmIdentifier: `300d06092a864886f70d01010d0500`
- ECDSA
  - P-256 keys, AlgorithmIdentifier: `300a06082a8648ce3d040302`
  - P-384 keys, AlgorithmIdentifier: `300a06082a8648ce3d040303`

No other encodings are permitted.

### 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 CP OID 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 may be 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 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 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".

The CRL extensions contain the following elements:

| Extension | Extension description and contents |
|---|---|
| Authority Key Identifier | 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. |
| CRL Number | Increasing sequence number for a given CRL scope and CRL issuer |

The following entry extensions may be included in a CRL:

| Extension | Extension description and contents |
|---|---|
| Serial Number | Serial number of the certificate that was revoked |

| Extension | Extension description and contents |
|---|---|
| Reason Code of the CRL Entry | For CRL Entries of Root CA, Subordinate CA and Cross-Certifier Subordinate CA reasonCode is always present.<br><br>For Certificates not capable of issuing certificates reasonCode is present unless reasonCode is "unspecified (0)" |
| Revocation Date | Date and time when certificate was revoked |

## 7.3 OCSP profile

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

### 7.3.1 Version number(s)

Version 1 of the OCSP specification as defined by RFC6960 (X.509 Internet Public Key Infrastructure Online Certificate Status Protocol) is implemented for the OCSP responders.

### 7.3.2 OCSP extensions

OCSP nonce extension should be used in requests.

# 8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The purpose of a compliance audit is to verify that the Telia root CAs and SubCAs operate accordance with this CP/CPS. Telia CA selects an independent Qualified Auditor for auditing its compliance assessments.

## 8.1 Frequency or circumstances of assessment

Telia CA maintains its compliance with the WebTrust/ETSI standards via a Qualified Auditor on an annual and contiguous basis.

## 8.2 Identity/qualifications of assessor

The CA's audit will be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

a. Independence from the subject of the audit;
b. The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section 8.4);
c. Employs individuals who have proficiency in examining PKI technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
d. (For audits conducted in accordance with any one of the ETSI standards) accredited in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403;
e. (For audits conducted in accordance with the WebTrust standard) licensed by WebTrust;
f. Bound by law, government regulation, or professional code of ethics; and
g. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage

## 8.3 Assessor's relationship to assessed entity

The Qualified Auditor should not have any financial, legal or organisational relationship with the audited party.

## 8.4 Topics covered by assessment

Telia CA undergo an audit in accordance with at least one of the following schemes:

1. "WebTrust for CAs v2.1 or newer" AND "WebTrust for CAs SSL Baseline with Network Security v2.3 or newer"; or
2. ETSI EN 319 411-1 v1.2.2, which includes normative references to ETSI EN 319 401 (the latest version of the referenced ETSI documents should be applied); or
3. If a Government CA is required by its Certificate Policy to use a different internal audit scheme, it MAY use such scheme provided that the audit either
   a. encompasses all requirements of one of the above schemes or
   b. consists of comparable criteria that are available for public review.

The audits incorporate periodic monitoring and/or accountability procedures to ensure that its audits continue to be conducted in accordance with the requirements of the scheme. The audit are conducted by a Qualified Auditor, as specified in Section 8.2.

For Delegated Third Parties which are not Enterprise RAs, then Telia CA obtains an audit report, issued under the auditing standards that underlie the accepted audit schemes found in Section 8.4, that provides an opinion whether the Delegated Third Party's performance complies with either the Delegated Third Party's practice statement or the CA's Certificate Policy and/or Certification Practice Statement. If the opinion is that the Delegated Third Party does not comply, then Telia CA will not allow the Delegated Third Party to continue performing delegated functions.

The audit period for the Delegated Third Party will not exceed one year (ideally aligned with the CA's audit). However, if the CA or Delegated Third Party is under the operation, control, or supervision of a Government Entity and the audit scheme is completed over multiple years, then the annual audit covers at least the core controls that are required to be audited annually by such scheme plus that portion of all non-core controls that are allowed to be conducted less frequently, but in no case may any non-core control be audited less often than once every three years.

