Certificate Policy and Certification Practice Statement for Telia Server Certificates

Prepared by the Telia's Certification Authority Policy Management Team

Release: 4.0

Valid From: 2021-05-14

Classification: Public

CONTENTS

Revision History

Version	Date	Change	Author
1.0	2012-06-11	The first official version	TeliaSonera CA Policy Management Team
1.01	2012-09-11	Fixed minor errors in references	TeliaSonera CA Policy Management Team
1.02	2012-12-21	Added OCSP support, In validation a call back to technical contact person is an option, Fixed AIA extension description, Mandatory 2048 bit RSA key length	TeliaSonera CA Policy Management Team
1.1	2013-04-03	Geographical definition to Server Certificates, Suspension no more used, small technical fixes	TeliaSonera CA Policy Management Team
1.2	2014-05-03	All Subject fields except O and OU will refer to registered O location. Small fixes and clarifications.	TeliaSonera CA Policy Management Team
1.3	2015-05-16	Extended Validation (EV) certificate processes were included, TeliaSonera Server CA v2 added, CA must understand all extensions in 3.2.4, validity max limited to 3y, OCSP specification rewritten, small clarifications in many places, fixed contact details	TeliaSonera CA Policy Management Team
1.4	2015-11-16	Clarifications mainly to EV processes, Revocation link added, CAA record handling	TeliaSonera CA Policy Management Team
1.5	2016-01-04	Clarifications mainly to EV processes based on EV pre-audit,	TeliaSonera CA Policy Management Team
1.6	2016-12-01	New company name “Telia”, New BR based OID values. LDAP references removed from CDP, new verification documentation, New ST value handling. Other improvements to CPS documentation.	Telia CA Policy Management Team
1.7	2017-03-23	Telia Company -> Telia	Telia CA Policy Management Team
1.8	2017-06-30	New domain validation methods, validity of verified data to 27 months when reusing it.	Telia CA Policy Management Team
1.9	2017-09-30	CAA support (starting 8th September 2017), OCSP fully supports rfc6960, small clarifications, several new server names	Telia CA Policy Management Team
2.0	2017-11-30	DV added	Telia CA Policy Management Team
2.1	2018-09-04	Certificate Transparency included, max 2y validity for TLS, Enterprise signing certificate aka Telia Seal certificate, clearer audit requirements, small fixes in multiple chapters	Telia CA Policy Management Team

2.2	2018-08-30	New v2 issuers for DV and Document signing, E values are discarded from CSR, domain validation methods 3.2.2.4.1 and 3.2.2.4.5 are no more used, modified CAA chapter, improvements in domain validation chapter	Telia CA Policy Management Team
2.3	2018-11-15	New test certificate description, IP validation description, Telia Document Signing CA v1 removed (never used), Seal certificate process near to EV process, clarified certificate problem reporting description, old verification data valid max 825 days and not 27 months, OU validation description, list of supported Subject attributes, improved description of Seal certificates which provide Adobe trust, new technical support phone number	Telia CA Policy Management Team
2.4	2019-03-15	New BR compatible contact channel in chapter 1.5.1	Telia CA Policy Management Team
2.5	2019-04-15	BR 1.6.4 compatible domain validation. BR 1.6.5 compatible Subject value. Adobe AATL compatibility in 6.2.4.	Telia CA Policy Management Team
2.6	2019-12-30	Seal certificate changes: a) EKU (7.1.2), b) Private key delivery (6.1.2, 6.2.6, 6.4.1), c) f2f in validation of authority (3.2.5); -v3 issuers added (1.2, 1.3, 2.1.2) -Updated audit scope (8.4); -Typographic corrections;	Telia CA Policy Management Team
2.7	2020-03-30	No stipulation replaced by a comment; Test certificate OID removed; Sections exactly like in RFC3647; More detailed re-key and modification chapters; support for ECC P521 removed; request tokens not used in domain validation; IP and wildcard validation added.	Telia CA Policy Management Team
2.8	2020-10-30	BR 1.6.8 compatible new file validation method v2, 1.3.1 Certification authorities, 1.3.2 Registration authorities, 2.3 Time or frequency of publication, 3.1.1 Types of names, 3.2.2 Authentication of organisation identity and/or domain name, 4.9 Certificate revocation and suspension, 4.9.1 Circumstances for revocation, 4.9.3 Procedure for revocation request, 4.10.1 Operational characteristics, 6.1.1 Key pair generation, 6.3.2 Certificate operational periods and key pair usage periods, 7.1 Certificate profile, 7.1.2 Certificate extensions, 7.1.3 Algorithm object identifiers, 7.1.5 Name constraints, 7.2 CRL profile, 7.3 OCSP profile	Telia CA Policy Management Team
2.9	2020-11-23	Added 3.2.2.6 Wildcard Domain Validation, 3.2.2.7 Data Source Accuracy, revision on contact info and some minor language changes	Telia CA Policy Management Team

3.0	2021-02-01	Merged with Telia root and production CPS, added clarification about the OU	Telia CA Policy Management Team
4.0	2021-05-14	ETSI compliance, removed the EV related information, revocation process, reformatting, alignment with new subscriber agreement and relying party agreement documents, removed Sonera Class 2, clarification on reporting key compromises	Telia CA Policy Management Team

1. INTRODUCTION

1.1 Overview

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

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

All certificates containing the Object Identifier (OID) value 2.23.140.1.2.2 are so called Organization Validation (OV) TLS certificates. All certificates containing the OID value 2.23.140.1.2.1 are so called Domain Validated (DV) certificates. Both OV and DV certificates conform to the current version of the Baseline Requirements (BR) aka “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates” published at http://www.cabforum.org. In the event of any inconsistency between this CPS and those documents, those documents take precedence over this CPS.

Telia TLS DV and OV certificates provide a mean for relaying parties to evaluate trust when relying on such certificates. In case of OV certificates Telia CA has verified the name and some other details of the entity that controls the website from official registers.

Telia Certificates do not, however, provide any guarantee that the Subject named in the Certificate is trustworthy, honest or reputable in its business dealings, or safe to do business with. Issued certificates only establish that Telia CA verified that the business was legally organised, used domain names were owned or managed by the Subject.

