Certificate Policy and Certification Practice Statement for Telia Client Certificates

Prepared by the Telia's Certification Authority Policy Management Team

Release: 2.0

Valid From: 2021- 02-17

Status: Released

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

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), Customers, Subscribers or Relying Parties.

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 current 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**: 2.0
- **OID**: 1.3.6.1.4.1.271.2.3.1.2.2
- **Location**: http://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:

Certificate type	Issuing CA	CP OID
User certificates for corporate Customers (Finnish Registration Authority (RA))	TeliaSonera Class 1 CA v2	1.3.6.1.4.1.271.2.3.1.1.11
User certificates for corporate Customers (Swedish RA)	TeliaSonera Class 2 CA v2	1.3.6.1.4.1.271.2.3.1.1.12
Short-lived personal certificates for individuals (External RA)	Telia Class 3 CA v1	1.3.6.1.4.1.271.2.3.1.1.13
Email certificates for Telia Group	TeliaSonera Email CA v4	1.3.6.1.4.1.271.2.3.1.1.14
User certificates for corporate Customers (Swedish RA)	Customer specific CA under TeliaSonera Root CA v1 or Telia Root CA v2	1.3.6.1.4.1.271.2.3.1.1.18

1.3 PKI participants

Telia Root CA will issue subordinate CA certificates to Telia and Customers of Telia that are hosting their CA at Telia as subCAs of TeliaSonera Root CA v1 or Telia Root CA v2.

A Customer 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 the Telia CA.

Telia CA will issue certificates mainly to Customers 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” (BusinessID 1475607-9). Telia Finland Oyj is part of Swedish company “Telia Company AB” (businessID 5561034249).

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, TeliaSonera Root CA v1 is cross-signed by Sonera Class2 CA. 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 keys and exist simultaneously. Clients can use either one when doing PKI path validation.

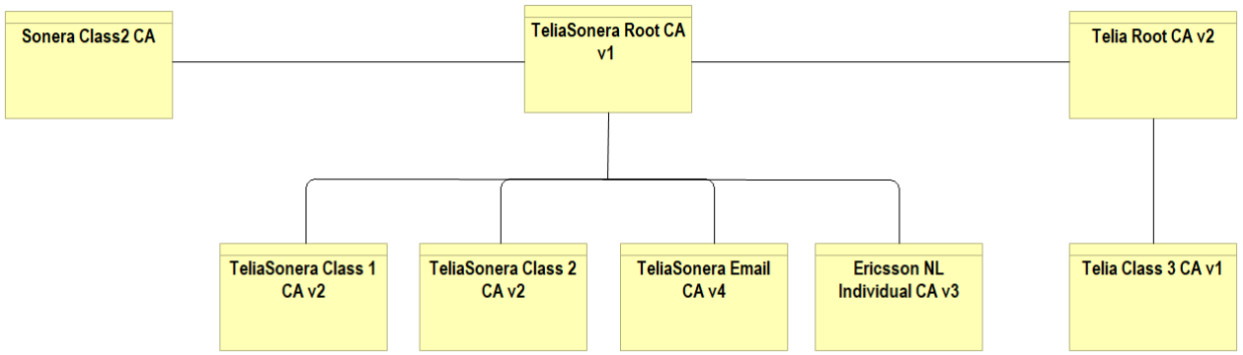

Figure 1, Telia CA Client Certificate PKI Hierarchy

The CA's 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 CPS covers all certificates issued and signed by the following CAs aka Telia CA.

Root CAs

- **Sonera Class2 CA**
  SHA2 Fingerprint: 7908B40314C138100B518D0735807FFBFCF8518A0095337105BA386B153DD927
- **TeliaSonera Root CA v1**
  SHA2 Fingerprint: DD6936FE21F8F077C123A1A521C12224F72255B73E03A7260693E8A24B0FA389
- **Telia Root CA v2**
  SHA2 Fingerprint: 242B69742FCB1E5B2ABF98898B94572187544E5B4D9911786573621F6A74B82C

Cross-signed Root CAs

- **TeliaSonera Root CA v1**
  SHA2 Fingerprint: E9563581E712B290F23A749346535EB0D981E3D4A39D56D604684CD0B1698C89
- **Telia Root CA v2**
  SHA2 Fingerprint: EF6F29F636F62BDD4753122F41F3419EE7C2877587BE4A9807ADF58946458E7F

Intermediate CA's

- **TeliaSonera Class 1 CA v2**
  SHA2 Fingerprint:
  B95AE54F838E3ABF0B57ACCC1B1266DC68C7A3FA774015FA128D60CDD1AAE280
- **TeliaSonera Class 2 CA v2**
  SHA2 Fingerprint:
  092829433D231949F4A9BC666CBF54B3AA27D7BEBCA048D75E59093E15A72EA5
- **TeliaSonera Email CA v4**
  SHA2 Fingerprint: D1F2656AC8382739A3B087C47AB5CAB945A32F162B6149C308783C7E06AF8AE8
- **Telia Class 3 CA v1**
  SHA2 Fingerprint: E7340DC9475E87C4E5A4572C82604C5EFF9BF60B231C5486943173B26A4CAFCC
- **Ericsson NL Individual CA v3**
  SHA2 Fingerprint: 63ED95B17FFDCB7AE30FEAC6A874653099264E21B268D836D957966F0B04BE43

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, Customer Organisations acting as Customers 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.

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 Customers	TeliaSonera Class 1 CA v2	Finnish RA systems and RA processes
User certificates for corporate Customers	TeliaSonera Class 2 CA v2	Swedish RA systems and RA processes
Email certificates for Telia Group	TeliaSonera Email CA v4	Special Telia internal RA system

The Registration Officer can be a physical person or a Virtual Registration Officer, e.g., a Telia's or Customer Organisation's system that is used to authenticate individual identity and submit the certificate request to the CA system. Virtual Registration Officer System shall be approved by the CA.

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	External RA that has partnership with Telia

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

1.3.3 Subscribers

Subscribers are legal or natural entities to whom certificates are issued according to this CPS and are in possession of the private keys corresponding to their certificates. A subscriber may be an organisation that is a Customer of Telia, or an individual employed by Telia or employed by a Customer to Telia.

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.

1.3.4 Relying parties

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

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 partners to assist in providing the certificate services to the 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.

A Certificate Manufacturer within Telia PKI is the Card Manufacturer responsible for the Smart Card life cycle.