## 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 Subscribers 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 Audit Report states explicitly that it covers the relevant systems and processes used in the issuance of all Certificates that assert one or more of the policy identifiers listed in Section 7.1.6.

Telia CA ensures its Audit Report publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, Telia CA provides an explanatory letter signed by the Qualified Auditor.

An authoritative English language version of the publicly available audit information will be provided by the Qualified Auditor and Telia CA ensures it is publicly available in PDF.

## 8.7 Self-audits

During the period in which Telia CA issues Certificates, the CA monitors adherence to its CP/CPS and CA/B Forum Requirements and strictly control its service quality by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

Telia CA has no delegated Trusted Third-Parties applicable to this CP/CPS that are applicable of self-audits.

# 9 OTHER BUSINESS AND LEGAL MATTERS

## 9.1 Fees

Fees are defined in applicable Subscriber 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

Subscriber pays Telia for a service and its use pursuant to a pricelist or agreement according to invoicing periods defined by Telia.

## 9.2 Financial responsibility

### 9.2.1 Insurance coverage

Telia CA maintain Professional Liability/Errors & Omissions insurance with a policy limit of at least 1 million Euros in coverage.

### 9.2.2 Other assets

No stipulation.

### 9.2.3 Insurance or warranty coverage for end-entities

Warranty coverage is explained in section “9.6 Representations and warranties”.

## 9.3 Confidentiality of business information

All Subscriber’s information that is collected, generated, transmitted, or maintained by the issuer is classified in accordance with the Telia’s Group Security Policy.

Information published in the Repository such as public certificates or certificate revocation information are not considered as confidential.

### 9.3.1 Scope of confidential information

The following information are kept confidential and private:

- CAs, RAs application records whether approved or rejected
- CAs and RAs audit reports
- CAs business continuity plan
- Security policy and related information
- Private keys
- Any other information identified as confidential by the PMT or the CAs that needs

to be considered confidential

Telia will disclose confidential information where this is required by law or by a decision of a court or public authority. Private keys linked to issued certificates cannot be disclosed when these are not stored by Telia.

### 9.3.2 Information not within the scope of confidential information

The following information is not deemed to be confidential in the relation between the CA and keyholder:

a. Information in issued certificates including public keys (but not private keys)
b. Revocation lists and OCSP responses
c. General Subscriber Agreement and CPSes

Exceptions may apply to key holder information if this is stated in a specific agreement with the key holder's organisation.

### 9.3.3 Responsibility to protect confidential information

All confidential information will be physically and/or logically protected by CA from unauthorised viewing, modification, or deletion.

Storage media used by the CA system is protected from environmental threats such as temperature, humidity and magnetism and that also applies to backup and archive media.

Confidentiality keys will in some cases be backed up by Telia, and in those cases the keys will be protected in accordance with Section 6, and will not be disclosed without prior consent of the Subscriber or a duly authorised representative of the issuing CA.

## 9.4 Privacy of personal information

Telia does not collect any sensitive or confidential data from Subscriber. Except in scenarios where the CA or RA archive copies of identification documents to validate the identity of a Subscriber. The collected personal information will not be used for any other purpose and Telia's privacy policy [4] governs the CA operations. Telia's Privacy Notice applies to all processing of personal data [5].

## 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 Company AB.

However, permission generally applies for reproducing and disseminating this CPS in its

[4] Telia Group Policy - Privacy and Data Protection: https://www.teliacompany.com/globalassets/telia-company/documents/about-telia-company/public-policy/group-policy---privacy-and-data-protection.pdf

[5] Telia Privacy Notice: https://www.telia.fi/tietosuoja-ja-tietoturva/privacy-notice

entirety if 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

### 9.6.1 CA representations and warranties

Telia CA (Root CA and Subordinate CA) makes no representation concerning the quality of the Services and does not promise that the Services will: (a) meet the Subscriber's requirements or be suitable for a particular purpose, including that the use of the Services will fulfil or meet any statutory role or responsibility of the Subscriber; or (b) The provided Services will be error free.

### 9.6.2 RA representations and warranties

The CA bears overall responsibility for the issued certificates. Registration responsibilities of the CA's overall responsibility can, however, be transferred through an agreement between the CA and a Relying Party, to the Relying Party, when the last-mentioned party acts also as Registration Authority.