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

All certificates containing the OID value 1.3.6.1.4.1.271.2.3.1.1.20 are so called Telia Enterprise Signing certificates aka Seal certificates and conform to the current version of the Adobe Approved Trust List Technical Requirements (AATL). Such certificates provide a mean for relaying parties to see Portable Document Format (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.

In summary following certificate types ("Services") are offered by Telia:

a. **Telia DV certificate:** to authenticate servers and establishing secure TLS sessions with end clients. In this type the domain name the server domain name is validated by Telia,
b. **Telia OV certificate:** to authenticate servers and establishing secure TLS sessions with end clients. In this type domain name of the server, existence of the organisation and other attributes including name, type, status, and physical address is validated by Telia,
c. **Telia client certificate**: for identifying individual users, securing email communications and document signing, or
d. **Telia document signing certificate:** for authenticating documents from Adobe PDF, Microsoft Office, OpenOffice, and LibreOffice.

Note! Telia Seal certificates are client certificates but are included in this document because they are issued and maintained under the WebTrust/BR requirements.

1.2 Document name and identification

This CP/CPS is identified by the following information:

- **Name**: Certificate Policy and Certification Practice Statement for Telia Server Certificates
- **Release**: 4.0
- **OID**: 1.3.6.1.4.1.271.2.3.1.2.1
- **Location**: http://cps.trust.telia.com/

This CPS is also a CP for Telia OV, DV and Seal certificates. The certificates issued according to this CPS contain 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 OIDs**
OV certificates	TeliaSonera Server CA v2 Telia Server CA v3	2.23.140.1.2.2 (from 2016-12-01)

DV certificates	Telia Domain Validation CA v2 Telia Domain Validation CA v3	2.23.140.1.2.1
Telia Enterprise Seal certificates	Telia Document Signing CA v3	1.3.6.1.4.1.271.2.3.1.1.20

1.3 PKI participants

Telia Root CA will issue subordinate CA server certificates to Telia.

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

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, 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 subject simultaneously. Clients can use either one when doing PKI path validation.

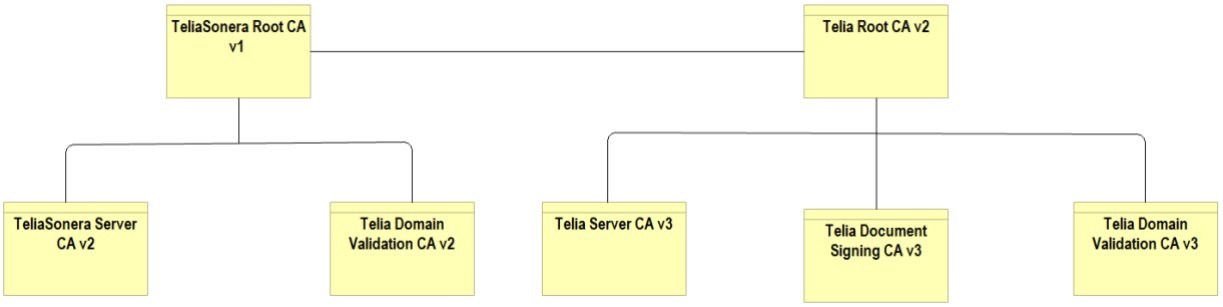

Figure 1, Telia Server Certificate PKI Hierarchy

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

- **TeliaSonera Root CA v1**
  SHA2 Fingerprint: DD6936FE21F8F077C123A1A521C12224F72255B73E03A7260693E8A24B0FA389
- **Telia Root CA v2**
  SHA2 Fingerprint: 242B69742FCB1E5B2ABF98898B94572187544E5B4D9911786573621F6A74B82C

Cross-signed Root CAs

- **Telia Root CA v2**

SHA2 Fingerprint: EF6F29F636F62BDD4753122F41F3419EE7C2877587BE4A9807ADF58946458E7F

Intermediate CA's

- **TeliaSonera Server CA v2**
  SHA2 Fingerprint:
  D721110388CA6F20BBA9FD1A8DBA4EFB8C16392A3DEBAD97C553EEAF0ACACAAC
- **Telia Domain Validation CA v2**
  SHA2 Fingerprint:
  5B312B7E11B70D07C14E0AB99F08D00748966098C52AA85A06A0822BBE59A02C
- **Telia Domain Validation CA v3**
  SHA2 Fingerprint:
  A7E83056E9B3D9DDB1816B95518F6A5E5A1DFDFA28F60533B1C850855EAA4263
- **Telia Server CA v3**
  SHA2 Fingerprint:
  1281AD8FABE883F209E9636448D1A80C373DAA7686C813A270FAD48F5F5E589A
- **Telia Document Signing CA v3**
  SHA2 Fingerprint:
  6924A4DD82948DA53F6FB933E895A0F6581C8DBDEBABB36FC11CAC25E9C0335A

Externally Operated Subordinate CAs

- **None**

1.3.2 Registration authorities

The CA's units are authorised to perform registration functions. Through those agreements, RAs are obliged to follow this CPS for their part.

The RA responsibilities for the following activities on behalf of a CA include:

- Identification and authentication of certificate subjects
- Initiating or passing along revocation requests for certificates
- Approving applications for renewal or re-keying certificates

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

1.3.3 Subscribers

Subscribers are legal entities to whom Certificates are issued according to this CPS and are in possession of the private keys corresponding to their certificates. For DV and OV TLS certificates and Seal certificates, the Subscriber may only be a legal entity (e.g. an organisation).

1.3.4 Relying parties

A Relying Party may be either a Subscriber of any Telia CA or any other organisation, person, application or device that is relying on a valid certificate issued by any of the CAs in this CPS that are chained to the Telia Root CA.

1.3.5 Other participants

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

1.4 Certificate usage

1.4.1 Appropriate certificate uses

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

- Root certificates: used to create subCAs

- TLS Server certificates: used to implement the TLS protocol on one or more servers
- Seal certificates to sign PDF documents

Telia server certificates can be used, for example, to identify servers and secure TLS sessions.

Telia Seal certificates are used to sign documents on behalf of an organisation.

