Certificate Policy and Certification Practice Statement for Telia Server Certificates

Prepared by the Telia's Certification Authority Policy Management Team

Release: 5.9

Valid From: 2025-02-04

Classification: Public

CONTENTS

1. INTRODUCTION 16
1.1. Overview 16
1.2. Document name and identification 17
1.3. PKI participants 18
1.3.1. Certification authorities 18
1.3.2. Registration authorities 21
1.3.3. Subscribers 21
1.3.4. Relying parties 21
1.3.5. Other participants 21
1.4. Certificate usage 21
1.4.1. Appropriate certificate uses 21
1.4.2. Prohibited certificate uses 22
1.5. Policy administration 22
1.5.1. Organization administering the document 22
1.5.2. Contact person 22
1.5.3. Person determining CPS suitability for the policy 23
1.5.4. CPS approval procedures 23
1.6. Definitions and acronyms 23
1.6.1. Definitions 23
1.6.2. Acronyms 32
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 34
2.1. Repositories 34
2.1.1. CPS Repository 34
2.1.2. Revocation Information Repository 34
2.1.3. Certificate Repository 34
2.2. Publication of certification information 34
2.3. Time or frequency of publication 35
2.4. Access controls on repositories 35
3. IDENTIFICATION AND AUTHENTICATION 36
3.1. Naming 36
3.1.1. Types of names 36

3.1.2. Need for names to be meaningful 38
3.1.3. Anonymity or pseudonymity of Subscribers 38
3.1.4. Rules for interpreting various name forms 38
3.1.5. Uniqueness of names 38
3.1.6. Recognition, authentication, and role of trademarks 38
3.2. Initial identity validation 38
3.2.1. Method to prove possession of private key 38
3.2.2. Authentication of Organization and Domain Identity 38
3.2.3. Authentication of individual identity 44
3.2.4. Non-verified Subscriber information 44
3.2.5. Validation of authority 45
3.2.6. Criteria for interoperation 45
3.3. Identification and authentication for re-key requests 45
3.3.1. Identification and authentication for routine re-key 45
3.3.2. Identification and authentication for re-key after revocation 46
3.4. Identification and authentication for revocation request 46
3.4.1. Revocation by Subscriber 46
3.4.2. Revocation by the Revocation Service of the CA 46
3.4.3. Revocation of CAs 46
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 47
4.1. Certificate Application 47
4.1.1. Who can submit a certificate application 47
4.1.2. Enrolment process and responsibilities 47
4.2. Certificate application processing 48
4.2.1. Performing identification and authentication functions 48
4.2.2. Approval or rejection of certificate applications 48
4.2.3. Time to process certificate applications 48
4.2.4. Certificate Authority Authorization (CAA) 49
4.3. Certificate issuance 50
4.3.1. CA actions during certificate issuance 50
4.3.2. Notification to Subscriber by the CA of issuance of certificate 50
4.4. Certificate acceptance 50
4.4.1. Conduct constituting certificate acceptance 51
4.4.2. Publication of the certificate by the CA 51

4.4.3. Notification of certificate issuance by the CA to other entities 51
4.5. Key pair and certificate usage 51
4.5.1. Subscriber private key and certificate usage 51
4.5.2. Relying party public key and certificate usage 51
4.6. Certificate renewal 51
4.6.1. Circumstance for certificate renewal 51
4.6.2. Who may request renewal 52
4.6.3. Processing certificate renewal requests 52
4.6.4. Notification of new certificate issuance to Subscriber 52
4.6.5. Conduct constituting acceptance of a renewal certificate 52
4.6.6. Publication of the renewal certificate by the CA 52
4.6.7. Notification of certificate issuance by the CA to other entities 52
4.7. Certificate re-key 52
4.7.1. Circumstance for certificate re-key 52
4.7.2. Who may request certification of a new public key 53
4.7.3. Processing certificate re-keying requests 53
4.7.4. Notification of new certificate issuance to subscriber 53
4.7.5. Conduct constituting acceptance of a re-keyed certificate 53
4.7.6. Publication of the re-keyed certificate by the CA 53
4.7.7. Notification of certificate issuance by the CA to other entities 53
4.8. Certificate modification 53
4.8.1. Circumstance for certificate modification 53
4.8.2. Who may request certificate modification 53
4.8.3. Processing certificate modification requests 54
4.8.4. Notification of new certificate issuance to subscriber 54
4.8.5. Conduct constituting acceptance of modified certificate 54
4.8.6. Publication of the modified certificate by the CA 54
4.8.7. Notification of certificate issuance by the CA to other entities 54
4.9. Certificate revocation and suspension 54
4.9.1. Circumstances for revocation 54
4.9.2. Who can request revocation 55
4.9.3. Procedure for revocation request 56
4.9.4. Revocation request grace period 58
4.9.5. Time within which CA must process the revocation request 59