Telia will require that all Registration Officers comply with all the relevant provisions of this CPS.

The Registration Officer is responsible for the identification and authentication of Subscribers according to section 3.2. The Registration Officer is also responsible for revoking certificates in accordance with the CPS.

Registration Officers are individually accountable for actions performed on behalf of a CA. Individually accountability means that there must be evidence that attributes an action to the person performing the action (audit logs). Records of all actions carried out in performance of RA duties shall identify the individual who performed the duty. When an RA submits Subscriber information to a CA, it will certify to that CA that it has authenticated the identity of that Subscriber and that the Subscriber is authorised to submit a certificate request in accordance with the CPS.

Submission of the certificate request to the CA will be performed in a secure manner as described in the CPS.

All Registration Officers are authenticated when performing any actions in the RA applications. The audit logs are the main tool to control any misuse of the RA personnel's authorities. For the processes authenticating the RA personnel see section 5 of this CPS.

Responsibilities of chapter 9.6.3 applies.

### 9.6.3 Subscriber representations and warranties

Telia will require that Subscribers comply with all the relevant provisions of this CPS. Subscribers are required to protect their private keys, associated pass phrase(s) and

tokens, as applicable, and to take all reasonable measures to prevent their loss, disclosure, modification, or unauthorised use.

Prior to the issuance of a Certificate Telia CA shall obtain either

1. The Applicant's agreement to the Subscriber Agreement with the CA, or
2. The Applicant's acknowledgement of the Terms of Use.

Any Subscriber information shall be complete, validated, and accurate with full disclosure of all required information in connection with a certificate or a query to a CA.

The Subscriber shall only use the keys and certificates for the purposes identified in applicable CPS and in any applicable agreement(s).

When a Subscriber suspects a private key compromise, the Subscriber shall notify Telia CA according to the information of section 1.5.1.

Telia is not a trustee, agent, fiduciary, or other representative of the Subscriber and the relationship between Telia and the Subscriber is not that of an agent and a principal. Telia makes no representation to the contrary, either implicitly, explicitly, by appearance or otherwise. The Subscriber does not have any authority to bind Telia by contract, agreement or otherwise, to any obligation.

### 9.6.4 Relying party representations and warranties

Telia will require that Relying Parties comply with all the relevant provisions of this CPS.

Prior to accepting a Subscriber's 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
c. Check the status of the certificate against the appropriate and current CRL or OCSP Responder in accordance with the requirements stated in this CPS. As part of this verification process the digital signature of the CRL or OCSP Responder should also be validated. If certificate status can't be received due to system failure or similar, the certificates shall not be accepted

It is also up to the relying party to study this CPS to decide whether the security level of the issuance process is appropriate for the actual application where to be used.

Telia will provide certificate status information identifying the access point to the CRL or on-line certificate status server in every certificate Telia issues in accordance with this CPS.

### 9.6.5 Representations and warranties of other participants

Telia will notify Mozilla (and other Application Software Providers, browsers and/or root stores) if a CA private key is suspected to have been compromised.

When a third-party suspect a private key compromise, the third-party shall notify Telia CA according to the information of section 1.5.1.

## 9.7 Disclaimers of warranties

Telia CA accepts no liability for damages incurred by a relying party accepting one of its certificates, or by a Subscriber whose valid certificate is refused or whose revoked certificate is unduly accepted by a Relying Party. It also accepts no liability for damages arising from the non-issuance of a requested certificate, or for the revocation of a certificate initiated by the CA or the appropriate RA acting in conformance with this CPS.

## 9.8 Limitations of liability

Telia assumes no liability except as stated in the relevant Subscriber contracts pertaining to certificate issuance and management.

## 9.9 Indemnities

Telia CA will not pay indemnities for damages arising from the use or rejection of certificates it issues. Subscribers shall indemnify and hold harmless the Telia and all appropriate RAs operating under the applicable CPS against all claims and settlements resulting from fraudulent information provided with the certificate application, and the use and acceptance of a certificate which violates he provisions of this 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 Repository.

### 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 Repository, 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

The PMT 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 PMT.

