



Certificate Policy and Certification Practice Statement for Telia Server Certificates

Prepared by the Telia's Certification Authority Policy Management
Team

Release: 4.8

Valid From: 2022-12-30

Classification: Public

© Telia Company

No part of this document may be reproduced, modified, or distributed in any form or by any means, in whole or in part, or stored in a database or retrieval system, without prior written permission of Telia. However, permission generally applies for reproducing and disseminating this CPS in its entirety if this is at no charge and that no information in the document is added to, removed or changed.

CONTENTS

1. INTRODUCTION	14
1.1 Overview	14
1.2 Document name and identification.....	15
1.3 PKI participants.....	15
1.3.1 Certification authorities.....	16
1.3.2 Registration authorities.....	17
1.3.3 Subscribers.....	17
1.3.4 Relying parties	17
1.3.5 Other participants.....	17
1.4 Certificate usage	18
1.4.1 Appropriate certificate uses.....	18
1.4.2 Prohibited certificate uses.....	18
1.5 Policy administration.....	18
1.5.1 Organisation administering the document.....	18
1.5.2 Contact person	19
1.5.3 Person determining CPS suitability for the policy.....	19
1.5.4 CPS approval procedures	19
1.6 Definitions and acronyms.....	20
1.6.1 Definitions.....	20
1.6.2 Acronyms.....	23
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES.....	25
2.1 Repositories.....	25
2.1.1 CPS Repository.....	25
2.1.2 Revocation Information Repository	25
2.1.3 Certificate Repository.....	25
2.2 Publication of certification information.....	25
2.3 Time or frequency of publication	26
2.4 Access controls on repositories	26
3. IDENTIFICATION AND AUTHENTICATION	27
3.1 Naming.....	27

3.1.1	Types of names.....	27
3.1.2	Need for names to be meaningful.....	29
3.1.3	Anonymity or pseudonymity of Subscribers.....	29
3.1.4	Rules for interpreting various name forms.....	29
3.1.5	Uniqueness of names	29
3.1.6	Recognition, authentication, and role of trademarks.....	29
3.2	Initial identity validation.....	29
3.2.1	Method to prove possession of private key.....	29
3.2.2	Authentication of organisation identity and/or domain name.....	30
3.2.3	Authentication of individual identity	33
3.2.4	Non-verified Subscriber information.....	33
3.2.5	Validation of authority.....	34
3.2.6	Criteria for interoperation.....	35
3.3	Identification and authentication for re-key requests	35
3.3.1	Identification and authentication for routine re-key	35
3.3.2	Identification and authentication for re-key after revocation.....	35
3.4	Identification and authentication for revocation request.....	35
4.	CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	37
4.1	Certificate Application.....	37
4.1.1	Who can submit a certificate application.....	37
4.1.2	Enrolment process and responsibilities	37
4.2	Certificate application processing	38
4.2.1	Performing identification and authentication functions.....	38
4.2.2	Approval or rejection of certificate applications	38
4.2.3	Time to process certificate applications.....	38
4.2.4	Certificate Authority Authorization (CAA)	39
4.3	Certificate issuance	39
4.3.1	CA actions during certificate issuance.....	39
4.3.2	Notification to Subscriber by the CA of issuance of certificate.....	39
4.4	Certificate acceptance	40
4.4.1	Conduct constituting certificate acceptance	40
4.4.2	Publication of the certificate by the CA.....	40
4.4.3	Notification of certificate issuance by the CA to other entities	40
4.5	Key pair and certificate usage	40

4.5.1	Subscriber private key and certificate usage	40
4.5.2	Relying party public key and certificate usage	40
4.6	Certificate renewal	41
4.6.1	Circumstance for certificate renewal	41
4.6.2	Who may request renewal	41
4.6.3	Processing certificate renewal requests	41
4.6.4	Notification of new certificate issuance to Subscriber	41
4.6.5	Conduct constituting acceptance of a renewal certificate.....	41
4.6.6	Publication of the renewal certificate by the CA	41
4.6.7	Notification of certificate issuance by the CA to other entities	41
4.7	Certificate re-key	42
4.7.1	Circumstance for certificate re-key	42
4.7.2	Who may request certification of a new public key	42
4.7.3	Processing certificate re-keying requests	42
4.7.4	Notification of new certificate issuance to subscriber	42
4.7.5	Conduct constituting acceptance of a re-keyed certificate.....	42
4.7.6	Publication of the re-keyed certificate by the CA.....	42
4.7.7	Notification of certificate issuance by the CA to other entities	42
4.8	Certificate modification	42
4.8.1	Circumstance for certificate modification.....	42
4.8.2	Who may request certificate modification	43
4.8.3	Processing certificate modification requests	43
4.8.4	Notification of new certificate issuance to subscriber	43
4.8.5	Conduct constituting acceptance of modified certificate	43
4.8.6	Publication of the modified certificate by the CA	43
4.8.7	Notification of certificate issuance by the CA to other entities	43
4.9	Certificate revocation and suspension	43
4.9.1	Circumstances for revocation	43
4.9.2	Who can request revocation.....	44
4.9.3	Procedure for revocation request.....	45
4.9.4	Revocation request grace period.....	47
4.9.5	Time within which CA must process the revocation request.....	48
4.9.6	Revocation checking requirement for relying parties	48
4.9.7	CRL issuance frequency	48

4.9.8	Maximum latency for CRLs	48
4.9.9	On-line revocation/status checking availability.....	48
4.9.10	On-line revocation checking requirements	48
4.9.11	Other forms of revocation advertisements available	49
4.9.12	Special requirements regarding key compromise	49
4.9.13	Circumstances for suspension	49
4.9.14	Who can request suspension.....	49
4.9.15	Procedure for suspension request.....	49
4.9.16	Limits on suspension period	49
4.10	Certificate status services	49
4.10.1	Operational characteristics.....	49
4.10.2	Service availability	49
4.10.3	Optional features	49
4.11	End of subscription	50
4.12	Key escrow and recovery	50
4.12.1	Key escrow and recovery policy and practices	50
4.12.2	Session key encapsulation and recovery policy and practices.....	50
5.	FACILITIES, MANAGEMENT, AND OPERATIONAL CONTROLS.....	51
5.1	Physical controls	51
5.1.1	Site location and construction.....	51
5.1.2	Physical access.....	51
5.1.3	Power and air conditioning.....	52
5.1.4	Water exposures	52
5.1.5	Fire prevention and protection	52
5.1.6	Media storage	53
5.1.7	Waste disposal	53
5.1.8	Off-site backup	53
5.2	Procedural controls.....	53
5.2.1	Trusted roles.....	53
5.2.2	Number of persons required per task.....	54
5.2.3	Identification and authentication for each role	55
5.2.4	Roles requiring separation of duties.....	56
5.3	Personnel controls	56
5.3.1	Qualifications, experience, and clearance requirements.....	56