CA name	Policy	Class	OID
TeliaSonera Root CA v1 Telia Root CA v2	Root CA	Root	1.3.6.1.4.1.271.2.3.1.1.2
TeliaSonera Server CA v2 Telia Server CA v3	TLS Server OV (Organisation Validated)	OV	2.23.140.1.2.2
Telia Domain Validation CA v2 Telia Domain Validation CA v3	TLS Server DV (Domain Validated)	DV	2.23.140.1.2.1
Telia Document Signing CA v3	Document Signing (Organisation Validated)	Adobe	1.3.6.1.4.1.271.2.3.1.1.20

1.4.2 Prohibited certificate uses

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

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

1.5 Policy administration

1.5.1 Organisation administering the document

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

Contact information:

Telia Finland Oyj (1475607-9)
FI-00510 Helsinki, Finland
Phone: +358 (0) 20401
Internet: https://cps.trust.telia.com/CPS

1.5.2 Contact person

Contact point in matters related to this CPS:

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

Other contact information:

Customer Service: +358 20 693 693 (normal office hour Help Desk services)
CA Customer Service: cainfo@telia.fi (PKI support issues)
Revocation Service Phone: +358 (0) 800156677 (revocation requests or any urgent issues)
Revocation Service Web: https://support.trust.telia.com/certificate_revocation_request_en.html

Certificate problem reporting:

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

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

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

1.5.3 Person determining CPS suitability for the policy

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

1.6.1 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.

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: An online database containing publicly-disclosed Telia PKI governance documents, and certificate status information, either in the form of a CRL or an OCSP response. Currently at this link: https://cps.trust.telia.com.

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

1.6.2 Acronyms

BR	Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DER	Distinguished Encoding Rules
DN	Distinguished Name

DSA	Digital Signature Algorithm
DV	Domain Validation
EAL	Evaluation Assurance Level
EID	Electronic Identification
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

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

2.1.1 CPS Repository

A full text version of this CPS is published at the Repository.

2.1.2 Revocation Information Repository

Following CRLs are published on the Telia's website:

Issuing CA	**CRL addresses**
TeliaSonera Root CA v1	http://httpcrl.trust.telia.com/teliasonerarootcav1.crl
Telia Root CA v2	http://httpcrl.trust.telia.com/teliarootcav2.crl
TeliaSonera Server CA v2	http://httpcrl.trust.telia.com/teliasoneraservercav2.crl
Telia Server CA v3	http://httpcrl.trust.telia.com/teliaservercav3.crl
Telia Domain Validation CA v2	http://httpcrl.trust.telia.com/teliadomainvalidationcav2.crl
Telia Domain Validation CA v3	http://httpcrl.trust.telia.com/teliadomainvalidationcav3.crl
Telia Document Signing CA v3	http://httpcrl.trust.telia.com/teliadocumentsigningcav3.crl

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

2.1.3 Certificate Repository

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

2.2 Publication of certification information

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

a. This CPS
b. CRLs and revocation status of revoked certificates
c. Issued CA certificates and cross certificates for cross-certified CAs

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

Each published 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 Subscriber.

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

3.1.1 Types of names

An X.501 Distinguished Name (DN) together with Subject Alternative Name values are used as an unambiguous name of the Subscriber. The naming will conclude of the following attributes as outlined in the followings.

3.1.1.1 Root CA

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

3.1.1.2 Subordinate CAs

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 Finland Oyj or TeliaSonera
Country (C, OID 2.5.4.6)	Qualifier for describing the country where the CA organisation is incorporated.

3.1.1.3 Subscriber Certificates

Attribute	**Description – OV TLS**	**Description – DV TLS**	**Description – Seal**
commonName (CN, OID 2.5.4.3)	A single host domain name (FQDN) or IP address which is owned or controlled by the Subject and to be associated with the Subject's server. Such server MAY be owned and operated by the Subject or another entity (e.g., a hosting service). The CN value is always one of the values contained in the Certificate's subjectAltName	A single host domain name (FQDN) which is owned or controlled by the Subject and to be associated with the Subject's server. Such server MAY be owned and operated by the Subject or another entity (e.g., a hosting service). The CN value is always one of the values contained in the Certificate's subjectAltName extension.	A name of the service or server (FQDN) which is owned or controlled by the Subject §

	extension.		
OrganizationName (O, OID 2.5.4.10)	Subscriber in relation to which the Subject is identified. Common variations or abbreviations may also be used provided that the name owner is unambiguous.	Not allowed.	Subscriber in relation to which the Subject is identified. Common variations or abbreviations may also be used provided that the named owner is unambiguous.
Locality (L, OID: 2.5.4.7)	City name. A component of the address of the physical location of the Subject's Place of Business.	Not allowed.	City name. A component of the address of the physical location of the Subject's Place of Business.
Country (C, OID: 2.5.4.6)	Two character country code. A component of the address of the physical location of the Subject's Place of Business.	Not allowed.	Two character country code. A component of the address of the physical location of the Subject's Place of Business.
subjectAltName: dNSName	One or more host domain names (FQDN) which are owned or controlled by the Subject and to be associated with the Subject's server. Such server MAY be owned and operated by the Subject or another entity (e.g., a hosting service). Wildcard names are allowed.	One or more host domain names (FQDN) which are owned or controlled by the Subject and to be associated with the Subject's server. Such server MAY be owned and operated by the Subject or another entity (e.g., a hosting service). Wildcard names are allowed.	The same value that was used in CN. Often useless in Seal certificates.
subjectAltName: iPAddress	One or more IP addresses which are owned or controlled by the Subject and to be associated with the Subject's server. Such server MAY be owned and operated by the Subject or another entity (e.g., a hosting service).	One or more IP addresses which are owned or controlled by the Subject and to be associated with the Subject's server. Such server MAY be owned and operated by the Subject or another entity (e.g., a hosting service).	Not applicable
jurisdictionCountry Name (OID: 1.3.6.1.4.1.311. 60.2.1.3)	Optional in normal OV certificates.	Not allowed.	Optional.
businessCategory (OID: 2.5.4.15)	Optional in normal OV certificates.	Not allowed.	Optional.
serialNumber (OID: 2.5.4.5)	Optional in normal OV certificates.	Not allowed.	Optional.

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

Attribute	**Description – OV TLS, Seal**
organizationalUnitName (OU,OID:2.5.4.11)	OU will not be included.

streetAddress (OID: 2.5.4.9)	Optional. Street address. A component of the address of the physical location of the Subject's Place of Business.
postalCode (OID: 2.5.4.17)	Optional. Postal code. A component of the address of the physical location of the Subject's Place of Business.