4.9.6. Revocation checking requirement for relying parties 59
4.9.7. CRL issuance frequency 59
4.9.8. Maximum latency for CRLs 59
4.9.9. On-line revocation/status checking availability 59
4.9.10. On-line revocation checking requirements 59
4.9.11. Other forms of revocation advertisements available 61
4.9.12. Special requirements regarding key compromise 61
4.9.13. Circumstances for suspension 61
4.9.14. Who can request suspension 61
4.9.15. Procedure for suspension request 61
4.9.16. Limits on suspension period 61
4.10. Certificate status services 61
4.10.1. Operational characteristics 61
4.10.2. Service availability 61
4.10.3. Optional features 61
4.11. End of subscription 61
4.12. Key escrow and recovery 62
4.12.1. Key escrow and recovery policy and practices 62
4.12.2. Session key encapsulation and recovery policy and practices 62
5. FACILITIES, MANAGEMENT, AND OPERATIONAL CONTROLS 63
5.1. Physical controls 64
5.1.1. Site location and construction 64
5.1.2. Physical access 64
5.1.3. Power and air conditioning 65
5.1.4. Water exposures 65
5.1.5. Fire prevention and protection 65
5.1.6. Media storage 65
5.1.7. Waste disposal 66
5.1.8. Off-site backup 66
5.2. Procedural controls 66
5.2.1. Trusted roles 66
5.2.2. Number of persons required per task 67
5.2.3. Identification and authentication for each role 68
5.2.4. Roles requiring separation of duties 69

5.3. Personnel controls 69
5.3.1. Qualifications, experience, and clearance requirements 69
5.3.2. Background check procedures 69
5.3.3. Training requirements 70
5.3.4. Retraining frequency and requirements 71
5.3.5. Job rotation frequency and sequence 71
5.3.6. Sanctions for unauthorised actions 71
5.3.7. Independent contractor requirements 71
5.3.8. Documentation supplied to personnel 71
5.4. Audit logging procedures 71
5.4.1. Types of events recorded 71
5.4.2. Frequency of processing log 72
5.4.3. Retention period for audit log 73
5.4.4. Protection of audit log 73
5.4.5. Audit log backup procedures 73
5.4.6. Audit collection system (internal vs. external) 73
5.4.7. Notification to event-causing subject 73
5.4.8. Vulnerability assessments 73
5.5. Records archival 73
5.5.1. Types of records archived 73
5.5.2. Retention period for archive 74
5.5.3. Protection of archive 74
5.5.4. Archive backup procedures 75
5.5.5. Requirements for timestamping of records 75
5.5.6. Archive collection system (internal or external) 75
5.5.7. Procedures to obtain and verify archive information 75
5.6. Key changeover 75
5.6.1. Self-Signed CA 75
5.6.2. CA Hierarchies 75
5.7. Compromise and disaster recovery 76
5.7.1. Incident and compromise handling procedures 76
5.7.2. Computing resources, software, and/or data are corrupted 76
5.7.3. Entity private key compromise procedures 76
5.7.4. Business continuity capabilities after a disaster 77