5.3.2	Background check procedures	56
5.3.3	Training requirements.....	57
5.3.4	Retraining frequency and requirements.....	57
5.3.5	Job rotation frequency and sequence	57
5.3.6	Sanctions for unauthorised actions	57
5.3.7	Independent contractor requirements	57
5.3.8	Documentation supplied to personnel.....	58
5.4	Audit logging procedures.....	58
5.4.1	Types of events recorded	58
5.4.2	Frequency of processing log	59
5.4.3	Retention period for audit log.....	59
5.4.4	Protection of audit log	59
5.4.5	Audit log backup procedures	59
5.4.6	Audit collection system (internal vs. external).....	59
5.4.7	Notification to event-causing subject	59
5.4.8	Vulnerability assessments.....	59
5.5	Records archival	60
5.6	Key changeover	61
5.7	Compromise and disaster recovery	62
5.8	CA or RA termination.....	63
6.	TECHNICAL SECURITY CONTROLS.....	65
6.1	Key pair generation and installation.....	65
6.1.1	Key pair generation	65
6.1.2	Private key delivery to Subscriber	65
6.1.3	Public key delivery to certificate issuer.....	65
6.1.4	CA public key delivery to relying parties	66
6.1.5	Key sizes	66
6.1.6	Public key parameters generation and quality checking.....	66
6.1.7	Key usage purposes (as per X.509 v3 key usage field).....	66
6.2	Private key protection and cryptographic module engineering controls.....	66
6.2.1	Cryptographic module standards and controls.....	66
6.2.2	Private key (n out of m) multi-person control	67
6.2.3	Private key escrow.....	67
6.2.4	Private key backup	67

6.2.5	Private key archival	67
6.2.6	Private key transfer into or from a cryptographic module	68
6.2.7	Private key storage on cryptographic module	68
6.2.8	Method of activating private key	68
6.2.9	Method of deactivating private key	68
6.2.10	Method of destroying private key	69
6.2.11	Cryptographic module rating	69
6.3	Other aspects of key pair management.....	69
6.3.1	Public key archival	69
6.3.2	Certificate operational periods and key pair usage periods.....	69
6.4	Activation data.....	70
6.4.1	Activation data generation and installation.....	70
6.4.2	Activation data protection.....	70
6.4.3	Other aspects of activation data	71
6.5	Computer security controls.....	71
6.6	Life cycle security controls.....	71
6.7	Network security controls	72
6.8	Timestamping	72
7.	CERTIFICATE, CRL, AND OCSP PROFILE	73
7.1	Certificate profile	73
7.1.1	Version number(s)	73
7.1.2	Certificate extensions.....	73
7.1.3	Algorithm object identifiers	76
7.1.4	Name forms.....	76
7.1.5	Name constraints	76
7.1.6	Certificate policy object identifier.....	76
7.1.7	Usage of Policy Constraints extension.....	76
7.1.8	Policy qualifiers syntax and semantics.....	77
7.1.9	Processing semantics for the critical Certificate Policies extension.....	77
7.2	CRL profile	77
7.2.1	Version number(s).....	77
7.2.2	CRL and CRL entry extensions	77
7.3	OCSP profile	77
7.3.1	Version number(s)	77

7.3.2	OCSP extensions.....	77
8.	COMPLIANCE AUDIT AND OTHER ASSESSMENTS.....	78
8.1	Frequency or circumstances of assessment.....	78
8.2	Identity/qualifications of assessor.....	78
8.3	Assessor's relationship to assessed entity.....	78
8.4	Topics covered by assessment.....	78
8.5	Actions taken as a result of deficiency.....	79
8.6	Communication of results.....	79
8.7	Self-audits.....	79
9.	OTHER BUSINESS AND LEGAL MATTERS.....	80
9.1	Fees.....	80
9.1.1	Certificate issuance or renewal fees.....	80
9.1.2	Certificate access fees.....	80
9.1.3	Revocation or status information access fees.....	80
9.1.4	Fees for other services.....	80
9.1.5	Refund policy.....	80
9.2	Financial responsibility.....	80
9.2.1	Insurance coverage.....	80
9.2.2	Other assets.....	80
9.2.3	Insurance or warranty coverage for end-entities.....	80
9.3	Confidentiality of business information.....	80
9.3.1	Scope of confidential information.....	80
9.3.2	Information not within the scope of confidential information.....	81
9.3.3	Responsibility to protect confidential information.....	81
9.4	Privacy of personal information.....	81
9.5	Intellectual property rights.....	81
9.6	Representations and warranties.....	82
9.6.1	CA representations and warranties.....	82
9.6.2	RA representations and warranties.....	82
9.6.3	Subscriber representations and warranties.....	82
9.6.4	Relying party representations and warranties.....	83
9.6.5	Representations and warranties of other participants.....	83
9.7	Disclaimers of warranties.....	83
9.8	Limitations of liability.....	83

CP & CPS for Telia Server Certificates

9.9	Indemnities.....	83
9.10	Term and termination	84
9.10.1	Term.....	84
9.10.2	Termination.....	84
9.10.3	Effect of termination and survival	84
9.11	Individual notices and communications with participants.....	84
9.12	Amendments.....	84
9.12.1	Procedure for amendment.....	84
9.12.2	Notification mechanism and period	85
9.12.3	Circumstances under which OID must be changed.....	85
9.13	Dispute resolution provisions	85
9.14	Governing law.....	85
9.15	Compliance with applicable law	85
9.16	Miscellaneous provisions	85
9.16.1	Entire agreement	85
9.16.2	Assignment.....	85
9.16.3	Severability.....	85
9.17	Other provisions	86