Additional Distinguished Name (DN) or Subject Alternative Name attributes may be used as necessary providing that CA is able to verify that the additional attributes belong to the Subject. None of the Subject attributes contains only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

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

3.1.2 Need for names to be meaningful

Names will be meaningful as stated in the section 3.1.1.

3.1.3 Anonymity or pseudonymity of Subscribers

Names will be meaningful as stated in the section 3.1.1.

3.1.4 Rules for interpreting various name forms

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

3.1.5 Uniqueness of names

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

3.1.6 Recognition, authentication, and role of trademarks

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

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

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

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

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

3.2.2 Authentication of organisation identity and/or domain name

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

In case of Seal, OV, Telia CA verifies the organisation name (O) of a new Subscriber by checking the existence of the company, its legal name, business identity code and other relevant organisation information from an official business register maintained by an applicable

government agency (e.g. “ytj.fi” in Finland). The list of applicable trusted registries is maintained in CA internal instructions. Subject’s registration number and address components (street, postalcode, locality, country) are typically verified using the same register. All attributes must have a successfully verified value. Certificates whose subjectAlternativeName extension or Subject commonName field contains a Reserved IP Address or Internal Name are not allowed, and there are internal checks to avoid issuing such certificates.

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

Telia verifies domain name and IP address ownership or control by using these methods listed in the BR

3.2.2.4.1 Validating the Applicant as a Domain Contact

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

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

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

3.2.2.4.3 Phone Contact with Domain Contact

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

3.2.2.4.4 Constructed Email to Domain Contact

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

3.2.2.4.5 Domain Authorization Document

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

3.2.2.4.6 Agreed-Upon Change to Website

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

3.2.2.4.7 DNS change

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

3.2.2.4.8 IP Address

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

Agreed-Upon Change to Website or 3.2.2.5.5. Phone Contact with IP Address Contact may be used.

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

3.2.2.4.15 Phone Contact with Domain Contact

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

3.2.2.4.18 Agreed-Upon Change to Website v2

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

3.2.2.4.19 Agreed-Upon Change to Website - ACME

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

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

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

These listed BR methods are not used:

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

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

Alternatively the Registration Officer may use another allowed authentication or verification methods listed in the BR (regarding OV and DV certificates) published at http://www.cabforum.org. If such special verification method is used, it is always separately approved by a supervising Telia PKI board.

3.2.2.5 Authentication for an IP Address

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

- 3.2.2.5.1 Having the Applicant demonstrate practical control over the IP Address by confirming the presence of Random Value contained in the content of a file or webpage in the form of a meta tag under the "/.well-known/pki-validation" directory on the IP Address, performed in accordance with BR Section 3.2.2.5.1;
- 3.2.2.5.2 Confirming the Applicant's control over the IP Address by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value, performed in accordance with BR Section 3.2.2.5.2;
- 3.2.2.5.3 Performing a reverse-IP address lookup and then verifying control over the resulting Domain Name, as set forth above and in accordance with BR Section 3.2.2.5.3;
- 3.2.2.5.4 Telia will not perform IP Address validations using the any-other-method method of BR Section 3.2.2.5.4;
- 3.2.2.5.5 Confirming the Applicant's control over the IP Address by calling the IP Address Contact's phone number, as identified by the IP Address RA, and obtaining a response confirming the Applicant's request for validation of the IP Address, performed in accordance with BR Section 3.2.2.5.5

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

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

3.2.2.6 Wildcard domain validation

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

3.2.2.7 Data Source Accuracy

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

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

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

3.2.3 Authentication of individual identity

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

3.2.4 Non-verified Subscriber information

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

3.2.5 Validation of authority

OV order via public web form or via using self-service software	Telia CA verifies that the administrative contact person defined in the certificate application is employed by the Subscriber. This is verified by calling the contact person via the Subscriber PBX number or by making a phone call to other verified number(s) in the organisation, which is looked up from a directory maintained by a trusted party. Authorization of the administrative and technical contact persons may also be based on attorney letter or FullTLS agreement from the actual Subscriber. In that case CA will verify the origin of the authorization document by verification phone call. CA will always verify that the Subscriber's administrative contact person approves the subscriber agreement at least once including information about Subscriber responsibilities, Company details, authorised Certificate Approvers and all relevant subject or domain values allowed in the TLS certificates. In online service the agreement details are available to him/her online in the CA web pages so that the agreement can be modified at any time. In non-authenticated TLS web order all order details are verified each time by CA. In online mode the authenticated administrative contact person may be authorised by CA to approve further additions to the TLS contract (e.g. who can be Certificate Requester or Certificate Approver in the Company or if new domains are requested from CA). All authenticated and authorised contact persons are allowed to make TLS certificates but only in the limits of the pre-verified values and individual role. Data expiration time limits specified by CA/Browser Forum are utilized in all pre-verified values. Authentication is based on secure combination of client certificates, SMS-OTP and weblinks with unique hash values. In internal Telia requests the authorization may be based on Employee register and authentication may be based on Telia email accounts. CA verifies that both technical and administrative contact persons are using approved Applicant company email addresses/domains and both persons are active employees of Telia Group according to the employee register and at least one representative is employee of Telia group and not an external worker.
DV order via public web form or via using self-service software.	Telia verifies host domain name/IP address ownership or control of those by using methods listed inthe BR.

Seal order via web form	Telia verifies that the administrative contact person defined in the certificate application is employed by the Subscriber by calling the contact person via the Subscriber's PBX number or by making a call to some other verified number in the organisation, which is looked up from a directory maintained by a trusted party. Authorization of the administrative and technical contact persons may also be based on attorney letter or Full TLS agreement from the actual Subscriber. In that case CA will verify the origin of the authorization document by verification phone call. In addition Applicant representative identity is verified using a strong identity proofing, based on a face-to-face meeting with the representative of the Applicant, or on a procedure that provides an equivalent assurance (e.g. by means of a secure video communication or using nationally accepted authentication (e.g. Telia Tunnistus identification) where face-to-face authentication has been a prerequisite or using trusted partner to do the same on behalf of Telia). CA will always verify that the Subscriber's administrative contact person approves the subscriber agreement at least once including information about Subscriber responsibilities, private key storage solution and Company details. In Seal certificate web order all order details are verified each time by CA.