5.8. CA or RA termination 77
6. TECHNICAL SECURITY CONTROLS 79
6.1. Key pair generation and installation 79
6.1.1. Key pair generation 79
6.1.2. Private key delivery to Subscriber 79
6.1.3. Public key delivery to certificate issuer 79
6.1.4. CA public key delivery to relying parties 80
6.1.5. Key sizes 80
6.1.6. Public key parameters generation and quality checking 80
6.1.7. Key usage purposes (as per X.509 v3 key usage field) 81
6.2. Private key protection and cryptographic module engineering controls 81
6.2.1. Cryptographic module standards and controls 81
6.2.2. Private key (n out of m) multi-person control 81
6.2.3. Private key escrow 82
6.2.4. Private key backup 82
6.2.5. Private key archival 82
6.2.6. Private key transfer into or from a cryptographic module 82
6.2.7. Private key storage on cryptographic module 82
6.2.8. Method of activating private key 82
6.2.9. Method of deactivating private key 83
6.2.10. Method of destroying private key 83
6.2.11. Cryptographic module rating 84
6.3. Other aspects of key pair management 84
6.3.1. Public key archival 84
6.3.2. Certificate operational periods and key pair usage periods 84
6.4. Activation data 85
6.4.1. Activation data generation and installation 85
6.4.2. Activation data protection 85
6.4.3. Other aspects of activation data 86
6.5. Computer security controls 86
6.5.1. Specific computer security technical requirements 86
6.5.2. Computer security rating 86
6.6. Life cycle security controls 86
6.6.1. System development controls 86

6.6.2. Security management controls 86
6.6.3. Life cycle security controls 87
6.7. Network security controls 87
6.8. Timestamping 87
7. **CERTIFICATE, CRL, AND OCSP PROFILE** 88
7.1. Certificate profile 88
7.1.1. Version number(s) 88
7.1.2. Certificate extensions 88
7.1.3. Algorithm object identifiers 92
7.1.4. Name forms 92
7.1.5. Name constraints 92
7.1.6. Certificate policy object identifier 92
7.1.7. Usage of Policy Constraints extension 92
7.1.8. Policy qualifiers syntax and semantics 92
7.1.9. Processing semantics for the critical Certificate Policies extension 93
7.2. CRL profile 93
7.2.1. Version number(s) 93
7.2.2. CRL and CRL entry extensions 93
7.3. OCSP profile 93
7.3.1. Version number(s) 93
7.3.2. OCSP extensions 93
8. **COMPLIANCE AUDIT AND OTHER ASSESSMENTS** 94
8.1. Frequency or circumstances of assessment 94
8.2. Identity/qualifications of assessor 94
8.3. Assessor's relationship to assessed entity 94
8.4. Topics covered by assessment 94
8.5. Actions taken as a result of deficiency 95
8.6. Communication of results 95
8.7. Self-audits 95
9. OTHER BUSINESS AND LEGAL MATTERS 97
9.1. Fees 97
9.1.1. Certificate issuance or renewal fees 97
9.1.2. Certificate access fees 97
9.1.3. Revocation or status information access fees 97

9.1.4. Fees for other services 97
9.1.5. Refund policy 97
9.2. Financial responsibility 97
9.2.1. Insurance coverage 97
9.2.2. Other assets 97
9.2.3. Insurance or warranty coverage for end-entities 97
9.3. Confidentiality of business information 97
9.3.1. Scope of confidential information 97
9.3.2. Information not within the scope of confidential information 98
9.3.3. Responsibility to protect confidential information 98
9.4. Privacy of personal information 98
9.5. Intellectual property rights 98
9.6. Representations and warranties 99
9.6.1. CA representations and warranties 99
9.6.2. RA representations and warranties 99
9.6.3. Subscriber representations and warranties 99
9.6.4. Relying party representations and warranties 100
9.6.5. Representations and warranties of other participants 100
9.7. Disclaimers of warranties 100
9.8. Limitations of liability 101
9.9. Indemnities 101
9.10. Term and termination 101
9.10.1. Term 101
9.10.2. Termination 101
9.10.3. Effect of termination and survival 101
9.11. Individual notices and communications with participants 101
9.12. Amendments 101
9.12.1. Procedure for amendment 102
9.12.2. Notification mechanism and period 102
9.12.3. Circumstances under which OID must be changed 102
9.13. Dispute resolution provisions 102
9.14. Governing law 102
9.15. Compliance with applicable law 102
9.16. Miscellaneous provisions 102