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

CP & CPS for Telia Server Certificates

Version	Date	Change	Author
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

CP & CPS for Telia Server Certificates

Version	Date	Change	Author
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
4.1	2021-06-11	Minor clarification on terminology, applicable law, and formatting	Telia CA Policy Management Team
4.2	2021-07-15	Removed the certificate OIDs from section 1.1, added further explanation about the audit requirements according to ETSI, clarifications on definitions, clarifications on Mozilla root program requirements, other minor changes	Telia CA Policy Management Team
4.3	2021-09-09	HTTPS status response code, Domain Names, and IP Addresses validation reuse period, ETSI updates	Telia CA Policy Management Team
4.4	2021-10-14	ETSI compliance	Telia CA Policy Management Team
4.5	2022-04-06	Update section 5.1 to reflect current state of operations, specifically sections 5.1.2.1 and 5.1.2.2 respectively. Minor typographic and spelling corrections throughout the document Section 7.1.2, Table defining certificate extensions use in TLS certificates, "Key Usage – CA" modified to meet industry best practices Minor changes in the CA termination plan.	Telia CA Policy Management Team

CP & CPS for Telia Server Certificates

Version	Date	Change	Author
4.6	2022-06-07	<p>As per [ETSI 319 401] REQ 6.3-9 and -10</p> <p>“Information security policy;</p> <p>The maximum interval between two checks shall be documented in the trust service practice statement”</p> <p>Disclosure of maximum interval added to the section 9.12</p> <p>Problem reporting contact information added to the section 1.5.2</p>	Telia CA Policy Management Team
4.7	2022-09-15	<p>Telia Sans font type face changed through the document to reflect Telia’s corporate document format policy.</p> <p>In sections 4.4.3 and 4.6.7 language clarified to express intended purpose</p> <p>Section 4.9.3, amended by Mozilla’s instructions as required by updated Mozilla’s Root Store Policy for revocation code use and instructions to Subscribers</p> <p>Wording changed in sections 1.1, 4.2.5 and 4.4.1 to clarify the meaning of information presented.</p>	Telia CA Policy Management Team
4.8	2022-12-14	<p>In section 1.5.4 disclosed PMT’s CPS review policy</p> <p>In section 3.2.5 for OV removed obsoleted “certificate based login option”</p>	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.

In the event of any inconsistency between this CPS and those documents, those documents take precedence over this CPS. 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

CP & CPS for Telia Server Certificates

establish that Telia CA verified that the business was legally organised, used domain names were owned or managed by the Subject.

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

- a. **Telia DV certificate:** to authenticate servers and establishing secure TLS sessions with end clients. In this type of certificate 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 of certificate domain name of the server, existence of the organisation and other attributes including name, type, status, and physical address is validated by Telia,
- c. **Telia client certificate:** for identifying individual users, securing email communications and document signing, or
- d. **Telia document signing (Seal) 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:** As stated on the cover page
- **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:

CA	Type	CP OIDs
<ul style="list-style-type: none">• TeliaSonera Root CA v1• Telia Root CA v2	Root CA	1.3.6.1.4.1.271.2.3.1.1.2
<ul style="list-style-type: none">• TeliaSonera Server CA v2• Telia Server CA v3	TLS OV certificates	2.23.140.1.2.2
<ul style="list-style-type: none">• Telia Domain Validation CA v2• Telia Domain Validation CA v3	TLS DV certificates	2.23.140.1.2.1
Telia Document Signing CA v3	Telia Seal certificates	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 key pairs and subject simultaneously (for validity check through self-signed or cross-signed path). Clients can use either one when doing PKI path validation.

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

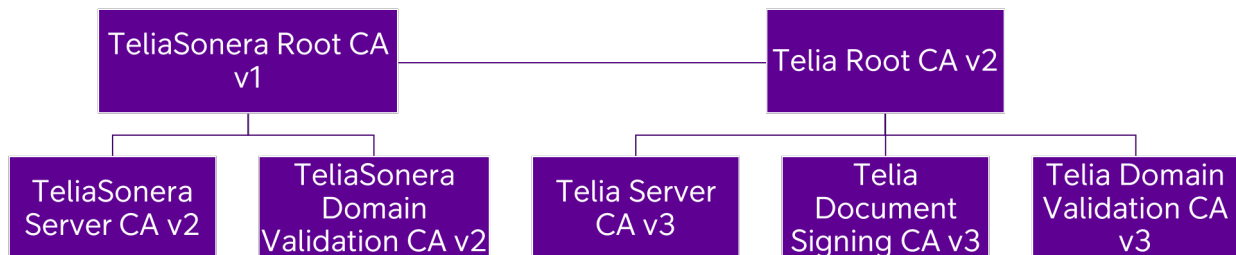


Figure 1, Telia Server Certificate PKI Hierarchy

The CAs are responsible for managing the certificate life cycle of End-Entity certificates signed by the CAs. This will include:

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

This 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

CP & CPS for Telia Server Certificates

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 Server CA v3**
SHA2 Fingerprint:
1281AD8FABE883F209E9636448D1A80C373DAA7686C813A270FAD48F5F5E589A
- **Telia Document Signing CA v3**
SHA2 Fingerprint:
6924A4DD82948DA53F6FB933E895A0F6581C8DBDEBABB36FC11CAC25E9C0335A
- **Telia Domain Validation CA v3**
SHA2 Fingerprint:
A7E83056E9B3D9DDB1816B95518F6A5E5A1DFDFA28F60533B1C850855EAA4263

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 in this CPS are performed internally by Telia. Telia will not delegate domain validation to be performed by a third-party.

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 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	Appropriate usage
<ul style="list-style-type: none"> • TeliaSonera Root CA v1 • Telia Root CA v2 	These CAs issue certificates for subCAs.
<ul style="list-style-type: none"> • TeliaSonera Server CA v2 • Telia Server CA v3 	These certificates are used for TLS (OV) communication where the risks of data compromise are moderate or high.
<ul style="list-style-type: none"> • Telia Domain Validation CA v2 • Telia Domain Validation CA v3 	These certificates are used for TLS (DV) communication where the risks of data compromise are low.
Telia Document Signing CA v3	These certificates are used for document signing (OV) such as Adobe documents to ensure the signed document is authentic and has not been compromised after signing by the author.