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

3.2.6 Criteria for interoperation

Not applicable.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

No special routine exists for renewal of Telia Server certificates. In Subject registration the same process will be followed as in the initial registration. The previous verification data may be utilized by CA if it is not expired as specified in chapter 4.2.1.

3.3.2 Identification and authentication for re-key after revocation

After revocation of a Subject's certificate, if the Subscriber wants to have a new certificate, then the same process will be followed as in the initial registration. The previous verification data may be utilized by CA if it is not expired as specified in chapter 4.2.1.

3.4 Identification and authentication for revocation request

Revocation by Subscriber

In cases where a Subscriber can issue TLS certificates using Telia's self-service software, the Subscriber shall submit a request for certificate revocation to the Registration Officer of its own organisation, who has additionally the rights of a Revocation Officer. The Revocation Officer in the Subscriber Organisation is responsible for the verification of the authenticity of the request to revoke the certificate. The identity of the Revocation Officer in the Subscriber Organisation is verified based on a certificate or another strong authentication method.

Revocation by the Revocation Service of the CA

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

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

Revocation of CAs

The authorised CA personnel can request revocation of a CA certificate.

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

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.

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.

4.1.1.2 TLS Certificates

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

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

4.1.2 Enrolment process and responsibilities

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 TLS Certificates

Seal, DV or OV order via public web form	A certificate to a Device (an OV or DV server certificate) is applied by filling in a form that is publicly available at Telia's web site. A CSR that is a standard format certificate request generated by the Device shall be attached to the form. The completed application forms are directed to Telia's RA office where the sufficiency of the application is checked. Before the application can be submitted, the Subscriber has to accept the Subscriber responsibilities and terms and conditions of the service.

DV and OV order using Telia's self-service software	A Certificate Requester in a Subscriber Organisation applies for certificates to Devices (OV server certificates) directly from the CA system by using the self-service application provided by Telia. The application will print all relevant certificate request values on screen for final review. If accepted by the Certificate Requester and by the CA configuration the request is processed automatically. It may contain only pre-defined values like Domain Names and Organization Names (for OV) that have been pre-validated by CA to this Subscriber. If the order includes new values or order is originated from a new person the subscriber's administrative contact must approve the new values or persons to be added to Subscriber's TLS contract. Then CA will verify that the Subscriber is allowed to use the new values before the certificate is created and the new values get pre-approved status for further orders. Only Telia Registration Officers may add new allowed Domain Name or Organization Name values for Subscriber that act as the RA role. New values are always verified according to 3.2. The Subscriber is bound through an TLS Service Agreement with Telia. The Registration Officers also accept Subscriber Responsibilities when they logon to Telia's self-service application for the first time.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

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

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

4.2.2 Approval or rejection of certificate applications

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

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

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

4.2.3 Time to process certificate applications

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

4.2.4 Certificate Authority Authorization (CAA)

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

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

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

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

4.3.1.1 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.

4.3.1.2 TLS certificate issuance

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

4.3.2 Notification to Subscriber by the CA of issuance of certificate

CAs	Telia CA Policy Management Team (PMT)
Seal, DV or OV order via public web form	Subscriber is informed of the acceptance or rejection of the certificate request. Telia's RA office delivers a web link to the contact person for fetching of the certificate.
DV or OV order using Telia's self-service software	The certificate is available for the Subscriber's Registration Officer in the RA tool after the issuance.

4.4 Certificate acceptance

By accepting a certificate, the Subscriber:

I. Agrees with the continuing responsibilities, obligations and duties required by Telia CA,
II. Agrees to the Telia CA Subscriber Agreement and Terms of Use,
III. Represents and warrants that no unauthorized access to the private key associated with the certificate,
IV. Represents and warrants that the provided information during the registration process is truthful and accurate, and
V. Review and verify the certificate contents for accuracy, completeness and the certificate is not damaged or corrupted.

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

4.4.1 Conduct constituting certificate acceptance

The Subscriber is considered to have accepted the certificate when:

- The subscriber use of the certificate's key pair, or
- One calendar month is passed from the certificate issuance date.

4.4.2 Publication of the certificate by the CA

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

All OV and DV certificates will be distributed to external directories as required by Certificate Transparency specification at http://www.certificate-transparency.org/.

4.4.3 Notification of certificate issuance by the CA to other entities

All publicly trusted CA certificates are published to CCADB database at https://ccadb.force.com before their usage will start.

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

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The Subscriber shall only use certificates and their associated key pairs for the purposes identified in this CPS and in applicable agreements with Telia. Issued certificates contain information which defines suitable areas of application for the certificate and its associated keys. Area of application labelling takes place in accordance with X.509 and chapter 7 of this CPS. For more information regarding appropriate Subscriber key usage see sections 1.4.1 and 6.1.7.

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

4.5.2 Relying party public key and certificate usage

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

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

4.6 Certificate renewal

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

4.6.1 Circumstance for certificate renewal

Certificates can be renewed anytime if it is demanded by the Subscriber, e.g. to extend the validity of the certificate. The other reason to resign a certificate is to create new or updated extensions, subject attributes or other fields.

4.6.2 Who may request renewal

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

4.6.3 Processing certificate renewal requests

CAs	Certificate renewal requests are processed like the initial certificate requests as described in section 4.2. 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.
Seal, DV or OV order via public web form	Certificate renewal requests are processed like the initial certificate requests as described in section 4.2. CA may use the stored data of previous validations if available and such data is not expired as specified in chapter 3.2.2.
DV or OV order using Telia's self-service software	Subscriber Certificate Requester has an option to renew certificates using the tools provided by the CA which may use the old CSR file to renew the certificate. Subscriber Certificate Requester is responsible to ensure that the certificate information is still valid and that there are no other obstacles to the renewal. CA will verify the renewal request like it were a new request. Even if all values were approved previously some pre-approvals or algorithms may have been expired or authorization may have been changed so the renewal request may now fail.

4.6.4 Notification of new certificate issuance to Subscriber

The Subscriber is notified as described in section 4.3.2

4.6.5 Conduct constituting acceptance of a renewal certificate

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

4.6.6 Publication of the renewal certificate by the CA

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

4.6.7 Notification of certificate issuance by the CA to other entities

All publicly trusted CA certificates are published to CCADB database at https://ccadb.force.com before their usage will start.