9.16.1. Entire agreement 102
9.16.2. Assignment 102
9.16.3. Severability 103
9.16.4. Enforcement (attorneys' fees and waiver of rights) 103
9.16.5. Force Majeure 103
9.17. Other provisions 103

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

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 organization identity and/or domain name, 4.9 Certificate revocation and suspension, 4.9.1 Circumstances for revocation, 4.9.3 Procedure for revocation request, 4.10.1 Operational characteristics, 6.1.1 Key pair generation, 6.3.2 Certificate operational periods and key pair usage periods, 7.1 Certificate profile, 7.1.2 Certificate extensions, 7.1.3 Algorithm object identifiers, 7.1.5 Name constraints, 7.2 CRL profile, 7.3 OCSP profile	Telia CA Policy Management Team

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

Version	Date	Change	Author
4.6	2022-06-07	As per [ETSI 319 401] REQ 6.3-9 and -10 “Information security policy; The maximum interval between two checks shall be documented in the trust service practice statement” Disclosure of maximum interval added to the section 9.12 Problem reporting contact information added to the section 1.5.2	Telia CA Policy Management Team
4.7	2022-09-15	Telia Sans font type face changed through the document to reflect Telia’s corporate document format policy. In sections 4.4.3 and 4.6.7 language clarified to express intended purpose 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 Wording changed in sections 1.1, 4.2.5 and 4.4.1 to clarify the meaning of information presented.	Telia CA Policy Management Team
4.8	2022-12-14	In section 1.5.4 disclosed PMT's CPS review policy In section 3.2.5 for OV removed obsoleted “cerficate based login option”	Telia CA Policy Management Team
4.9	2023-03-21	Annual review of the CPS by Telia CA Policy Management Team Changes identified by PMT’s annual CP/CPS review in various sections of this CP/CPS	Telia CA Policy Management Team
5.0	2023-06-13	CP/CPS updates after PMT review of Telia CA’s annual self-assessment to improve information provided in CP/CPS and to give explicit statements of current practice. Detailed list of changes recorded by PMT in its meeting minutes.	Telia CA Policy Management Team
5.1	2023-10-23	Telia CA Policy Management Team review and verification of compliance to upcoming 2.0.2 version of TLS BR and recommended non-normative changes introduced in the SC-066 Ballot (clean-up). Minor typographic changes made, consistency in the certificate field and profile definitions improved. No normative and/or policy changes in this version.	Telia CA Policy Management Team

Version	Date	Change	Author
5.2	2023-11-22	Telia Root v3 hierarchy TLS root CAs added to the CP/CPS (self-signed and cross-signed intermediate CAs).	Telia CA Policy Management Team
5.3	2024-01-18	Accepted RSA key lengths restriction to allow only 2048, 3072, 4096 and 8192 for key size. New CP/CPS to be put on public review and effective 5.2.2024.	Telia CA Policy Management Team
5.4	2024-03-06	Telia CA Policy Management Team annual review of the CP/CPS performed. Section 4.2.4 (CAA) changed to indicate support for RFC 8657. Section 8.4 updated for ETSI references. CA certificate disclosure practice / CCADB updated. Section 4.1.1.2 minor update.	Telia CA Policy Management Team
5.5	2024-04-12	CP/CPS update, new root hierarchy update, subordinate CAs. Changes identified in annual review by PMT incorporated to this version.	Telia CA Policy Management Team
5.6	2024-05-30	Removal of Document signing CA and related practices from TLS CP/CPS as the Document signing CA is not governed by CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates	Telia CA Policy Management Team
5.7	2024-09-18	Updates to the sections 4.7 (Certificate re-key) and 4.8 (Certificate modification) and updates to Definitions and Acronyms tables. Removed terminated CA Telia Domain Validation CA v2 from the CP/CPS	Telia CA Policy Management Team
5.8	2024-10-22	Updated practice for DVC methods 3.2.2.4.13 Email to DNS CAA Contact 3.2.2.4.14 Email to DNS TXT Contact	Telia CA Policy Management Team
5.9	2025-01-15	Conforming to SC-083v3: Winter 2024-2025 Cleanup Ballot, CA commitment statement to CA/B TLS requirements, URL changed to https from http. Certificate SHA2 fingerprints updated for resigned CA certificates and cross-certificates of the new Root hierarchy. Certificate Problem Reporting details added.	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 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.