1.4.2 Prohibited certificate uses

Applications using certificates issued under this CPS shall consider 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 considered 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:

CP & CPS for Telia Server Certificates

Telia Finland Oyj Pasilan Asema-aukio 1 FI-00520 Helsinki, Finland Phone: +358 (0) 20401 Internet: https://cps.trust.telia.com/CPS Business ID: 1475607-9
--

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

Problem reporting instructions, please see:

https://support.trust.telia.com/palvelinvarmenneturvallisuus_en.html

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.

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

1.6 Definitions and acronyms

1.6.1 Definitions

Affiliate	A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.
Agent	A person, contractor, service provider that is providing a service to an organisation under contract and are subject to the same corporate policies as if they were an employee of the organisation.
Applicant	The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Initial Certificate was created (initialization), the Applicant is referred to as the Subscriber. For Certificates issued to End-entities, the Subscriber (Certificate Applicant) is the entity that controls or operates/maintains the end-entity to which the Certificate is issued, even if the end-entity is sending the actual certificate request.
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.
CA/Browser Forum	A group of representatives from certificate authorities and browser vendors to discuss issues surrounding the existing market for server certificates, e.g., certificates used in authenticating TLS-enabled web sites and other servers (e.g., mail servers) to users.
CAA	From RFC 6844 (http://tools.ietf.org/html/rfc6844): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify the Certification Authorities (CAs) authorised to issue certificates for that domain. Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate mis-issue."
Certificate	An electronic document issued by Telia to a person or entity mainly for verifying the identity of the sender/receiver of an electronic message, and/or for providing the means to encrypt/decrypt messages between sender and receiver (e.g., binding an entity to their public key).
Certificate Policy (CP)	Named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements. It is the principal statement of certificate policy governing the organisational PKI. The CP is a high-level document that describes the requirements, terms and conditions, and policy for issuing, utilizing and managing certificates issued by a CA.
Certificate Request	A process where a natural person (the Subscriber or someone employed by the Subscriber) or an authorised agent with the authority of representing the Subscriber that completes and submits a certificate request.

CP & CPS for Telia Server Certificates

Certificate Revocation List (CRL)	A periodically issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation. CRL can be used to check the status of certificates.
Certification Authority (CA)	CA is a trusted entity such as Telia that is authorised to create, sign, distribute, and revoke certificates. CA is also responsible for distributing certificate status information and providing a repository where certificates and certificate status information is stored.
Certification Chain	An ordered list of Certificates containing a Subscriber Certificate and CA Certificates, which terminates in a root Certificate.
Certification Practice Statement (CPS)	CPS is a document that defines the legal, commercial and technical practices for approving, issuing, using and managing Telia Server and Client certificates. It also outlines the roles and responsibilities of the parties involved in maintaining the Telia public key infrastructure.
Client Certificate	A digital certificate in which information about the organization and email of holding the certificate has been validated by Telia.
Cross Certification	The process describing the establishing of trust between two or more CAs. Usually involves the exchange and signing of CA certificates and involves the verification of assurance levels.
Cryptographic Module	A unit in which encryption keys are stored together with a processor which can carry out critical cryptographic algorithms. Examples of cryptographic modules include electronic ID D cards.
Digital Signature	A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents.
Distinguished Name (DN)	It is a unique entry identifier throughout the complete directory. No two entries can have the same DN within the same directory. A DN is used in certificates to uniquely identify a certificate-owner.
Document Signing (Seal) Certificate	Used for authenticating documents from Adobe PDF (AATL), Microsoft Office, OpenOffice, and LibreOffice.
Domain Name	The label assigned to a node in the Domain Name System (DNS).
Domain Name Registrant	Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.
Domain Name Registrar	A person or entity that registers Domain Names under the auspices of or by agreement with: i. the Internet Corporation for Assigned Names and Numbers (ICANN), ii. a national Domain Name authority/registry, or iii. a Network Information Center (including their affiliates, contractors, delegates, successors, or assignees).
Domain Namespace	The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.
Domain Validated (DV) TLS Certificate	A digital certificate for a web site or other server in which the information about the domain name has been validated by Telia.
Dual Control	A process utilizing two or more separate entities (usually persons), operating in concert, to protect sensitive functions or information, whereby no single entity is able to access or utilize the materials, e.g., cryptographic key.
End-Entity	User of PKI certificates and/or end user system that is the subject of a certificate and cannot sign other certificates.
Enterprise RA	An employee or agent of an organisation unaffiliated with the CA who authorises issuance of Certificates to that organisation.

CP & CPS for Telia Server Certificates

Internal Server Name	A Server Name (which may or may not include an Unregistered Domain Name) that is not resolvable using the public DNS.
Key	When used in the context of cryptography, it is a secret value, a sequence of characters that is used to encrypt and decrypt data. A key is a unique, generated electronic string of bits used for encrypting, decrypting, e-signing or validating digital signatures.
Key Pair	Often referred to as public/private key pair. One key is used for encrypting and the other key used for decrypting. Although related, the keys are sufficiently different that knowing one does not allow derivation or computation of the other. This means that one key can be made publicly available without reducing security, provided the other key remains private.
Legal Entity	An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.
Object Identifier	The unique alpha-numeric identifier registered under the ISO registration standard to reference a standard object or class.
OCSP Responder	An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.
Online Certificate Status Protocol	An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.
Private Key	The private key is one of the keys in a public/private key pair. This is the key that is kept secret as opposed to the other key that is publicly available. Private keys are utilized for digitally signing documents, uniquely authenticating an individual, or decrypting data that was encrypted with the corresponding public key.
Public Key	The community verification key for digital signature and the community encryption key for encrypting information to a specific Subscriber.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Publicly Trusted Certificate	A Certificate that is trusted by virtue of the fact that its corresponding Root certificate is distributed as a trust anchor in widely available application software.
Qualified Auditor	A natural person or Legal Entity that meets the requirements of Section 8.2.
Registered Domain Name	A Domain Name that has been registered with a Domain Name Registrar.
Registration Authority (RA)	An entity that performs registration services on behalf of a CA. RAs work with a particular CA to vet requests for certificates that will then be issued by the CA.
Re-keying	The process of replacing or updating the key(s). The expiration of the crypto period involves the replacement of the public key in the certificate and therefore the generation of a new certificate.
Reliable Data Source	An identification document or source of data used to verify Subject Identity Information that is generally recognised among commercial enterprises and governments as reliable, and which was created.
Relying Party	Anybody who relies on the certificates issued by Telia (including all end users and operating system vendors who trust Telia certificates).
Repository	An online database containing publicly disclosed Telia PKI governance documents, and certificate status information, either in the form of a CRL or an OCSP response. Currently at this link: https://cps.trust.telia.com .