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 customers. Telia considers such External Partners as External 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 subCAs
- 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	Certificate uses	OID
TeliaSonera Class 1 CA v2	TeliaSonera Class 1 certificates are issued for persons and devices within Telia's Customers and Telia. The certificates are intended for Customer's internal use in VPN, login, email and other similar services and are not intended to be used or relied outside the Customer.	1.3.6.1.4.1.271.2.3.1.1.11
TeliaSonera Class 2 CA v2	TeliaSonera Class 2 certificates are issued for persons within Telia's Customers and Telia. The certificates are intended for securing email and other similar services.	1.3.6.1.4.1.271.2.3.1.1.12
TeliaSonera Email CA v4	TeliaSonera Email CA issues individual certificates to be used for signing and encrypting e-mails. Certificates are issues to Telia employees within the Telia Group and to individuals contracted by Telia.	1.3.6.1.4.1.271.2.3.1.1.14
Telia Class 3 CA v1	Short-lived personal certificates for document signing by natural individuals.	1.3.6.1.4.1.271.2.3.1.1.13

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", "Time stamping" and "OCSP signing" 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 Company AB SE-169 94 Solna, Sweden Phone: +46 8 504 550 00 Internet: https://support.trust.telia.com/support_feedback_lomake_en.html

1.5.2 Contact person

Contact person in matters related to this CPS:

Telia CA Policy Management Team (PMT) Email: cainfo@telia.fi Phone: +358 20 401 Internet: https://cps.trust.telia.com/CPS

Other contact information:

Finland	Customer Service: +358 20 693 693 Revocation Service: +358 800 156 677 Support: cainfo@telia.fi
Sweden	Customer Service and Revocation: 020 323 262, +46 771 323 262 kundtjanst-eid@teliacompany.com

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.

1.6 Definitions and acronyms

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

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

2.1.1 CPS Repository

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

2.1.2 Revocation Information Repository

Following CRLs are published in the Telia's website:

Issuing CA	**CRL addresses**
Sonera Class 2 CA	http://httpcrl.trust.telia.com/soneraclass2ca.crl
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
Telia Class 3 CA v1	http://httpcrl.trust.telia.com/teliaclass3cav1.crl
Ericsson NL Individual CA v3	http://crl.trust.telia.com/ericssonnlindividualcav3.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 Customer agreement and the payment method.

2.1.3 Certificate Repository

CA certificates are published at https://cps.trust.telia.com/. All issued certificates are stored in the local database of the CA system. Certificates may also be published to other repositories if it is a part of the Telia CA Service or agreed with a Customer.

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.

2.3 Time or frequency of publication

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

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 Subscriber certificates or root CA level information stored in the local database of the CA system.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

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

Attribute	**Description of value (Sonera Class 2 CA)**	**Description of value (TeliaSonera Root CA v1)**	**Description of value (Telia Root CA v2)**
commonName (CN, OID 2.5.4.3.)	Sonera Class2 CA	TeliaSonera Root CA v1	Telia Root CA v2
OrganizationName, (O, OID 2.5.4.10)	Sonera	Telia	Telia Finland Oyj
Country (C, OID 2.5.4.6)	FI	-	FI

3.1.1.2 Subordinate CAs

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

3.1.1.3 Client Certificates

Attribute	**Description of value**
commonName (CN, OID 2.5.4.3)	Name of the Subject.
OrganizationName (O, OID 2.5.4.10)	Customer Organisation in relation to which the Subject is identified.

Additionally, the “Subject” field may include all or some of the following attributes depending on the usage purpose of the certificate:

Attribute	**Description of value**

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 otherwise similar Subject names, e.g. personal ID number or username.
organizationalUnitName (OU, OID 2.5.4.11)	Determined by the application or the implementation of the service with which the certificate is used.
State or province (ST, OID 2.5.4.8)	Qualifier for describing the location of the Subscriber or the Subject.
Locality (L, OID 2.5.4.7)	Qualifier for describing the location of the Subscriber or the Subject.
Country (C, OID 2.5.4.6)	Qualifier for describing the 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.

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.
iPAddress	iPAddress field may contain one or more IP addresses of the Device.

Additional Distinguished Name (DN) and Subject Alternative Name attributes may be used as necessary if they are verified by CA.

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 contains always a Customer Organisation's name that accurately identifies the customer.

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	The commonName is composed of the username or similar used by the Customer Organisation to identify users or devices in the VPN or other service that the certificates are used for.
TeliaSonera Class 2 CA v2 **TeliaSonera Email CA v4**	The commonName is composed of the given and sur name of the Subject, and it can additionally contain other given names or initials. 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 resources such as Swedish BankID.
Ericsson NL Individual CA v3	The commonName is composed of the given and surname of the Subject, and it can additionally contain other given names or initials. 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 Customer Organisation in relation to which the Subject is identified. Normally Organisation 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 Organisation name attribute that is other than the official registered name of the Organisation, if the name is commonly used or there is otherwise no risk of confusion.

The Organization (O) attribute states the Customer 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 Customer Organisation is not able to change the organisation name that the CA has recorded for the organisation in the CA system. The Customer 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 Customer 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

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, e.g. it's generated by the Customer Organisation, the CA or RA can verify the possession of the private key by verifying the electronic signature included in the certificate request.

3.2.2 Authentication of organisation identity and/or domain name

Telia verifies the organisation name of a new Customer Organisation by checking the existence of the company. Its legal name, business identity code and other relevant organisation information are confirmed from an official business register maintained by an applicable government agency (e.g., ytj.fi in Finland) 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 Customer Organisation.

3.2.3 Authentication of individual identity

The Customer Organisation can agree with Telia to act as a Registration Officer within the Customer Organisation and to register Telia certificates for the persons or client devices related to the organisation. The Customer Registration Officer is restricted to register certificates only within their own Organizations (O). Before enabling the service, the CA verifies the organisation's identity as described in section 3.2.2.

For the short-lived certificates Customer Organisation does not do the identity verification process because Telia already ensures verification of the identities using trusted identity sources (e.g. Swedish Bank ID).

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

TeliaSonera Class 1 CA v2	Telia or Customer Registration Officer 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. 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. . 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. If CA API connection is used CA will pre-approve all allowed domain names and O values that can be used in Customer Subject data.
TeliaSonera Class 2 CA v2	Customer or Telia Registration Officer is responsible for authenticating the Subject. The Registration Officers are obliged to follow the policies and instructions given by the CA. 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 including the email address, Or the Registration Officer should verify the information by checking the Subject's identity card.
TeliaSonera Email CA v4	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: - givenName (G) - surName (S) - commonName (CN) - Serial Number
Ericsson NL Individual CA v3	The Customer Organisation act as a Registration Officer within the Customer Organisation and to register certificates for the persons or client devices related to the organisation. Customer is responsible for authenticating the Subject. The Registration Officers are obliged to follow the policies and instructions given by the CA. 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 including the email address, or the Registration Officer should verify the information by checking the Subject's identity card.

3.2.4 Non-verified Subscriber information

Domain name ownership of domains in email addresses is not verified by Telia except when CA API is utilized by the Customer. Telia verifies only the following Subject information:

TeliaSonera Class 1	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 Customer

CA v2	Registration Officer is responsible for verifying the other subject information according to the Customer's internal policy. Telia does not verify other information within the certificate request.
TeliaSonera Class 2 CA v2	Telia verifies Organization Name (O) information as described in section 3.2.2. Customer or Telia Registration Officer is required to verify the following Subject information as described in section 3.2.3: - commonName (CN) If emailAddress (EA), surName (S) and givenName (G) attributes or Subject Alternative Name extensions are used then the Registration Officer should verify them also. Other information is not verified by Telia or Customer Organisation.
TeliaSonera Email CA v4	Telia verifies the following Subject information as described in section 3.2.3: - commonName (CN) - emailAddress (EA) - serialNumber - Organization Name (O) Telia does not use other subscriber information within the certificate request.
Ericsson NL Individual CA v3	The Customer Registration Officer is required to verify the following Subject information as described in section 3.2.3: - commonName (CN) If email address (EA), Surname (S) and givenName (G) attributes or Subject Alternative Name extensions are used then the Registration Officer should verify them also. Other information is not verified by Telia or Customer Organisation.