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

This CPS conforms to the IETF PKIX Internet X.509 Public Key Infrastructure CP and CPS Framework (RFC 3647).

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

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 organization 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.

This CP/CPS governs certificates of type (a and (b.

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

This CPS is also a CP for Telia OV and DV 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
• TeliaSonera Root CA v1 • Telia Root CA v2	Root CA	
• Telia RSA TLS Root CA v3 • Telia EC TLS Root CA v3	Root CA	
• Telia RSA TLS Root CA v3 • Telia EC TLS Root CA v3	Cross-Certified Subordinate CA	2.5.29.32.0

CA	Type	CP OIDs
• TeliaSonera Server CA v2 • Telia Server CA v3	TLS OV certificates	2.23.140.1.2.2
• Telia RSA OV CA v4	TLS OV certificates	2.5.29.32.0 (CA certificates) 2.23.140.1.2.2 1.3.6.1.4.1.271.2.3.1.1.15
• Telia Domain Validation CA v3	TLS DV certificates	2.23.140.1.2.1
• Telia RSA DV CA v4 • Telia EC DV CA v4	TLS DV certificates	2.5.29.32.0 (CA certificates) 2.23.140.1.2.1 1.3.6.1.4.1.271.2.3.1.1.16

1.3. PKI participants

Telia Root CAs (TeliaSonera Root CA v1, Telia Root CA v2, Telia RSA TLS Root CA v3 and Telia EC TLS Root CA v3) issue Subordinate CA certificates to Telia and Subscribers hosting their CA at Telia. NOTE, Telia RSA TLS Root CA v3 and Telia EC TLS Root CA v3 are NOT yet included in any root program providing public trust in the global PKI domain. Telia CA SHALL make required inclusion requests to TLS root programs before end of 2024.

Telia 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 organizations shall undertake what is stated in this CP/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. Telia Root CA v2 self-signed certificate and cross-certified Telia Root CA v2 - subordinate certificate have the same key pair and subject. Clients can use either one when doing PKI path validation.

Figure 2 presents the new generation (v3) TLS dedicated hierarchy of, self-signed Root CAs Telia RSA TLS Root CA v3 and Telia EC TLS Root CA v3. Both new Root CAs have been cross-certified by Telia Root CA v2. Telia RSA TLS Root CA v3 root CA certificate and cross-certified Telia RSA TLS Root CA v3 subordinate certificate have the same key pair and subject. Telia EC TLS Root CA v3 root CA certificate and cross-certified Telia EC TLS Root CA v3 subordinate certificate have the same key pair and subject. Clients can use either one when doing PKI path validation.

In the hierarchy of subordinate CAs up to root CAs (see Figures 1 and 2), the Telia CA is responsible for ensuring the subordinate-CAs comply with the applicable policy requirements.