CP & CPS for Telia Server Certificates

Revocation	PKI, revocation is the action associated with revoking a certificate. Revoking a certificate is to make the certificate invalid before its normal expiration. The Certification Authority that issued the certificate is the entity that revokes a certificate. The revoked status is normally published on a CRL.
Subject	The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.
Subject Identity Information	Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field.
Subordinate CA	A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.
Subscriber	A person or entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement and Terms of Use.
Subscriber Agreement	An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.
Terms of Use	Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with the CA/B Forum requirements when the Applicant/Subscriber is an Affiliate of the Telia CA or is the CA.
TLS Certificate	Certificate utilized to verify the authentication of a web or application server to the end user (client) when a connection is being established via an TLS session (secure channel). There are different types of TLS certificates: single-domain, multi-domain and wild-card (SAN).
Token	Hardware devices, normally associated with a reader, used to store and/or generate encryption keys, such as smartcards and USB tokens.
Trustworthy System	Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.
Unregistered Domain Name	A Domain Name that is not a Registered Domain Name.
Valid Certificate	A Certificate that passes the validation procedure specified in RFC 5280.
Validity Period	Prior to 2020-09-01, the period of time measured from the date when the Certificate is issued until the Expiry Date. For Certificates issued on or after 2020-09-01, the validity period is as defined within RFC 5280, Section 4.1.2.5: the period of time from notBefore through notAfter, inclusive.
WHOIS	Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.
Wildcard Certificate	A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully Qualified Domain Names contained in the Certificate.
Wildcard Domain Name	A Domain Name consisting of a single asterisk character followed by a single full stop character ("*.") followed by a Fully Qualified Domain Name.

1.6.2 Acronyms

AATL	Adobe Approved Trust List
BR	Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
CA	Certification Authority
CP	Certificate Policy

CP & CPS for Telia Server Certificates

CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DER	Distinguished Encoding Rules
DN	Distinguished Name
DSA	Digital Signature Algorithm
DV	Domain Validation
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
OCSP	On-line Certificate Status Protocol
OID	Object Identifier
PDF	Portable Document Format
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509 (IETF Working Group)
PMT	Policy Management Team
RA	Registration Authority
RFC	Request for Comments
RSA	Rivest-Shamir-Adleman asymmetric encryption algorithm
S/MIME	Secure Multipurpose Internet Mail Extension
SHA	Secure Hash Algorithm
TLS	Transport Layer Security
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VPN	Virtua Private Network

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

2.1.1 CPS Repository

A full text version of this CPS is published at the [Repository](#).

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/>.

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

2.2 Publication of certification information

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

- a. This CPS
- b. 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

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

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

3.1.1.2 Subordinate CAs

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

Attribute	Description of value
commonName (CN, OID 2.5.4.3)	Name of the subordinate CA
OrganizationName (O, OID 2.5.4.10)	Name of the CA organisation. The name is either Telia Finland Oyj or TeliaSonera
Country (C, OID 2.5.4.6)	Country where the CA organisation is incorporated

3.1.1.3 Subscriber Certificates

The following attributes are used in the Subject field of the 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	A single host domain name (FQDN) which is owned or controlled by the Subject	A name of the service or server (FQDN) which is owned or controlled by

CP & CPS for Telia Server Certificates

Attribute	Description – OV TLS	Description – DV TLS	Description – Seal
	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.	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.	the Subject.
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 OV certificates.	Not allowed	Optional
businessCategory (OID: 2.5.4.15)	Optional in OV certificates.	Not allowed	Optional
serialNumber	Optional in OV	Not allowed	Optional

Attribute	Description – OV TLS	Description – DV TLS	Description – Seal
(OID: 2.5.4.5)	certificates.		

For Seal and OV certificates, the “Subject” field may also include following attributes depending on the usage and purpose of the certificate:

Attribute	Description – OV TLS, Seal
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.

Distinguished Name (DN) or Subject Alternative Name attributes may be used additionally if necessary and they are verified by the CA. 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 punycode converted version of the string will be used.

3.1.2 Need for names to be meaningful

Names will be meaningful as stated in the section 3.1.1.

3.1.3 Anonymity or pseudonymity of Subscribers

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 third-party (e.g. 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 (CSR) or separately on the order form so that the latter will override the former if both exist.

In case of Seal and 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 Server 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 CSR has IP address, Telia will verify 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.

For validations performed, redirects are the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, Section 6.4, or a 308 HTTP status code response, as defined in RFC 7538, Section 3. Redirects are the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2.

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 CA Security 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 CA Security 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

<p>OV order via public web form or via using self-service software</p>	<p>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.</p> <p>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.</p> <p>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.</p> <p>Authentication is based on secure combination of SMS-OTP and weblinks with unique hash values.</p> <p>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.</p>
<p>DV order via public web form or via using self-service software.</p>	<p>Telia verifies host domain name/IP address ownership or control of those by using methods listed in the BR.</p>
<p>Seal order via web form</p>	<p>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.</p> <p>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).</p> <p>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.</p>

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 and authorisation 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. The Revocation Service is responsible for the verification of the authenticity and authorisation of the request to revoke the certificate.

In certain situations where there is an identified risk of abuse of the private key or when it is obvious that the authorised use of the key is prevented, it may be necessary to revoke the certificate 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. The Security Board in the CA is responsible for the verification of the authenticity and authorisation of the request to revoke the certificate.

For the TLS/Seal certificates, Subscriber contact person requesting revocation is

CP & CPS for Telia Server Certificates

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 Roles 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	Similar to 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	<p>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.</p> <p>Before the application can be submitted, the Subscriber has to accept the Subscriber responsibilities and terms and conditions of the service.</p>
---	---

<p>DV and OV order using Telia's self-service software</p>	<p>A person in a Subscriber Organisation applies for certificates to Devices (OV 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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
---	--

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. Provided verification data will expire in 825 days for OV and DV certificate applications. However, the maximum validation reuse periods for FQDN and IP Address validation is 398 days.