3.2.5 Validation of authority

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

Physical and logical access controls are used to restrict access to CA management operations for the authorised CA personnel only. Multiple trusted CA personnel are required to gain access to create a new CA or CA certificate in the CA system.

TeliaSonera Class 1 CA v2 **TeliaSonera Class 2 CA v2** **Ericsson NL Individual CA v3**	The Administrative Contact Person, who grants the necessary authorisations in the Customer 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 Customer's PBX number or by making a call to some other verified number in the organisation, which is looked up from a directory maintained by a trusted party. 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. 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 Customer. 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	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.

3.2.6 Criteria for interoperation

Not applicable.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

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

Revocation by Customer Organisation

Customer'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 Customer Organisation. In the latter case The Revocation Officer is responsible for the verification of the authenticity 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.

Revocation by the Revocation Service of the CA

The Subject, or Subscriber, or Registration Officer in a Customer Organisation 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 digital signature or the Revocation Service will make a call back to the Customer Organisation 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 Customer Organisation. If the data match the certificate will be revoked.

In certain situations where there is an identified risk of abuse of the private key or when it is obvious that the authorised use of the key is prevented, it may be necessary to revoke the certificate 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.

Revocation of CAs

The authorised CA personnel can request revocation of a CA certificate. Authorised Customer contact person can request revocation of that Customer's CA certificate.

Customer contact person requesting revocation is authenticated by digital signature, call-back to the Customer 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.

Two-factor authentication mechanisms are used to authenticate users to CA system. Multiple trusted persons of CA are required to gain access to revoke a CA certificate in the CA system.

Reinstatement of suspended certificate

Customer Registration Officers may reinstate suspended certificates in their own organisations if there is such service agreement with CA.

Reinstatement of a suspended certificate can be requested by the Subject or by the Registration Officer operating in the Customer Organisation. A request from the Subject will be executed only after confirmation from the Registration Officer. A request or confirmation received from the Registration Officer in an e-mail message or in an electronic form will be verified based on an electronic signature, or the Registration Officer shall be authenticated using certificates, some other strong authentication or by making a call back to the Customer Organisation and asking and checking data recorded of the Subject or Registration Officer at registration, or checking information that can be found in the agreements made with the Subscriber or Customer Organisation.

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 Customer that has made an agreement to host their CA at Telia.

4.1.1.2 Client Certificates

TeliaSonera Class 1 CA v2 **TeliaSonera Class 2 CA v2** **Ericsson NL Individual CA v3**	When a certificate is requested for a person or Device, it is required that the ordering organisation is a customer of Telia with which the Subject has a contractual relation. Certificate request can be submitted by a. A Registration Officer in a Customer Organisation b. An employee or other individual contracted by a Customer Organisation (Subject) c. An Administrative contact person of a Customer Organisation
TeliaSonera Email CA v4	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 in order to use the certificate services.

Authorised Telia personnel can also submit certificate applications.

4.1.2 Enrolment process and responsibilities

A Customer that has agreed to and executed an Agreement with Telia can have a hosted CA at the Telia CA. In the Agreement, the Customer 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. An internal Telia CA Installation Form document is used for the final application.

Multiple trusted persons 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. An internal Telia CA Installation Form document is used for such applications.

4.1.2.2 Client certificates

TeliaSonera Class 1 CA v2 **TeliaSonera Class 2 CA v2** **Ericsson NL Individual CA v3**	Certificates can be applied for either through the RA office of the CA or directly from the CA system by using the tools delivered by the CA. a. The Registration Officer in the Customer Organisation 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 Registration Officer or the Subject generates the key pair and submits the certificate request to the CA system containing the certificate information defined by the Registration Officer during the pre-registration and the public key. 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 using browser software and submits the certificate request containing the certificate information. The Registration Officer in the Customer Organisation verifies the information in the request and sends the Subject a link to pick up the issued certificate. c. The self-service software provided by Telia is integrated with the existing authentication solution at the customer site. The subject uses the user credentials in the customer organisations authentication solution to enrol for a certificate (applicable to **Ericsson NL Individual CA v3**). d. Certificate is applied for through the RA office of the CA. The Registration Officer 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 Registration Officer of the Customer Organisation. The Customer Organisation is bound to registration policies and Customer responsibilities through a certification service agreement with Telia. Customer Organisation's Registration Officers also accept Customer Responsibilities when they logon to Telia's self-service application first time.
TeliaSonera Email CA v4	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.
Test and pilot certificates (for the above CAs)	<u>TeliaSonera Class 1, Class 2 and E-mail certificates</u> The CA has granted special authorities to a few of its employees to apply for test certificates for tests that must be carried out in the production system. The applicant of a certificate is authenticated based on his certificate. One of the following details in the contents of the "Subject" field of a certificate will serve as an indication of a test certificate: - the word "Test" or "Testi" comprises the contents of the "Organization Name" field (the primary method), - the "Common Name" field contains the word "test", or - another field contains the word "test". A test certificate is valid at most seven (7) days or it shall always be revoked after seven (7) days of its coming into force, at the latest. If such a test case emerges where the contents of the certificate cannot indicate the test nature of the certificate, it must be revoked immediately after the test. The CA has granted a few of its employees' special authorities to apply for certificates in the pilot phase of information security services of Sonera, when

	the registration responsibilities have not yet been moved to the RA office of the CA. The applicant of a pilot certificate is authenticated based on his certificate. The same certificate application requirements, which apply in the production phase of the service, shall be followed when applying for pilot certificates.
Telia Class 3 CA v1	1. User will receive an email with a link from signing portal. 2. User will click on the link and will then have to be to be authenticated (e.g. Swedish Bank ID[1]). 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). 4. Telia will issue a certificate with short validity. 5. Issued certificate will be used in signing operation and it will be deleted immediately afterwards.

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.

4.2.2 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 Customer.

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.

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

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 Client certificate issuance

TeliaSonera Class 1 CA v2 **TeliaSonera Class 2 CA v2** **Ericsson** NL **Individual CA v3**	The certificate is available for the Customer Organisation's Registration Officer or for the Subject in the registration tool after the issuance.
TeliaSonera Email CA v4	The certificate is available for 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

4.4.1 Conduct constituting certificate acceptance

The Subject, or when certificates to Devices are concerned, the Subscriber, is considered to have accepted the certificate when the private key associated with it has been used for the first time, or when the certificate has been installed into a device.

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 Customer 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 before their usage will start.