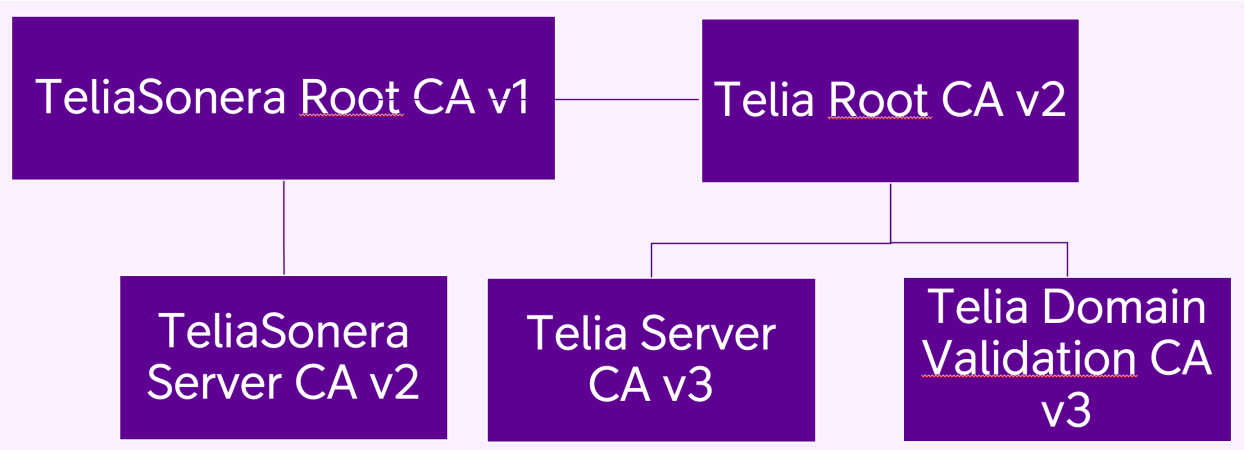

Figure 1, Telia Server Certificate PKI Hierarchy

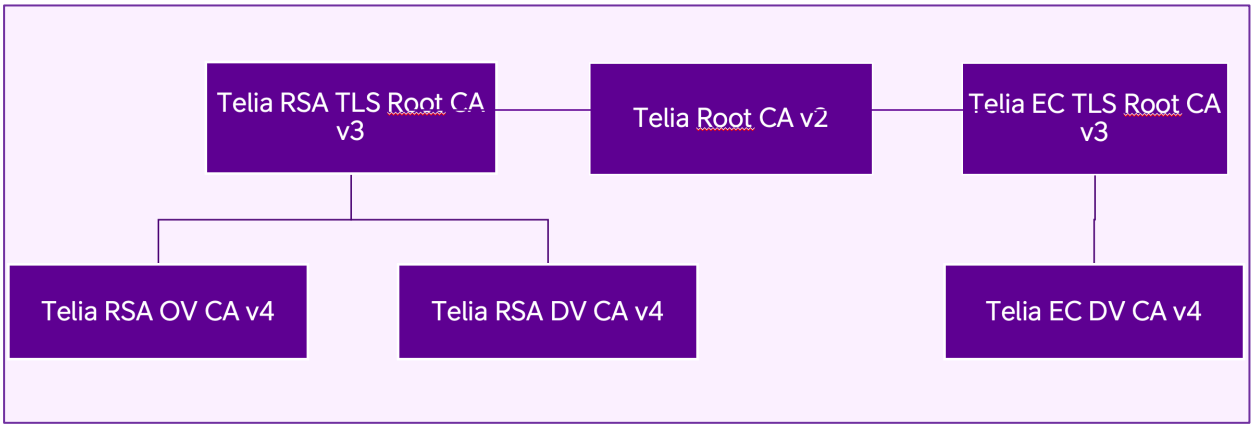

Figure 2, Telia Server Certificate PKI Hierarchy

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.

Root CAs

- **TeliaSonera Root CA v1**
  SHA2 Fingerprint:
  DD6936FE21F8F077C123A1A521C12224F72255B73E03A7260693E8A24B0FA389
- **Telia Root CA v2**
  SHA2 Fingerprint:
  242B69742FCB1E5B2ABF98898B94572187544E5B4D9911786573621F6A74B82C
- **Telia RSA TLS Root CA v3**
  SHA2 Fingerprint:
  D13DB1294C45EBC6FC86C6BBF69FA29BDFE692DFF7C713C243C7A956C6A2284C
- **Telia EC TLS Root CA v3**
  SHA2 Fingerprint:
  098E08A91DBBF77478B96CCEB89B1413A5DA37B7C862606A955DEB07179F4326