DV and OV certificates are distributed to external directories as required by Certificate Transparency specification at http://www.certificate-transparency.org/.

4.7 Certificate re-key

Certificate re-key is the re-issuance of a certificate using new public and private keys but same subject and SAN values than before.

4.7.1 Circumstance for certificate re-key

When old certificate is about to expire the subscriber has to renew the certificate. The key pairs are generated by the Subscriber and the CA does not check if the certificate renewal request is made using the existing or a new key pair. However, Telia recommends that the Subscriber creates new key pair when renewing the certificate.

4.7.2 Who may request certification of a new public key

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

4.7.3 Processing certificate re-keying requests

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

4.7.4 Notification of new certificate issuance to subscriber

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

4.7.5 Conduct constituting acceptance of a re-keyed certificate

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

4.7.6 Publication of the re-keyed certificate by the CA

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

4.7.7 Notification of certificate issuance by the CA to other entities

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

4.8 Certificate modification

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

Certificate subject or extension modification is possible within certificate renewal process which is covered in section 4.6.1.

4.8.1 Circumstance for certificate modification

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

4.8.2 Who may request certificate modification

Certificate modification is not technically supported.

4.8.3 Processing certificate modification requests

Certificate modification is not technically supported.

4.8.4 Notification of new certificate issuance to subscriber

Certificate modification is not technically supported.

4.8.5 Conduct constituting acceptance of modified certificate

Certificate modification is not technically supported.

4.8.6 Publication of the modified certificate by the CA

Certificate modification is not technically supported.

4.8.7 Notification of certificate issuance by the CA to other entities

Certificate modification is not technically supported.

4.9 Certificate revocation and suspension

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

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

4.9.1 Circumstances for revocation

Telia CA will revoke a 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 BR 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 BR expires or is revoked or terminated, unless the Telia CA has made arrangements to continue maintaining the CRL/OCSP Repository; or
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 authorization;
3. Telia CA obtains evidence that the Subscriber's private key corresponding to the public key in the certificate suffered a key compromise;
4. Telia CA obtains evidence that the validation of domain authorization or control for any Fully Qualified Domain Name (FQDN) or IP address in the Certificate should not be relied upon.

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

1. The Certificate no longer complies with the BR of Sections 6.1.5 and 6.1.6;
2. Telia CA obtains evidence that the certificate was misused;
3. Telia CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
4. Telia CA is made aware of any circumstance indicating that use of a FQDN or IP address in the certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
5. Telia CA is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subordinate FQDN;
6. Telia CA is made aware of a material change in the information contained in the certificate;
7. Telia CA is made aware that the certificate was not issued in accordance with the BR or the applicable CSP;

8. Telia CA determines or is made aware that any of the information appearing in the certificate is inaccurate;
    a. Telia CA's right to issue certificates under the BR expires or is revoked or terminated, unless Telia CA has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by Telia CA' applicable CPS; or
10. Telia CA is made aware of a demonstrated or proven method that exposes the Subscriber's private key to compromise, methods have been developed that can easily calculate it based on the public key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the private key was flawed.

4.9.2 Who can request revocation

The revocation of a certificate can be requested by:

1. A Subscriber or Certificate Requester;
2. Personnel of Telia or Telia CA; or
3. Owner of the server or device that possesses the certificate.

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.

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

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

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

Revocation of certificates using ACME is also available.

4.9.4 Revocation request grace period

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

When a reason for the revocation of a certificate appears, the Subscriber shall immediately inform the Revocation Service.

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

The CA shall not be responsible for the damage caused by illicit use of the Subject's private key.

The CA shall be responsible for the publication of the revocation information on the CRL according to the principles given in this CPS.

4.9.5 Time within which CA must process the revocation request

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

4.9.6 Revocation checking requirement for relying parties

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

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

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

4.9.7 CRL issuance frequency

The 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 server 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

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

4.9.8 Maximum latency for CRLs

Normally latency will be a matter of seconds.

4.9.9 On-line revocation/status checking availability

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

4.9.10 On-line revocation checking requirements

In general all OCSP requests will be signed.

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

The OCSP service is using near-real-time CA database information. The OCSP responder may use the previous status value for a certificate if it is fresher than two hours old (refresh time). In rare circumstances where the connection between OCSP and CA is broken the status information

may be up to 48 hours old (grace period). OCSP responder will respond with an "unknown" status for certificates that do not exist in the CA database.

4.9.11 Other forms of revocation advertisements available

Not applicable.

4.9.12 Special requirements regarding key compromise

In case of CA private key compromise, the procedures defined in 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.

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

4.9.13 Circumstances for suspension

Suspension is not used after March 2013.

4.9.14 Who can request suspension

Suspension is not used after March 2013.

4.9.15 Procedure for suspension request

Suspension is not used after March 2013.

4.9.16 Limits on suspension period

Suspension is not used after March 2013.

4.10 Certificate status services

4.10.1 Operational characteristics

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

4.10.2 Service availability

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

4.10.3 Optional features

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

4.11 End of subscription

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

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

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

Key escrow is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorised third party may gain access to those keys[1].

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

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable

[1] Key escrew: https://en.wikipedia.org/wiki/Key_escrow

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.

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.

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 " Entrance to facility"	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 are 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 and
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 Subscribers 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 Subscriber accounts, privileges and values to enable Telia's self-service software for Subscribers.

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

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 takes 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 taking action 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, and
- 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 CP/CPS 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; and
    - 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 CPS;
    - Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
    - Acceptance and rejection of certificate requests;
    - Issuance of Certificates; and
    - Generation of CRLs 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; and
    - 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 Subscriber CA or the registration or revocation functions are performed by Registration Officer by a Subscriber, 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 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, Telia's Key Compromise Response procedures are followed. 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 to cease operation, Telia makes a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination.