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 as long as 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 than 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 Customer Service.

4.7.3 Processing certificate re-keying requests

TeliaSonera Class 1 CA v2	If the certificate re-key is started by the Registration Officer in the Customer Organisation, 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

TeliaSonera Class 2 CA v2 **Ericsson NL Individual CA v3**	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. 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	Re-key is processed in the same way as the initial certificate application as described in section 4.1 – 4.4.

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 in writing
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 for 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 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

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 Baseline Requirements of Sections 6.1.5 and 6.1.6
2. Telia CA obtains evidence that the certificate was misused
3. Telia CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use
4. Telia CA is made aware of any circumstance indicating that use of a FQDN
5. 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)
6. Telia CA is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subordinate FQDN
7. Telia CA is made aware of a material change in the information contained in the certificate;
8. Telia CA is made aware that the certificate was not issued in accordance with the Baseline Requirements or the applicable CSP
9. Telia CA determines or is made aware that any of the information appearing in the certificate is inaccurate
10. Telia CA's right to issue certificates under the Baseline Requirements expires or is revoked or terminated, unless Telia CA has agreed to continue maintaining the CRL/OCSP Repository
11. Revocation is required by Telia CA' applicable CPS
12. Telia CA is made aware of a demonstrated or proven method that exposes the Subscriber's private key to compromise, methods have been developed that can easily calculate it based

on the public key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the private key was flawed.

4.9.2 Who can request revocation

The revocation of a certificate can be requested by:

1. A Subject whose name the certificate is issued under
2. A Subscriber or Registration Officer in the Customer Organisation 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 Customer 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.

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. The Registration Officer in the Customer Organisation makes the revocation request using the administration interface

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

If the revocation request cannot be carried out in accordance with a) or b), the Registration Officer in the Customer Organisation 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 immediately inform the Revocation Service directly or the Customer Organisation through its Registration Officer. Also the Registration Officer shall revoke the certificate using the administration interface or inform Telia's Revocation Service immediately, 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 Customer.

4.9.6 Revocation checking requirement for relying parties

Prior to using a certificate, it is the Relying Party's responsibility to check the status of all certificates in the certificate validation chain 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 one year
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 customer

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

4.9.8 Maximum latency for CRLs

Normally latency will be a matter of seconds and latest within five minutes.

4.9.9 On-line revocation/status checking availability

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

The service is only accessible provided that the Relying Party has an agreement with Telia. Availability of the service will be provided in the agreement.

4.9.10 On-line revocation checking requirements

In general, all OCSP requests will be signed.

All responses will be signed by a private key corresponding to a public key certified by the CA on which the OCSP request is made. A separate key pair will be used for the responses of each CA.

OCSP service uses online checking from the CA database...

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.

4.9.13 Circumstances for suspension

Suspension is not used after March 2013.

4.9.14 Who can request suspension

Suspension is not used after March 2013.

4.9.15 Procedure for suspension request

Suspension is not used after March 2013.

4.9.16 Limits on suspension period

Suspension is not used after March 2013.

4.10 Certificate status services

4.10.1 Operational characteristics

The CRLs are published in Telia's website as disclosed in section 2.1.2.

4.10.2 Service availability

The certificate status services are available 24 hours per day, 7 days per week excluding scheduled maintenance or other planned breaks.

4.10.3 Optional features

Not applicable.

4.11 End of subscription

The end of a subscription as a result 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 as a result 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.

4.12 Key escrow and recovery

4.12.1 Key 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 be not be escrowed but Telia may keep a backup of the keys if so agreed between Telia and the Customer. 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 Customer.

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 a 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

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, which meet the requirements of Security and Audit Requirements..

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 (54B/2014) issued by Ficora (Finnish Communications Regulatory Authority). 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.

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. No keys or codes are left unmonitored.

In the case where the CA is a Customer'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 premises' external protection such as locks and alarm systems are monitored each day on a 24-hour basis by security staff on duty.

Unescorted access to the CA and RA sites and servers is limited to personnel identified on access lists. Personnel that is not included on the access lists will be escorted by authorised personnel and supervised during their work.

Site access is monitored in real time or access logs are inspected periodically at least quarterly by qualified personnel. The inspection documentation is retained for at least a one-year period to support audit requirements.

All access control and monitoring systems are tied to UPS's. The UPS systems are inspected and tested at least annually 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 by four tiers of physical security where the CA systems and other important CA devices have been placed in a security vault. At least one of the security vaults has been placed in a rock shelter that provide good structural security and fire protection for the CA equipment. Progressively restrictive physical access privileges control access to each tier.

The characteristics and requirements of each tier are described in the table below.

Tier	**Description**	**Access Control Mechanisms**
Physical Security Tier 1	Physical security tier one refers to the outermost physical security barrier for the facility.	Access to this tier requires the use of a proximity card employee badge and related PIN code. Physical access to tier one is automatically logged.
Physical Security Tier 2 "Facility hallways"	Tier two includes common areas including restrooms and common hallways.	Tier two enforces individual access control for all persons entering the common areas of the CA facility through the use of a proximity card employee badge. Physical access to tier two is automatically logged.
Physical Security Tier 3 "CA Security area"	CA Security Area is the room that separates the Security Vault from the common areas.	Access to CA Security Area requires the usage of an individual access card combined with a PIN code. In addition a separate burglar alarm system has to be inactivated by individual access codes. Physical access is automatically logged, video recorded and a special notification is generated to the PMT members about each access to CA Security Area.

Physical Security Tiers 4 "CA Vault"	The CA Security Vault is where the CA systems and other critical devices are placed and where sensitive CA operations occur. Tier four is the only tier where local maintenance access to servers is possible.	The tier four data centre enforces individual access control with a PIN code and it enforces dual control if incoming persons have access also to Tiers 5. Dual control is enforced through special individual partial access control to doors and burglar alarm systems. To such person or to outsider the authorisation for unescorted access to the tier four rooms is not given. Physical access to tier four is automatically logged and video monitored and a special notification is generated to the PMT members. The PMT member will always check, grant and document each access to Tiers 4.

Tier	**Description**	**Access Control Mechanisms**
Physical Security Tiers 5 "Key Management"	Key Management tiers five serve to protect CA HSMs keying material and other most critical components.	Online HSMs and other most critical components are protected through the use of locked cabinets that always require dual control to be accessed. Offline keying material like CA system or root key backups and secret shares are protected through the use of locked safes, cabinets and containers. Access to HSMs and keying material is restricted in accordance with Telia's segregation of duties requirements. The opening and closing of cabinets or containers in this tier is logged for audit purposes. All access is video monitored.

5.1.2.2 RA Site Physical access

The Telia RA systems are protected by four tiers of physical security, with access to the lower tier required before gaining access to the higher tier. Progressively restrictive physical access privileges control access to each tier. The characteristics and requirements of each tier are described in the table below.

Tier	**Description**	**Access Control Mechanisms**
Physical Security Tier 1	Physical security tier one refers to the outermost physical security barrier for the facility.	Access to this tier requires the use of a proximity card employee badge. Physical access to tier one is automatically logged.