Cross-Certified Subordinate CAs

- **Telia Root CA v2**
  SHA2 Fingerprint:
  EF6F29F636F62BDD4753122F41F3419EE7C2877587BE4A9807ADF58946458E7F
- **Telia RSA TLS Root CA v3**
  SHA2 Fingerprint:
  5573DFB5C894B95B85D26F9C57591257561A09CD37726D13835ECAC28A1E9C7C
- **Telia EC TLS Root CA v3**
  SHA2 Fingerprint:
  70F84634C3246A43E9722CB1E0ABC5BB9BCA62FFFB70EB7EA73F4BB706C853C1

Subordinate CA's

- **TeliaSonera Server CA v2**
  SHA2 Fingerprint:
  D721110388CA6F20BBA9FD1A8DBA4EFB8C16392A3DEBAD97C553EEAF0ACACAAC
- **Telia Server CA v3**
  SHA2 Fingerprint:
  1281AD8FABE883F209E9636448D1A80C373DAA7686C813A270FAD48F5F5E589A
- **Telia Domain Validation CA v3**
  SHA2 Fingerprint:
  A7E83056E9B3D9DDB1816B95518F6A5E5A1DFDFA28F60533B1C850855EAA4263
- **Telia RSA OV CA v4**
  SHA2 Fingerprint:
  DCC4EA67E1B46C2D00745046F3FBF3115A4E819B92AEE7B92A0F8DBA0796CF9A
- **Telia RSA DV CA v4**
  SHA2 Fingerprint:
  BF062E12C8BBF2E6685831FE000CAF67342E225A8A249187CC3953B38D40DE04
- **Telia EC DV CA v4**
  SHA2 Fingerprint:
  69E4AA2C42958ADABC4B171A41C2D9E7B2EB7C91772FBD4B5EFB1C845CD52FAF

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 the Subscriber may only be a legal entity (e.g. an organization).

1.3.4. Relying parties

A Relying Party may be either a Subscriber of any Telia CA or any other organization, 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
- Cross-certifier Subordinate CAs to provide interoperability across Root CA hierarchies.
- TLS certificates: used to implement the TLS protocol on one or more servers

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

CA	Appropriate usage
TeliaSonera Root CA v1 Telia Root CA v2	CAs issue certificates for subCAs.
Telia RSA TLS Root CA v3 Telia EC TLS Root CA v3	CAs to issue TLS subordinate CAs for v3 hierarchy
Telia RSA TLS Root CA v3 Telia EC TLS Root CA v3	Cross-certified subordinate CAs to allow interoperability across Root v2 and Root v3 hierarchies for TLS subscriber certificates.

TeliaSonera Server CA v2 Telia Server CA v3 Telia RSA OV CA v4	These certificates are used for TLS (OV) communication where the risks of data compromise are moderate or high.
Telia Domain Validation CA v3 Telia RSA DV CA v4 Telia EC DV CA v4	These certificates are used for TLS (DV) communication where the risks of data compromise are low.

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. Organization administering the document

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

Contact information:

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

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

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.

NOTE, to ensure that problem reports are duly received and processed, Telia CA does NOT accept attachment in the problem report emails. Should the reported case require exchange of additional materials that cannot be included in the email text the reporter MUST inform Telia CA in the initial report. Telia CA SHALL instruct reporter of the means to deliver such information when responding to the initial report.

Problem reporting instructions, please see:
https://support.trust.telia.com/palvelinvarmenneturvallisuus_en.html

1.5.3. Person determining CPS suitability for the policy

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

1.5.4. CPS approval procedures

The PMT will review any modifications, additions or deletions from this CPS and determine if modifications, additions, or deletions are acceptable and do not jeopardize operations or the security of the production environment.

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

1.6. Definitions and acronyms

1.6.1. Definitions

Affiliate	A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.
Agent	A person, contractor, service provider that is providing a service to an organization under contract and are subject to the same corporate policies as if they were an employee of the organization.
Applicant	The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate is issued, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.