Subscribers will not be notified if the CPS document is changed. When changes are made, they will be published in the Repository for public review and after 15 days will be in effect. Changes to the Telia Group Security Policy will be communicated to third parties, where applicable.

Non normative changes to this CP/CPS (like fixing of broken links, font type face changes, document style corrections / modifications etc.) may be made without executing the said 15 days notice / comment period if approved by PMT according to provisions set forth in this section.

This CPS and Telia Group Security Policy is regularly reviewed and checked against Telia CA's security policies and interval between subsequent checks shall not exceed twelve (12) months. Such check is documented by the PMT in its records.

### 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 PMT will post the notification at the CPS publishing point at the Repository. 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.

The PMT 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

Telia notify an amendment to this CPS by publishing it to the Repository.

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.

### 9.12.3 Circumstances under which OID must be changed

If the PMT determines that a new OID is required, the PMT will assign a new OID and required amendments will be made.

## 9.13 Dispute resolution provisions

Before taking any Court action, a party must use best efforts to resolve any dispute under through good faith negotiations. Otherwise, any disputes arising from or relating to this CPS shall be finally settled by arbitration in accordance with the Arbitration Rules of the Finland Chamber of Commerce. The number of arbitrators shall be one, unless the other party requires that the arbitral tribunal be composed of three members. The place of arbitration is Helsinki, Finland, and the language of the arbitration is Finnish. Without prejudice to the above, the parties have the right to bring a legal action at the Helsinki District Court when the value of the dispute does not exceed one hundred thousand (100,000) Euros.

## 9.14 Governing law

This CPS is governed by, and must be interpreted in accordance with, the laws of Finland

without regard to the conflict of law provisions.

## 9.15Compliance with applicable law

All activities including the request, validation, issuance, use or acceptance of a Telia CA certificate shall comply with Finnish law. Activities initiated from or destined for another country than Finland are also subject to applicable law of that country.

## 9.16Miscellaneous provisions

### 9.16.1 Entire agreement

The interpretation and enforcement requirements in this section are reflected in the applicable Subscriber and Relying Party Agreements.

### 9.16.2 Assignment

Any entities operating under this CPS may not assign their rights or obligations without the prior written consent of Telia CA.

### 9.16.3 Severability

If any provision of this CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CPS will remain valid and enforceable. Each provision of this CPS that provides for a limitation of liability, disclaimer of a warranty, or an exclusion of damages is severable and independent of any other provision.

In the event of a conflict between these Requirements and a law, regulation or government order (hereinafter 'Law') of any jurisdiction in which a CA operates or issues certificates, Telia CA may modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction. This applies only to operations or certificate issuances that are subject to that Law.

If Telia CA chooses to modify requirements as said foregoing chapter, Telia CA shall execute the following:

- Prior to issuing a certificate under the modified requirement
    - include in this Section of this CP/CPS a detailed reference to the Law requiring a modification of these Requirements under this section, and the specific modification to these Requirements implemented by Telia CA.
    - inform CA/Browser forum in accordance with the Baseline Requirements

Any modification to Telia CA practice enabled under this section shall be discontinued if and when the Law no longer applies, or the Baseline Requirements are modified by CA/Browser Forum to make it possible to comply with both them and the Law simultaneously.

An appropriate change in practice, modification to this CP/CPS and a notice to the CA/Browser Forum, as outlined above, shall be made within 90 days.

### 9.16.4 Enforcement (attorneys' fees and waiver of rights)

Telia CA may seek indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct.

### 9.16.5 Force Majeure

Telia shall not be held responsible for any delay or failure in performance of its obligations hereunder to the extent such delay or failure is caused by fire, flood, strike, civil, governmental or military authority, acts of terrorism or war, sabotage, or other similar causes beyond its reasonable control and without the fault or negligence of Telia or its subcontractors.

## 9.17 Other provisions

Telia CA as part of the Telia Company adhere with the company level policies such as cybersecurity, privacy and HR. Particularly, the CA aims at providing non-discriminatory services to ensure equal opportunities for persons with disabilities whenever feasible.

Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the CA will also notify the natural or legal person of the breach of security or loss of integrity without undue delay.