Physical Security Tier 2	Tier two includes common areas including restrooms and common hallways.	Tier two enforces individual access control for all persons entering the common areas of the RA facility through the use of a proximity card employee badge. Physical access to tier two is automatically logged.
Physical Security Tier 3	Tier three is the first tier at which sensitive central RA systems are located and where operational activity takes place.	Tier three enforces individual access control through the use of two factor authentication including biometrics or proximity card employee badge and PIN code. Unescorted personnel are not allowed into a tier-three secured area. Physical access to tier three is automatically logged.
Physical Security Tiers 4	Tier four is used only in Telia Sweden. Tier four is the tier at which especially sensitive RA operations occur. There are two distinct tier four areas: the online tier four data centre and the offline tier four key storage room.	The tier four data centre enforces individual access control through the use of two factor authentication. Authorisations for unescorted access to tier four are not given to any individuals. Physical access to tier four is automatically logged and video monitored. Offline keying material like RA-system key backups and secret shares are protected through the use of safes. Access to keying material is restricted in accordance with Telia's segregation of duties requirements. The opening and closing of the safes are logged for audit purposes.

5.1.3 Power and air conditioning

Telia secure premises are equipped with primary and backup:

a. Power systems to ensure continuous, uninterrupted access to electric power
b. Heating/ventilation/air conditioning systems to control temperature and relative humidity

5.1.4 Water exposures

Telia has taken reasonable precautions to minimize the impact of water exposure to Telia systems. Exposure to water damages is prevented with structural solutions.

5.1.5 Fire prevention and protection

Telia has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. Telia's fire prevention and protection measures have been designed to comply with local fire safety regulations and Inergen gaz are used as extinguishing method in certain data centres.

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 the manufacturers' guidance prior to disposal. 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 Persons 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 central 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, including personnel having access to restricted portions of its repository
f. The handling of Subscriber information or requests

Trusted Persons include, but are not limited to:

a. Customer 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 Persons having a Trusted Position. Persons chosen to become Trusted Persons by obtaining a Trusted Position must successfully complete the screening requirements of section 5.3.

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

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

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

Security Manager:

Overall responsibility for the security of the Telia CA Service.

Information Systems Security Officer (ISSO):

Typical duties which may be administered by the ISSO include:

a. Works in conjunction with the SAs to get physical access to the systems where dual control is required
b. Supervision of the SAs work at the operational system level where dual control is required and responsible for that the SAs are carrying out their role within the framework of their authority
c. May have a degree of delegated security responsibility for the CA and RA services

Registration Officer:

RA Office and Customer Service staff of the CA. Registration Officers in the Customers are not trusted persons. 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 Customer accounts, privileges and values to enable Telia's self-service software for Customers.

Telia has chosen to divide the responsibility for the above roles into sub-roles in order to increase security. These roles are described in the Telia Operational Documentation.

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 multiple Trusted Persons.

These internal control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the device. Access to CA and central RA cryptographic hardware is strictly enforced by multiple Trusted Persons 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 split control over both physical and logical access to the device. No persons have alone both physical access to cryptographic modules and hold activation data. Requirements for CA private key activation data is specified in section 6.2.2.

Physical and operational system access to the central CA and certain RA servers require the participation of at least 2 Trusted Persons that works in conjunction. Either persons work physically together or the other Trusted Person 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 the 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 SA or RO do not simultaneously work in any of the other roles involving the system.

5.2.3 Identification and authentication for each role

For all personnel chosen to become Trusted Persons, verification of identity is performed through the personal (physical) presence of such personnel before Trusted Persons performing Telia HR [or equivalent] or security functions and a check of well-recognized forms of identification (e.g., passports, driver licenses and other nationally accepted identification cards). Identity is further confirmed through the background checking procedures described in section 5.3.1.

Telia ensures that personnel have achieved Trusted Status and departmental approval has been given before such personnel are:

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
e.

Each of these certificates and accounts (with the exception of the CA signing certificates) is:

a. Personal and directly attributable to the Trusted Person
b. Restricted to actions authorised for that role through the use of CA and RA software, operating system 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) takes 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, software based keys and certificates 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

The Trusted roles according to section 5.2.1 are assigned only to specially selected and reliable persons who have proved their suitability for such a position. Same personnel controls apply to Telia personnel and to affiliate or partner company personnel if Telia is outsourcing any Trusted roles.

Trusted persons may not have other roles which may be deemed to be in opposition to the role assigned.

Personnel identified to become Trusted Persons must present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily.

5.3.2 Background check procedures

Prior to commencement of employment in a Trusted Role, Telia conducts background checks. The actual background checks conducted depend on the local law and other circumstances. In Sweden the following background checks are conducted for persons in Trusted Roles:

- 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

In Finland, the background checks include:

- Confirmation of previous employment
- Check of professional reference
- Security clearance from the Finnish Police

Background checks are repeated periodically for personnel holding Trusted Positions, if permitted by the local laws. The factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted Positions or for acting against an existing Trusted Person generally include the following:

- Misrepresentations made by the candidate or Trusted Person
- Highly unfavourable or unreliable personal references
- Certain criminal convictions

- Indications of a lack of financial responsibility

Reports containing such information are evaluated by human resources and security personnel, who determine the appropriate course of action in light of the type, magnitude, and frequency of the behaviour uncovered by the background check. Such actions may include measures up to and including the cancellation of offers of employment made to candidates for Trusted Positions or the termination of existing Trusted Persons.

The use of information revealed in a background check to take such actions is subject to the applicable federal, state, and local laws.

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 necessary.

Telia's training programs are tailored to the individual's responsibilities and include the following as relevant:

- Basic PKI concepts
- Job responsibilities
- Telia security and operational policies and procedures
- Use and operation of deployed hardware and software
- Incident and Compromise reporting and handling

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

In limited circumstances, independent contractors or consultants may be used to fill Trusted Positions. Any such contractor or consultant is held to the same functional and security criteria that apply to a Telia employees in a comparable position.

Independent contractors and consultants who have not completed the background check procedures specified in section 5.3.2 are permitted access to Telia's secure facilities only to the extent that they are escorted and directly supervised by Trusted Persons.