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

<p>CA</p>	<p>Telia will process the applications within reasonable time frame.</p>
<p>Seal, DV or OV order via public web form</p>	<p>Telia process the applications within reasonable time frame and usually within one workday.</p>

<p>DV or OV order using Telia's self-service software</p>	<p>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.</p>
--	--

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 will not 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

Telia has multiple Lint-like checks to verify certificate structure before enrolment to prevent any misissuance. Also, Lint is used the night after enrolment to verify the syntax. Any failure in pre-checks will prevent enrolment and any failure in Lint check would cause quick revocation according to this CPS.

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

<p>CAs</p>	<p>Telia CA Policy Management Team (PMT)</p>
<p>Seal, DV or OV order via public web form</p>	<p>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.</p>
<p>DV or OV order using Telia's self-service software</p>	<p>The certificate is available for the Subscriber's Registration Officer in the RA tool after the issuance.</p>

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

4.4.2 Publication of the certificate by the CA

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

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> prior CA certificate is used for issuance of certificates.

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
- 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	<p>The person has an option to renew certificates using the tools provided by the CA which may use the old CSR file to renew the certificate.</p> <p>Subscriber Certificate Requester is responsible to ensure that the certificate information is still valid and that there are no other obstacles to the renewal.</p> <p>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.</p>

4.6.4 Notification of new certificate issuance to Subscriber

The Subscriber is notified as described in section 4.3.2

4.6.5 Conduct constituting acceptance of a renewal certificate

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

4.6.6 Publication of the renewal certificate by the CA

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

4.6.7 Notification of certificate issuance by the CA to other entities

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

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
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:

CP & CPS for Telia Server Certificates

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
5. Telia CA is made aware of a demonstrated or proven method that exposes the Subscriber's private key to compromise, methods have been developed that can easily calculate it based on the public key (such as a Debian weak key, see <http://wiki.debian.org/SSLkeys>), or if there is clear evidence that the specific method used to generate the private key was flawed

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

1. The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;
2. The CA obtains evidence that the Certificate was misused;
3. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
4. The CA is made aware of any circumstance indicating that use of a Fully Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
5. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully Qualified Domain Name;
6. The CA is made aware of a material change in the information contained in the Certificate;
7. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the applicable CP/CPS;
8. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate;
9. The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
10. Revocation is required by the applicable CP/CPS; or
11. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.

4.9.2 Who can request revocation

The revocation of a certificate can be requested by:

1. A Subscriber or Certificate Requester
2. Personnel of Telia or Telia CA
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. The Subscriber of a revoked certificate, where possible, will be informed of the change of status of the certificate. If the request cannot be confirmed within 24 hours, then the status will not be changed.

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.

Instructions and obligation for subscribers submitting revocation request

TLS Certificates may be revoked ONLY for one of the following reasons (Telia CA will reject subscriber revocation requests made with any other reason):

- keyCompromise (RFC 5280 CRLReason #1)
- privilegeWithdrawn (RFC 5280 CRLReason #9), this option is only for Telia CA's use and is not made available to subscribers
- cessationOfOperation (RFC 5280 CRLReason #5)
- affiliationChanged (RFC 5280 CRLReason #3)
- superseded (RFC 5280 CRLReason #4)
- unspecified (RFC 5280 CRLReason #0), this is the default option available for revocation request

The revocation reason codes listed above are listed in order of priority such that if the situation is that multiple revocation reasons apply, the revocation reason of higher priority (as per the list) should be indicated.

For example, if both cessationOfOperation and superseded apply, then cessationOfOperation should be used.

Guidance and instructions on how to set the appropriate reason and reason code

- **keyCompromise (RFC 5280 CRLReason #1)**
The certificate subscriber must choose the “keyCompromise” revocation reason when they have reason to believe that the private key of their certificate has been compromised, e.g. an unauthorized person has had access to the private key of their Certificate.
- **privilegeWithdrawn (RFC 5280 CRLReason #9)**
Telia CA must use this revocation code when there has been a subscriber-side infraction that has not resulted in keyCompromise, such as the certificate subscriber provided misleading information in their certificate request or has not upheld their material obligations under the subscriber agreement or terms of use

This revocation code is not available for subscriber revocation request.

- **cessationOfOperation (RFC 5280 CRLReason #5)**
The certificate subscriber should choose the "cessationOfOperation" revocation reason when they no longer own all the domain names in the Certificate or when they will no longer be using the Certificate because they are discontinuing their website
- **affiliationChanged (RFC 5280 CRLReason #3)**
The certificate subscriber should choose the "affiliationChanged" revocation reason when their organization's name or other organizational information in the Certificate has changed.

This reason code is not available for DV certificates and thus **MUST NOT** be used when revoking DV certificate.

- **superseded (RFC 5280 CRLReason #4)**
The certificate subscriber should choose the "superseded" revocation reason when they request a new certificate to replace their existing certificate.
- **No reason provided or unspecified (RFC 5280 CRLReason #0)**
When the reason codes below do not apply to the revocation request, the subscriber must not provide a reason code other than "unspecified".
NOTE, this reason code is the default if nothing else is provided by the subscriber. For unspecified reason code the CRL shall not contain reason code.

Additional guidance on and explanation of the significance and consequences of the keyCompromise reason

When key compromise has been demonstrated Telia CA **MUST** revoke all instances of

that key across all subscribers. Therefore, Telia CA MUST consider situations that may occur when the certificate subscriber requests that their Certificate be revoked for the keyCompromise revocation reason. With the acknowledgement that a certificate signing request (CSR) alone does not prove possession of the certificate's private key for the purpose of initiating a revocation.

Following clarification is made regarding the scope of revocation when the certificate subscriber requests revocation for keyCompromise revocation reason:

- a) The scope of revocation depends on whether the certificate subscriber has proven possession of the private key of the Certificate.
- b) If anyone requesting revocation has previously demonstrated or can currently demonstrate possession of the private key of the Certificate, then Telia CA MUST revoke all instances of that key across all subscribers.
- c) If the certificate subscriber requests that Telia CA revoke the Certificate for keyCompromise and has not previously demonstrated and cannot currently demonstrate possession of the associated private key of that Certificate, Telia CA MAY revoke all certificates associated with that subscriber that contain that public key.

Telia CA WILL NOT assume that it has evidence of private key compromise for the purposes of revoking the certificates of other subscribers, but MAY block issuance of future certificates with that key for that subscriber.