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

a. Provision of notice to parties affected by the termination, such as Subscribers Relying Parties, and Supervisory bodies and informing them of the status of the CA
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. Revoke all active Certificates at the end of the three months' notice period
d. Destroy private keys, including backup copies, in a manner such that the private keys cannot be retrieved
e. 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
f. Terminate all rights for subcontractors to act in the name of the CA which will cease to operate
g. Ensure that all archives and logs are stored for the stated storage time and in accordance with stated instructions
h. Prior terminating the CA services - if applicable depending on the agreed contracts, Telia may transfer provision of the CA services for its existing Subscribers to another CA successor entity

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

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

The CA'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 generates the key pair using server software or hardware security module. Third party key generation systems (e.g., OpenSSL) can be used if the server itself isn't supporting key generation. Telia CA does not create keys for DV and OV certificates.

In case of Seal certificates, the keys are directly generated by and stored in such a secure cryptographic hardware device that complies with AATL technical requirements (FIPS 140-2 level2 or equivalent)

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

6.1.2 Private key delivery to Subscriber

Within DV and OV certificates Telia never creates private keys.

In case of Seal certificates Subscriber typically creates and manages private key according to Subscriber agreement that list relevant AATL requirements. In case when Telia has initiated key generation and delivered such hardware token to Subscriber the activation code (PIN code) delivery is protected in a cryptographically secure manner so that only Subscriber can get it.

6.1.3 Public key delivery to certificate issuer

Subscribers and RAs submit their public key to Telia for certification electronically through the use of a PKCS#10 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 delivered digitally signed in a CSR file and using an encrypted connection.

6.1.4 CA public key delivery to relying parties

Telia makes the CA certificates for Telia CAs available to Subscribers and Relying Parties through the Telia CA's Repository.

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 CAs require that the Subscribers generate at least 2048 bit RSA keys or ECC curve NIST P256 or P384 keys.

6.1.6 Public key parameters generation and quality checking

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

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

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

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

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

6.2.3 Private key escrow

Telia CA does not escrow Subscriber private keys.

6.2.4 Private key backup

Telia CA creates backup copies of CA'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.

Backups may be made of the Subscribers' or RA's private confidentially keys. 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.

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.

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

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

6.2.5 Private key archival

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.

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

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

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 Subscriber's organisation 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.

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

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

6.2.9 Method of deactivating private key

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

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

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

6.2.11 Cryptographic module rating

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.

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

1. FIPS 140-2 Level 2

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

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

6.3 Other aspects of key pair management

6.3.1 Public key archival

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

6.3.2 Certificate operational periods and key pair usage periods

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

Private CA keys 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 certificates between different generations of CA keys are 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.

DV and OV certificates are given a maximum validity period of 398 days. Seal certificates are given maximum validity period of three years.

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

- Certificates issued on or after 1 September 2020 don’t have a validity period greater than 397 days.
- Certificates issued after 1 March 2018, but prior to 1 September 2020, do not have a validity period greater than 825 days.
- Certificates issued after 1 July 2016 but prior to 1 March 2018 do not have a validity period greater than 39 months.

6.4 Activation data

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

6.4.1 Activation data generation and installation

Activation data (Secret Shares) used to protect Telia CA and private keys are 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 Subscribers that acts as the RA role 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.

If Telia CA is not providing the hardware and activation data, the Subscriber is responsible for activation data generation and installation. The Subscriber is recommended to use passwords or strong authentication methods to authenticate users to servers or other devices before the private key is activated. If passwords are used, the CA recommends that Subscriber uses passwords that consists of sufficiently many characters and cannot be easily guessed or concluded. Check also 6.2.8 regarding Seal certificates.

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

6.4.2 Activation data protection

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 Subscriber organisations are strongly recommended to protect the activation data for their private keys against loss, disclosure, modification, or unauthorised use.

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

6.4.3 Other aspects of activation data

Not applicable.

6.5 Computer security controls

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 Certificate Revocation List (CRL) Profile".

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

Field name	Field description and contents
Version	This field states which of the certificate versions defined in the X.509 standard the certificate conforms to. The issued certificates conform to the version 3.
Serial number	The CA generates an individual serial number for every certificate. The number that has been given in this field is unique for every certificate created by the CA system. The software manages the uniqueness of the serial number automatically.
Signature algorithm	The signature algorithm is the set of mathematical rules according to which the CA software executes the signing of the certificate. Identifiers have been allocated for the algorithms that are generally used. The identifier of the algorithm used for the signing of the certificate is given in this field. The signature cannot be verified if the algorithm used is not known. The algorithm that is used for the signing of the certificates is sha256RSA.
Issuer	This field states the name of the Issuer of the certificate. The Issuer name in the certificates of each CA has been described in section 1.3.1. Every DN will be in the form of an X.501 DirectoryString and Issuer DN is same than Subject DN of the Issuing CA in certificates.
Validity	The validity of the certificate is that period of time during which the CA guarantees that it maintains status information of the certificate, in other words about the possible revocation of the certificate. This field states the date and time when the certificate comes into force, and the date and time after which the certificate is no more valid. The certificate can be trusted during its validity period if the certificate has not been published on the CRL Backdating of certificates in order to avoid some deadline or code-enforced restriction is not used by Telia CA.
Subject	This field identifies the Subscriber under whose possession the server possessing the certificate is. The contents of the field have been described in section 3.1.
Subject public key info	This field states the algorithm under which the public key of the Subject shall be used. The Subject's public key itself is also given in this field. The algorithms and key lengths of the Subject keys are described in section 6.1.5.

7.1.1 Version number(s)

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

7.1.2 Certificate extensions

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

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

Extension	Authority	Extension description and contents
Authority key identifier	CA	The identifier of the issuing CA public key is given in this extension. The identifier can be used to identify the public key that corresponds to the private key used for the signing of the certificate. SHA-1 hash algorithm is used to calculate the identifier.