5.3.8 Documentation supplied to personnel

Telia personnel involved in the operation of Telia CA Services will be made aware of the requirements of applicable Certificate Policies, Certification Practice Statements and any other specific policies, procedures, documents, and/or contracts needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit logging procedures

5.4.1 Types of events recorded

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

a. CA and system keys life cycle management events, including:
- Key generation, backup, storage, recovery, archival, and destruction
- Cryptographic device lifecycle management events

b. CA, RA, Subscriber and system certificate life cycle management events, including:
- Certificate requests, renewal, and re-key requests, and revocation
- All verification activities stipulated in these Requirements and the CA's Certification Practice Statement
- Date, time, phone number used, persons spoken to, and end results of verification telephone calls
- Acceptance and rejection of certificate requests;
- Issuance of Certificates
- Generation of Certificate Revocation Lists and OCSP entries

c. Security-related events including:
- Successful and unsuccessful PKI system access attempts
- PKI and security system actions performed
- Security profile changes
- System crashes, hardware failures, and other anomalies
- Firewall and router activities
- Entries to and exits from the CA facility

Log entries include at least the following elements:
- Date and time of the entry
- Identity of the entity making the journal entry
- Kind of entry

Telia RAs log Certificate Application information including:
- Kind of identification document(s) presented by the Certificate Applicant
- Storage location of copies of applications and identification documents
- Identity of entity accepting the application
- Method used to validate organisation and individual identity and authority

The following information concerning revocation requests is recorded at the Telia's Revocation Service:
- Information concerning the person requesting revocation
- Method of verifying the identity of the person requesting revocation
- Revocation request reception time
- Information concerning the certificate to be revoked

In the case where the CA is a Customer's CA or the registration or revocation functions are performed by Registration Officer in a Customer, the information above may not be logged by the RAs.

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 years 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. 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 those 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 years, 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 time-stamping 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 UTC time source.

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 as long as 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, for example, 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, for example, 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 of time.

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, Customer 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

In the event that it is necessary for a Telia CA or a Customers 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. Where CA termination is required, Telia and, in the case of a Customer CA, the applicable Customer, will develop a termination plan to minimize disruption to Customers, Subscribers, and Relying Parties. Such termination plans may address the following, as applicable:

a. Provision of notice to parties affected by the termination, such as Subscribers, Relying Parties, and Customers, informing them of the status of the CA
b. In case that the CA is publicly used, make public announcement at least three months in advance that operations will cease for the CA
c. 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
d. Terminate all rights for subcontractors to act in the name of the CA which will cease to operate
e. Ensure that all archives and logs are stored for the stated storage time and in accordance with stated instructions

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

The CA's issuer keys are generated in FIPS 140-2 level 3 validated cryptographic hardware modules which are dedicated to storing and processing such keys. When generating issuer keys, a number of people's presence is required. The hardware modules are physically protected as per section 5.1 which, among other things, means that physical access to these requires the simultaneous presence of at least two authorised operators.

Some CA keys are stored in offline state (e.g. "TeliaSonera Root CA v1"). They are activated only when needed. Two privileged CA Officers are required to temporarily activate an offline key. The key ceremony of WebTrust audited CA keys is always witnessed by an independent party and/or videotaped for examination.

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 normally generates the key pair using browser software. 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 Customer 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 Customer 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 keys that are generated securely by the External RA will not be 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 Registration Officer can download the PKCS#12 file directly from the application or send the Subject a one-time password. The Subject can access the self-service software with the one-time password and generate a key pair and download 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 keys to the address specified in the card order, which is normally the address of the Registration Officer of the Customer 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 certification digitally through the use of a PKCS#10 Certificate Signing Request (CSR), Certificate Request Syntax (CRS) or other digitally signed package in a session secured by TLS. Where CA, RA, or end-user Subscriber key pairs are generated by Telia, this requirement is not applicable.

The public key is digitally signed and delivered through an encrypted connection, from the site where the key has been generated, to the CA system.

6.1.4 CA public key delivery to relying parties

Telia makes the CA certificates for Telia CAs and for Customer CAs, if the Customers so agrees, available to Subscribers and Relying Parties through the Telia CA Service repository https://cps.trust.telia.com/.

Certain Telia root CA certificates are delivered to Subscribers and Relying Parties through the web browser software.

Telia generally provides the full certificate chain (including the issuing CA and any CAs in the chain) to the end-user Subscriber upon Certificate issuance.

6.1.5 Key sizes

The CAs' issuer keys are generated as RSA keys with a minimum length 4096 bits.

The length of the Subscriber keys generated by the CA in connection with the RSA algorithm is at least 2048 bits.

For the customer certificates we are following the WebTrust requirements for usage of RSA or EC Keys by end-user.

6.1.6 Public key parameters generation and quality checking

All CA Signature keys will be generated using a random or pseudo-random process as described in ISO 9564-1 and ISO 11568-5 that are capable of satisfying the statistical tests of FIPS PUB 140-2, level 3. CA keys are protected by a secure cryptographic hardware module rated at least FIPS 140-2, Level 3.

Telia may check the quality of keys before accepting the certificate request.

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):

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.

6.2 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 Customers 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 rated to at least FIPS 140-2 Level 3. The cryptographic module is physically protected in a separate safe which is stored 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 in a cryptographic module in smart cards.

End entities 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. In some hardware cases keys in smart cards are generated outside the smart card but pre-installed by a smart card factory with vendor specific methods
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.

The Subscriber private keys may be stored in the software of a workstation or the private keys may be stored in a Smart Card or in a USB token.

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 individuals to perform sensitive CA cryptographic operations. Telia uses "Secret Sharing" to split the activation and 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 activate or 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 creates backup copies of CA's or RA's private keys for routine recovery and disaster recovery purposes. Backups are dealt with in accordance with the same access protection rules which apply to the original keys. At least two privileged CA Officers are required to manage CA private key backups.

Offline CA keys are stored as offline key backups. When an offline CA key is activated it is temporarily restored to the offline CA system.

Backups may be made of the subscribers' private confidentially keys if so agreed between Telia and the Customer. The keys are then copied and stored in encrypted form and protected at a level no lower than stipulated for the primary version of the keys.

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 disaster recovery purposes.

Telia CA does 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. Where CA key pairs are transferred to another hardware cryptographic module for clustering reasons such key pairs are transported between modules in encrypted form using private networks dedicated for Telia CA.

In addition, Telia CA makes encrypted copies of CA key pairs for routine recovery and disaster recovery purposes.

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.

For Subscriber private key storage see 6.2.6.

6.2.8 Method of activating private key

CA keys:

The activation of the private key of the CA is included in the procedure described in paragraph 6.1.1. At least one person serving in a trusted role of the CA and authenticated with a two-factor

authentication method is required for the re-activation. 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 encrypted. 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.

Telia strongly recommends that Subscribers and Registration Officers in Customers store their private keys in encrypted form and protect their private keys through 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 Customer Organisations use passwords for private key activation undersection 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 private key of the Subject requires the use of activation data as described in section 6.4.

6.2.9 Method of deactivating private key

CA keys:

The CA private issuer key is deactivated, for example, by closing the application using it, restarting or removing the cryptographic module.

Software keys:

Locking of the private key of the Subject depends on the software in use.

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. Reliable de-magnetizer or physical destruction is used when destroying the media

When the Subscriber's certificate of a Subject is expired and is not renewed, the private key related to it cannot be used anymore in connection with certification services. The key is not returned to the CA to be destroyed but it remains in possession of the Subscriber.

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 such personal certificates will never be stored in any device (e.g., USB token, smart card or hard disk) except the External RA servers' random-access memory that are highly secured.

6.2.11 Cryptographic module rating

All CA digital signature key generation, CA digital signature key storage and certificate signing operations are performed in a secure cryptographic hardware module rated to at least FIPS 140-2 Level 3.