All the above guidance and instructions must also be adhered to when requesting Certificate revocation using Telia's certificate automation services such as Automated Certificate Management Environment (ACME) or equivalent certificate automation service provided by Telia.

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

4.9.13 Circumstances for suspension

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

4.10.2 Service availability

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

4.10.3 Optional features

Relying parties may decide if they are using OCSP or CRL to verify certificate status. Telia recommends using OCSP as primary method and CRL as secondary method. However, there might be possible to have minor delays due to technical issues affecting the status updates.

4.11 End of subscription

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

The end of a subscription because 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

¹Key escrow: 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 (TRAFICOM/54045/03.04.05.00/2020) issued by TRAFICOM (Finnish Transport and Communications Agency). Within these server rooms, key components are locked in separate, freestanding security cabinets.

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

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

5.1.1.2 RA Site location and construction

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

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

- 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 are 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 components are tied to an uninterruptible power supply system.

This system is 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 up to five (5) tiers of distinctive physical security layers where the CA systems and other important CA devices have been placed in a security vault. Protection and controls are progressively restrictive from tier to tier.

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

5.1.2.2 RA Site Physical access

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

5.1.3 Power and air conditioning

Telia secure premises are equipped with primary and backup:

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

5.1.4 Water exposures

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

5.1.5 Fire prevention and protection

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

5.1.6 Media storage

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

5.1.7 Waste disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or erased in accordance the manufacturers' guidance prior to disposal. Other waste is disposed of in accordance with Telia's normal waste disposal requirements.

5.1.8 Off-site backup

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

5.2 Procedural controls

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

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

5.2.1 Trusted roles

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

- a. The administration of CA private keys and 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 Roles 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 Roles having a Trusted Role. Persons chosen to become Trusted Roles by obtaining a Trusted Role must successfully complete the screening requirements of section 5.3.

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

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

Typical duties which may be administered by the CAA include:

- a. creating CA certificates
- b. personalising cards
- c. generating CA and central RA keys
- d. configuration of CA and RA applications
- e. generating revocation lists
- f. Checking the certificate issue log

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

Typical duties which may be administered by the SA include:

- a. installations of hardware and software
- b. system maintenance
- c. changing of backup media

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

5.2.1.4 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.

5.2.1.5 Registration Officer: RA Office and Customer Service staff of the CA. Registration Officers in the Subscribers are not Trusted Roles. Typical duties of the Registration Officer include processing and approving certificate applications and submitting certificate requests to the CA system that issues and signs the certificates. Registration Officers also create new Subscriber accounts, privileges, and values to enable Telia's self-service software for Subscribers.

Telia has chosen to divide the responsibility for the above roles into sub-roles to increase security.

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 Roles.

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 Roles 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 Roles that works in conjunction. Either persons work physically together, or the other Trusted Roles is involved via following security controls:

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

Other requirements in terms of the presence of people when carrying out other tasks involving 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 CA System Administrator or Registration Officer do not simultaneously work in any of the other roles involving the system.

5.2.3 Identification and authentication for each role

For all personnel chosen to become Trusted Roles, verification of identity is performed through the personal (physical) presence of such personnel before Trusted Roles 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 (except for the CA signing certificates) is:

- a. Personal and directly attributable to the Trusted Roles;

- b. Restricted to actions authorised for that role in respective CA and RA software, operating system, and procedural controls.

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

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

Identification of the RA roles takes place within the CA and RA system applications, and it is based on strong authentication either using personal operator cards, 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 Roles may not have other roles which may be deemed to be in opposition to the role assigned.

Personnel identified to become Trusted Roles 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 Roles, if permitted by the local laws. The factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted Roles or for acting against an existing Trusted Roles generally include the following:

CP & CPS for Telia Server Certificates

- Misrepresentations made by the candidate or Trusted Role,
- 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 considering 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 Roles or the termination of existing Trusted Roles.

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 Roles. 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 Roles.

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

5.5 Records archival

Telia 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.

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

5.5.4 Archive backup procedures

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

5.5.5 Requirements for timestamping of records

All documents archived pursuant to this section will be marked with the date of their creation or execution.

The date and time information in the CA system and certain other system logs is synchronized with an external coordinated universal time source (UTC). The time used for the provision of revocation services is synchronized with UTC at least once every 24 hours.

5.5.6 Archive collection system (internal or external)

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

5.5.7 Procedures to obtain and verify archive information

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

5.6 Key changeover

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

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

5.6.1 Self-Signed CA

Changing of CA keys for a self-signed CA will be done, 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.

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. Monitoring activities are considered based on the sensitivity/criticality of any information collected or analysed.

Detailed instructions are provided in the Telia CA operations 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 compromised 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 centers located in different cities.

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

5.8 CA or RA termination

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

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

- a. Ensure that any disruption caused by the termination of an Issuing CA is minimized as much as possible
- b. Provision of notice to parties affected by the termination, such as Subscribers Relying Parties, and Supervisory bodies and informing them of the status of the CA
- c. Make public announcement in the CA repository at least three months in advance that operations will cease for the CA

CP & CPS for Telia Server Certificates

- d. Revoke all active Certificates before the end of the three months' notice period
- e. Destroy private keys, including backup copies, in a manner such that the private keys cannot be retrieved
- f. Cease all revocation checking services relating to certificates issued using the CA keys of which use will cease. This means that all associated revocation lists are removed from their assigned locations and that no new revocation lists are issued to replace those that are removed
- g. Terminate all rights for subcontractors to act in the name of the CA which will cease to operate
- h. Ensure that all archive records of the issuing CA are retained
- i. Prior terminating the CA services - if applicable depending on the agreed contracts, Telia may transfer provision of the CA services for its existing Subscribers to another CA successor entity
- j. Notify relevant parties such as auditors, CA root programs and CCADB

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

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

The CA's issuer keys are generated in FIPS 140-2 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. The CA keys used by revocation and registration services are generated and kept secret.

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

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/ETSI 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 level 2 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 or other digitally signed package in a session secured by TLS. Where CA, RA, or end-entity 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

² FIPS PUB 140-2, Security Requirements for Cryptographic Modules,
<https://web.archive.org/web/20070825103724/http://csrc.nist.gov/cryptval/140-2.htm>

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 satisfy 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 using 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

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

Private CA keys are used for a maximum of twenty-five (25) years 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 because of development work will be first tested in a separate development system. After a successful testing the changes are taken into the test system that is like the production system. The acceptance test is performed in the test system before the changes are taken into production.