Subject key Identifier	CA	The identifier of the Subject public key that is contained in the certificate is given in this extension. The identifier can be used to pick up those certificates that contain a given public key. SHA-1 hash algorithm is used to calculate the identifier.
Certificate policies	CA	This extension states the policies according to which the certificate has been issued. The relevant policy is identified based on an individual identifier (object identifier, OID) assigned to the policy document or certain certificate type. The identifiers covered by this CPS have been given in section 1.2. This extension is mandatory in Telia TLS certificates. Telia asserts the compliance with the applicable CA Browser Forum standard as described in section 1.1.
CRL distribution points	CA	This extension gives the location where the CRL is available. The exact addresses of the CRLs corresponding to the different certificate classes are given in section 2.1.2.
Key usage	CA	The key usage purposes of the public key contained in the certificate are given in this extension. The CA is not responsible for use other than the given key usage purposes. The key usage extension is optional for Telia server certificates. Purposes KeyCertSign and cRLSign are never set. The key usage purposes of the public keys contained in the OV and DV certificates typically include: Digital Signature, Key Encipherment, Data Encipherment The key usage purposes of the public keys contained in the Seal certificates typically includes: nonRepudiation, Digital Signature
Extended key usage	CA	This extension contains other key usage purposes of the public key except those contained in the "Key usage" extension. A key usage purpose given in this extension may be generally known or privately defined for a certain application. The extended key usage purposes of the public keys contained in the OV and DV certificates include: Server authentication and Client authentication The extended key usage purposes of the public keys contained in the Seal certificates includes: 1.3.6.1.4.1.311.10.3.12 (Microsoft Doc. signing) 1.2.840.113583.1.1.5 (Adobe Authentic Documents Trust)
Subject alternative name	Subscriber	This extension should be used to relate identification information to the Subject. Subject alternative name information used in the Certificates is described in section 3.1.1.
Authority Info Access	CA	This extension may contain two values: a. The URL to CA-certificate b. OCSP service address Typically all server certificates include both listed values.

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

Application of RFC 5280

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

7.1.3 Algorithm object identifiers

SHA-1 functionality was discontinued in 2014 except that old TeliaSonera Root certificates still use SHA-1.
Telia CA certificates are signed using one of the following algorithms:

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

7.1.7 Usage of Policy Constraints extension

Not applicable.

7.1.8 Policy qualifiers syntax and semantics

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

7.1.9 Processing semantics for the critical Certificate Policies extension

Not applicable.

7.2 CRL profile

Telia CAs issue CRLs that are compliant with RFC 5280.

7.2.1 Version number(s)

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

7.2.2 CRL and CRL entry extensions

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

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

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

7.3 OCSP profile

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

7.3.1 Version number(s)

Telia CA OCSP responders conform to RFC6960.

7.3.2 OCSP extensions

The OCSP Nonce extension should be used in OCSP requests.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

An annual Compliance Audit will be performed by an independent, qualified third party. Audits are divided into an unbroken sequence of audit periods. An audit period must not exceed one year in duration.

8.2 Identity/qualifications of assessor

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

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

8.3 Assessor's relationship to assessed entity

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

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

8.4 Topics covered by assessment

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

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

The audit for all certificates covered by this CPS is done in accordance with the relevant version of WebTrust for CAs (http://www.webtrust.org). All OV and DV certificates are audited also in accordance with WebTrust SSL Baseline with Network Security.

In addition, Compliance Audit verifies that Seal certificates are compatible with requirements in relevant Adobe AATL technical specification. TLS DV and OV certificates are compatible with requirements in relevant Mozilla Root Store Policy.

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, the Telia CA Service operator may revoke the CA's certificate.

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

8.6 Communication of results

The Compliance Auditor shall provide the Telia CA Service management with a copy of the results of the Compliance Audit. The results will not be made public unless required by law. Audit reports are published on the Repository and are informed to vendors that have root agreement with Telia. Detailed findings are stored by Telia CA and are not published.

8.7 Self-audits

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

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

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

9.1.1 Certificate issuance or renewal fees

See section 9.1.

9.1.2 Certificate access fees

See section 9.1.

9.1.3 Revocation or status information access fees

See section 9.1.

9.1.4 Fees for other services

See section 9.1.

9.1.5 Refund policy

Subscriber pays Telia for a service and its use pursuant to a price-list or agreement according to invoicing periods defined by Telia. If Subscriber revokes Certificate(s) or requests a revocation to be done by Telia within a calendar month, then the purchase fee will be cancelled and Subscriber is not required to pay the Certificate invoice.

9.2 Financial responsibility

9.2.1 Insurance coverage

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

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

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

9.3 Confidentiality of business information

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

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

9.3.1 Scope of confidential information

The following information are kept confidential and private:

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

considered confidential

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

9.3.2 Information not within the scope of confidential information

The following information is not deemed to be confidential:

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

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

9.3.3 Responsibility to protect confidential information

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

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

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

9.4 Privacy of personal information

Telia does not collect any sensitive or confidential data from Subscriber. Except in scenarios where the CA or RA archive copies of identification documents to validate the identity of a Subscriber. The collected personal information will not be used for any other purpose and Telia's privacy policy[2] governs the CA operations. Telia's Privacy Notice applies to all processing of personal data[3].

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.

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

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

9.6 Representations and warranties

9.6.1 CA representations and warranties

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

9.6.2 RA representations and warranties

The CA bears overall responsibility for the issued certificates. Registration responsibilities of the CA's overall responsibility can, however, be transferred through an agreement between the CA and a Relying Party, to the Relying Party, when the last-mentioned party acts also as Registration Authority. A Subscriber 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 Subscriber responsibility descriptions to Subscribers acting as RA and will require them to comply with the registration policies and Subscriber responsibility descriptions through a certification service agreement. The registration policies and Subscriber 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; and
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 CA accepts no liability for damages incurred by a relying party accepting one of its certificates, or by a Subscriber whose valid certificate is refused or whose revoked certificate is unduly accepted by a Relying Party. It also accepts no liability for damages arising from the non-issuance of a requested certificate, or for the revocation of a certificate initiated by the CA or the appropriate RA acting in conformance with this CPS.

9.8 Limitations of liability

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

9.9 Indemnities

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

9.10 Term and termination

9.10.1 Term

This CPS remains in force until notice of the opposite is communicated by Telia on its web site in the Repository.

9.10.2 Termination

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

9.10.3 Effect of termination and survival

The conditions and effect resulting from termination of this document will be communicated, on the Repository, upon termination outlining the provisions that may survive termination of the document and remain in force.

9.11 Individual notices and communications with participants

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

9.12 Amendments

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

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

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.

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, PMT will assign a new OID and required amendments will be made.

9.13 Dispute resolution provisions

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

9.14 Governing law

This CPS is governed by, and must be interpreted in accordance with, the laws of Finland without regard to the conflict of law provisions.

9.15 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.