See section 6.2.1 for a more detailed description.

6.3 Other aspects of key pair management

6.3.1 Public key archival

Telia CA retain archives of certificates according to the section 5.5 of this CPS.

6.3.2 Certificate operational periods and key pair usage periods

Private Root CA keys and certificates are used for a maximum of twenty-five (25) years in order to issue subordinate CA certificates.

Private subordinate CA keys and certificates are used for a maximum of twenty-five (25) years in order to issue Subscriber certificates and revocation lists. CA certificates are given a maximum validity period to cover the time from generation up to and including the point when associated private keys cease to be used for signing of Subscriber certificates and revocation lists. Cross certificate private keys are also given a maximum validity period of twenty-five (25) years.

Subscriber certificates issued in accordance with this CPS are issued both for new keys and for existing keys which have been certified previously in connection with the keys being generated on smart cards. The usage period of the Subject keys and certificates shall not be longer than five (5) years.

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

6.4 Activation data

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

Telia CA and RA operators are either using smart cards with the private keys protected by PINs or have the private keys stored on a hard disk. If the keys are stored on a hard disk the CA and RA operators are required to select strong passwords to protect the private keys.

Telia strongly recommends that Subscribers and Registration Officers in Customers choose passwords that meet the same requirements. Telia also recommends the use of two factor authentication mechanisms (e.g., token and pass phrase or biometric and token) for private key activation.

The Subscriber uses his private keys with the help of activation data, which are given on the keyboard of a card reader, workstation, mobile phone or other device.

6.4.1 Activation data generation and installation

Software keys:

When the Subject or Registration Officer in the Customer Organisation generates the key pair, a password can be chosen as activation data according to Customer Organisation policy.

If the Registration Officer of the CA generates the key pair, the activation data will be generated using sufficient number of characters to be secure.

Smart Cards and USB tokens:

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

When it is possible for the Subscriber to change the activation data, the Subscriber is recommended to make sure that the new activation data consists of sufficiently many characters to be secure.

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.

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 and their browser's "high security" option. Telia CA and RA operators are required and Subscribers and Registration Officers in Customers are strongly recommended to protect the activation data for their private keys against loss, disclosure, modification, or unauthorised use.

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 is obtained by using:

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

When the RA office of the CA generates the key pair, the activation data and the private key are sent as separate deliveries through different channels to the Subscriber. The activation data can be delivered for example to a mobile phone as an SMS or it can be given over the phone.

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

The Subscriber shall instruct the Subject to keep his activation data safe enough. He/she should memorize the activation data. The activation data must not be disclosed to others.

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 as a result 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 similar to 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
The CA follows the policies defined by Telia's Corporate Security Unit in security management. Furthermore, the CA follows the Security Policy, CP, and CPS defied by it in all of its operations. The auditing of the operation has been described in paragraph 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

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 monitored and alerted by the IDS.

6.8 Time-stamping

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-2.

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.
Signature algorithm	The signature algorithm is the set of mathematical rules according to which the CA software executes the signing of the certificate. Identifiers have been allocated for the algorithms that are generally used. The identifier of the algorithm used for the signing of the certificate is given in this field. The signature cannot be verified if the algorithm used is not known. The algorithm that is used for the signing of the certificates is sha1RSA or sha256RSA.
Issuer	This field states the name of the Issuer of the certificate. The Issuer name in the certificates of each CA has been described in section 1.3.1.
Validity	The validity of the certificate is that period of time during which the CA guarantees that it maintains status information of the certificate, in other words about the possible revocation of the certificate. This field states the date and time when the certificate comes into force, and the date and time after which the certificate is no more valid. The certificate can be trusted during its validity period if the certificate has not been published on the CRL.
Subject	This field identifies the 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.
Subject public key info	This field gives the algorithm under which the public key of the Subject shall be used. The Subject's public key itself is also given in this field. The algorithms and key lengths of the Subject keys are described in section 6.1.5.

7.1.1 Version number(s)

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

7.1.2 Certificate extensions

Certificate extensions will be supported in accordance with RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and 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. Within Telia PKI the key usage purposes of the public key of the CA are: - Certificate signing (KeyCertSign) - CRL signing (CRLSign)	Yes
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". "pathLenConstraint" field of the extension 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: a. The URL to CA-certificate b. OCSP service address as defined by RFC6960 Typically, all subordinate CA certificates include both listed values.	No

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	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

identifier		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. 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. E.g. the following key usage purposes may be given in a Certificate: ClientAuthentication, WindowsLogon, SMIME
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.
Smartcard serial number	Subscriber	<u>Certificate stored on a Smart Card:</u> 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.

		Certificate stored in a USB token: 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

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

Telia certificates are signed using one of the following algorithms:

1. sha1withRSAEncryption OBJECT IDENTIFIER ::== {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha1-with-rsa-signature(5)}
2. sha256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1)member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
3. ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2 }
4. ecdsa-with-SHA384 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }

Telia CA only uses NIST “Suite B” curves for EDCSA.

7.1.4 Name forms

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

7.1.5 Name constraints

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

7.1.6 Certificate policy object identifier

The 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 that are compliant with RFC 5280.

7.2.1 Version number(s)

All issued CRL’s are X.509 version 2 CRL’s in accordance with the RFC 5280 “Internet X.509

Public Key Infrastructure Certificate and 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 CRL Profile.

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

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

7.3 OCSP profile

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

7.3.1 Version number(s)

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

8.1 Frequency or circumstances of assessment

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

8.2 Identity/qualifications of assessor

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

8.3 Assessor's relationship to assessed entity

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

8.4 Topics covered by assessment

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

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

The scope of the compliance audit includes CAs in scope of this CPS.

8.5 Actions taken as a result of deficiency

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

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

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

8.6 Communication of results

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

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Fees are defined in applicable Customer agreement.

9.2 Financial responsibility

9.2.1 Insurance coverage

Telia and all CAs residing in the Telia production environment will maintain adequate levels of insurance necessary to support its business practices.

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

9.3.1 Scope of confidential information

Information which is not excluded in section 9.3.2 is treated as confidential by the CA in relation to the Customer and/or keyholder and will not be disclosed without the consent of the Customer and/or key holder.

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 the Customer and/or keyholder:

a. Information in issued certificates including public keys (but not private keys)
b. Revocation lists and OCSP responses
c. General key holder terms and conditions

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 processes personal data in accordance with the European General Data Protection Regulation

EU (GDPR) and applicable national legislations and any agreement with Customer and/or keyholder.

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 entirety provided that this is at no charge and that no information in the document is added to, removed or changed.

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

9.6 Representations and warranties

9.6.1 CA representations and warranties

Telia will operate in accordance with this CPS, when issuing and managing certificates provided to CAs, RAs, sub-CAs and Subscribers. Telia will require that all the RAs operating on its behalf will comply with the relevant provisions of this CPS concerning the operations of the RAs. Telia will take commercially reasonable measures to make Subscribers and Relying Parties aware of their respective rights and obligations with respect to the operation and management of any keys, certificates or End-Entity hardware and software used in connection with the PKI. Subscribers will be notified as to procedures for dealing with suspected key compromise and service cancellation.