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

6.6.2 Security management controls

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

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

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

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

6.6.3 Life cycle security controls

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

6.7 Network security controls

Telia CA services are secured by two-factor authentication through VPN to protect data and systems from unauthorised personnel. Suspicious login attempts or activities will be monitored and alerted by the intrusion detection system. Industry best practices are followed for securing the CA networks, for example by conforming to the CA/B Forum Network Security Guidelines³.

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.

6.8 Timestamping

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

³ Network and Certificate System Security Requirements, <https://cabforum.org/network-security-requirements/>
Page 72

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 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 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”.

CP & CPS for Telia Server Certificates

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: <ul style="list-style-type: none"> - 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". The extension field "pathLenConstraint" defines the maximum number of CA certificates that may follow this certificate in a certification path. Root CA certificates have a "pathLenConstraint" field set to a value of "none" e.g., there is no restrictions for length subordinate CA path length. Subordinate CAs that may only issue end-user certificates have a "pathLenConstraint" set to a value of "0".	Yes
Authority information access	non-critical	This extension may contain two values: <ul style="list-style-type: none"> 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	<p>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.</p> <p>The key usage extension is optional for Telia server certificates. Purposes KeyCertSign and cRLSign are never set.</p> <p>The key usage purposes of the public keys contained in the OV and DV certificates typically include: Digital Signature, Key Encipherment. Key usage may include Data Encipherment in OV certificates.</p> <p>The key usage purposes of the public keys contained in the Seal certificates typically includes: nonRepudiation, Digital Signature</p>
Extended key usage	CA	<p>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.</p> <p>The extended key usage purposes of the public keys contained in the OV and DV certificates include: Server authentication and Client authentication</p> <p>The extended key usage purposes of the public keys contained in the Seal certificates includes:</p> <ul style="list-style-type: none"> 1.3.6.1.4.1.311.10.3.12 (Microsoft Doc. signing) 1.2.840.113583.1.1.5 (Adobe Authentic Documents Trust)

Extension	Authority	Extension description and contents
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 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".

The CRL extensions contain the following elements:

Extension	Extension description and contents
Authority Key Identifier	The identifier of the issuing CA public key is given in this extension. The identifier can be used to identify the public key that corresponds to the private key used for the signing of the certificate. SHA-1 hash algorithm is used to calculate the identifier.
CRL Number	Increasing sequence number for a given CRL scope and CRL issuer

The following entry extensions may be included in a CRL:

Extension	Extension description and contents
Serial Number	Serial number of the certificate that was revoked
Reason Code of the CRL Entry	The reason for revocation can be one of the following: KeyCompromise, CACompromise, AffiliationChanged, Superseded, CessationOfOperation
Revocation Date	Date and time when certificate was revoked

7.3 OCSP profile

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

7.3.1 Version number(s)

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

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

8.1 Frequency or circumstances of assessment

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

8.2 Identity/qualifications of assessor

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

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

8.3 Assessor's relationship to assessed entity

The Qualified Auditor should not have any financial, legal, or organisational relationship with the audited party. A person cannot be a Qualified 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
- e. is in debt to Telia or any other company referred to in a. to c. above

8.4 Topics covered by assessment

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

1. "WebTrust for CAs v2.1 or newer" AND "WebTrust for CAs SSL Baseline with Network Security v2.3 or newer"; or
2. ETSI EN 319 411-1 v1.2.2, which includes normative references to ETSI EN 319 401

(the latest version of the referenced ETSI documents should be applied); or

3. If a Government CA is required by its Certificate Policy to use a different internal audit scheme, it MAY use such scheme provided that the audit either
 - a. encompasses all requirements of one of the above schemes
 - b. consists of comparable criteria that are available for public review

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

8.5 Actions taken as a result of deficiency

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

- a. The Qualified Auditor may note the deficiency as part of the report
- b. The Qualified 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 Qualified 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 Audit Report states explicitly that it covers the relevant systems and processes used in the issuance of all Certificates that assert one or more of the policy identifiers listed in Section 7.1.6.1.

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

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

8.7 Self-audits

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

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

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Fees are defined in 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 pricelist 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 ⁴ governs the CA operations. Telia's Privacy Notice applies to all processing of personal data ⁵.

9.5 Intellectual property rights

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

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

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

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

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

be made to Telia in accordance with section 1.5.2.

9.6 Representations and warranties

9.6.1 CA representations and warranties

Telia CA 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 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 Telia CA according to the contact information of section 1.5.1.

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

9.6.4 Relying party representations and warranties

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

Prior to accepting a Subscriber's certificate, a relying party is responsible to:

- a. Verify that the certificate is appropriate for the intended use
- b. Check the validity of the certificate, i.e. verify the validity dates and the validity of the certificate and issuance signatures
- c. Check the status of the certificate against the appropriate and current CRL or OCSP Responder in accordance with the requirements stated in this CPS. As part of this verification process the digital signature of the CRL or OCSP Responder should also be validated. If certificate status can't be received due to system failure or similar, the certificates shall not be accepted.

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

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

9.6.5 Representations and warranties of other participants

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

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

9.7 Disclaimers of warranties

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

9.8 Limitations of liability

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

9.9 Indemnities

Telia CA will not pay indemnities for damages arising from the use or rejection of

certificates it issues. Subscribers shall indemnify and hold harmless the Telia and all appropriate RAs operating under the applicable CPS against all claims and settlements resulting from fraudulent information provided with the certificate application, and the use and acceptance of a certificate which violates the 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.

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

9.12.1 Procedure for amendment

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

Changes which shall take place with notification can be made to this CPS 15 days after notification. The PMT will post the notification at the CPS publishing point at the Repository. Changes affecting the terms of an agreement shall be notified in writing to the address given in the contact information of the signatory of the agreement.

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

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

9.16 Miscellaneous provisions

9.16.1 Entire agreement

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

9.16.2 Assignment

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

9.16.3 Severability

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

9.16.4 Enforcement (attorneys' fees and waiver of rights)

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

9.16.5 Force Majeure

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

9.17 Other provisions

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

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