When a CA publishes or delivers a certificate, it declares that it has issued a certificate to a Subscriber and that the information stated in the certificate was verified in accordance with the applicable CPS.

CA personnel associated with PKI roles will be individually accountable for actions they perform. "Individually accountable" means that there shall be evidence that attributes an action to the person performing the action.

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

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. A Customer can, through an agreement, take responsibility for a separately defined part of the CA’s responsibilities related to registration.

Telia will require that all Registration Officers comply with all the relevant provisions of this CPS. Telia will make available registration policies and Customer responsibility descriptions to Customers acting as RA and will require them to comply with the registration policies and Customer responsibility descriptions through a certification service agreement. The registration policies and Customer responsibility descriptions contain all relevant information pertaining the rights and obligations of the Registration Officers, Subscribers and Relying Parties.

The Registration Officer is responsible for the identification and authentication of Subscribers following section 3.1 and section 4.1. 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 particular 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 applicable 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.

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.

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 the issuing Certification Authority in the manner specified in applicable CPS. When any other entity suspects private key compromise, they should notify the issuing CA.

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

No stipulation.

9.7 Disclaimers of warranties

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

9.8 Limitations of liability

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

9.9 Indemnities

If a claim for damages will be presented against the CA based on the matters listed below, the Customer shall be bound to compensate the CA for any damages and costs due to the claim and the necessary statement of defence, including any legal expenses. The Customer shall compensate the CA for any damage caused by:

a. the Subject's failure to protect his private key or prevent it from being lost, disclosed or compromised
b. the failure to submit a certificate revocation request to the Revocation Service under the conditions that require notification to the CA, as stated in section 9.6.3
c. the Customer's failure as a Relying Party to verify the validity of the certificate according to section 9.6.4
d. the Customer's otherwise non-justified trust on the certificate as Relying Party, in consideration of the circumstances

The CA shall notify the Customer of any such claim in writing within a reasonable time after being informed of a claim.

9.10 Term and termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of termination and survival

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

9.11 Individual notices and communications with participants

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

9.12 Amendments

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.

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 (https://cps.trust.telia.com). Changes affecting the terms of an agreement shall be notified in writing to the address given in the contact information of the signatory of the agreement.

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

See 9.12.1

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

If a dispute relating to this CPS is not successfully resolved by negotiations, it shall be settled by arbitration in accordance with the Reconciliation and Arbitration Rules of the International Chamber of Commerce (ICC). The Stockholm or Helsinki Chamber of Commerce shall administer the reconciliation in accordance with the ICC's rules, and the venue for arbitration shall be Stockholm or Helsinki. The proceedings shall be held in Swedish or Finnish unless the parties

agree to hold them in English.

9.14 Governing law

Swedish or Finnish law shall apply to the interpretation of this CPS depending where the related Customer agreement has been made, if not otherwise agreed.

9.15 Compliance with applicable law

Telia will, in relation to the CA Service, comply with applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees and orders including but not limited to restrictions on exporting or importing software, hardware or technical information.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

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

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

No stipulation.

ACRONYMS

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DER	Distinguished Encoding Rules
DN	Distinguished Name
DSA	Digital Signature Algorithm
DV	Domain Validation
EAL	Evaluation Assurance Level
EID	Electronic Identification
EV	Extended Validation
FIPS	Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest 5
OCSP	On-line Certificate Status Protocol
OID	Object Identifier
PMT	Policy Management Team
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509 (IETF Working Group)
RA	Registration Authority
RFC	Request for Comments
RSA	Rivest-Shamir-Adleman asymmetric encryption algorithm
SEIS	Secure Electronic Information in Society

SHA –1	Secure Hash Algorithm
S/MIME	Secure Multipurpose Internet Mail Extension
SSL	Secure Sockets Layer
TTP	Trusted Third Party
UPS	Uninterruptible Power Supply
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

DEFINITIONS

Access control: The granting or denial of use or entry.

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

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

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

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

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

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

Authorisation: The granting of permissions of use.

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

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

Base certificate: See primary certificate.

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

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

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

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

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

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

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

Certification Authority (CA): An authority trusted by one or more users to manage X.509 certificates and CRLs.

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

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

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

Certificate Revocation List (CRL): A periodically issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation. CRL can be used to check the status of certificates.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

FIPS 140-2: Federal Information Processing Standard 140-2(FIPS 140-2) is a standard that describes US Federal government requirements that IT products shall meet for Sensitive, but Unclassified (SBU) use. The standard was published by the National Institute of Standards and Technology (NIST), has been adopted by the Canadian government's Communication Security Establishment (CSE), and is likely to be adopted by the financial community through the American National Standards Institute (ANSI). The different levels (1 to 4) within the standard provide different levels of security and in the higher levels, have different documentation requirements.

FIPS 180-1: Standard specifying a Secure Hash Algorithm, SHA-1, for computing a condensed representation of a message or a data file.

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

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

ISO 11568-5: Basic principles and requirements for Key lifecycle for public key cryptosystems, provides instructions to financial institutions in the development, implementation and/or the operation of systems and procedures throughout Key's lifecycle

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

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

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

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

MD5: A Message Digest Algorithm.

Non-repudiation: Protection against the denial of the transaction or service or activity occurrence.

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

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

Operator: Employee of a CA.

Out of band process: Communications which occur outside of a previously established communication method or channel.

PKCS #1: Standard that provides recommendations for the implementation of public-key cryptography based on the RSA algorithm, covering the following aspects: cryptographic primitives; encryption schemes; signature schemes, etc.

PKCS #7: A cryptographic message format or syntax managed and edited by RSA Laboratories. A standard describing general syntax for data that may have cryptography applied to it, such as digital signatures and digital envelopes.

PKCS #10: A certificate request format or syntax managed and edited by RSA Laboratories. It is a standard describing syntax for a request for certification of a public key, a name, and possibly a set of attributes.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Storage module: In this document relates to cryptographic module.

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

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

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

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

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

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

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

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

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

URI: Universal Resource Indicator - an address on the Internet.

UTF8String: UTF-8 is a type of Unicode, which is a character set supported across many commonly used software applications and operating systems. UTF-8 is a multi-byte encoding in which each character can be encoded in as little as one byte and as many as four bytes. Most Western European languages require less than two bytes per character. Greek, Arabic, Hebrew, and Russian require an average of 1.7 bytes. Japanese, Korean, and Chinese typically require three bytes per character. Such Unicode is important to ensure that universal /foreign characters are supported.

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

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

Vulnerability: Weaknesses in a safeguard or the absence of a safeguard.

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

X.500: Specification of the directory service required to support X.400 e-mail initially but commonly used by other applications as well.

X501 PrintableString: String format for representing names, such as Common Name (CN), in X.509 certificates. The encoding of a value in this syntax is the string value itself; an arbitrary string of printable characters.

X.509: ITU standard that describes the basic format for digital certificates.