Applicant Representative	A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant who signs and submits, or approves a certificate request on behalf of the Applicant, and/or who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.
Application Software Supplier	A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.
Attestation Letter	A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.
Audit Period	In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA.) The coverage rules and maximum length of audit periods are defined in Section 8.1.
Audit Report	A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.
Authorization Domain Name	The FQDN used to obtain authorization for a given FQDN to be included in a Certificate. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If a Wildcard Domain Name is to be included in a Certificate, then the CA MUST remove "*." from the left-most portion of the Wildcard Domain Name to yield the corresponding FQDN. The CA may prune zero or more Domain Labels of the FQDN from left to right until encountering a Base Domain Name and may use any one of the values that were yielded by pruning (including the Base Domain Name itself) for the purpose of domain validation.
Authorized Ports	One of the following ports 80 (http), 443 (https), 25 (smtp), 22 (ssh).
Baseline Requirements	Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates
Base Domain Name	The portion of an applied-for FQDN that is the first Domain Name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most Domain Name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.
CAA	From RFC 8659 (http: //tools.ietf.org/html/rfc8659) "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify one or more Certification Authorities (CAs) authorized to issue certificates for that domain name. CAA Resource Records allow a public CA to implement additional controls to reduce the risk of unintended certificate mis-issue."
CA Certificate	Certificate which certifies that a particular public key is the public key for a specific CA.

CA Key	Key pair where the private key is used by the CA in order to sign certificates and where the public key is used to verify the same certificate.
CA Key Pair	A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s).
Certificate	An electronic document that uses a digital signature to bind a public key and an identity.
Certificate Authority / 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.
Certification Chain	An ordered list of Certificates containing a Subscriber Certificate and CA Certificates, which terminates in a root Certificate.
Certificate Data	Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.
Certificate Management Process	Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.
Certificate Policy	A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.
Certificate Problem Report	Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.
Certificate Profile	A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7, e.g. a Section in a CA's CPS or a certificate template file used by CA software.
Certificate Request	A process where a natural person (the Subscriber or someone employed by the Subscriber) or an authorised agent with the authority of representing the Subscriber that completes and submits a certificate request.
Certificate Revocation List	A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.
Certification Authority	An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Root CAs and Subordinate CAs.
Certification Practice Statement	One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.
Client Certificate	A digital certificate in which information about the organization and email of holding the certificate has been validated by Telia.
Control	"Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors ; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.

Country	Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.
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.
Cross-Certified Subordinate CA Certificate	A certificate that is used to establish a trust relationship between two CAs.
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.
CSPRNG	A random number generator intended for use in a cryptographic system.
Delegated Third Party	A natural person or Legal Entity that is not the CA but is authorized by the CA, and whose activities are not within the scope of the appropriate CA audits, to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.
Digital Signature	A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents.
Distinguished Name (DN)	It is a unique entry identifier throughout the complete directory. No two entries can have the same DN within the same directory. A DN is used in certificates to uniquely identify a certificate-owner.
DNS CAA Email Contact	The email address defined in Appendix A.1.1 of the TLS BR.
DNS CAA Phone Contact	The phone number defined in Appendix A.1.2 of the TLS BR.
DNS TXT Record Email Contact	The email address defined in Appendix A.2.1 of the TLS BR.
DNS TXT Record Phone Contact	The phone number defined in Appendix A.2.2 of the TLS BR.
Document Signing (Seal) Certificate	Used for authenticating documents from Adobe PDF (AATL), Microsoft Office, OpenOffice, and LibreOffice.
Domain Contact	The Domain Name Registrant, technical contact, or administrative contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.
Domain Label	From RFC 8499 (http://tools.ietf.org/html/rfc8499) “An ordered list of zero or more octets that makes up a portion of a domain name. Using graph theory, a label identifies one node in a portion of the graph of all possible domain names.”

Domain Name	An ordered list of one or more Domain Labels assigned to a node in the Domain Name System.
Domain Namespace	The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.
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 the Internet Corporation for Assigned Names and Numbers (ICANN), a national Domain Name authority/registry, or a Network Information Center (including their affiliates, contractors, delegates, successors, or assignees).
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 organization unaffiliated with the CA who authorizes issuance of Certificates to that organization.
Expiry Date	The "Not After" date in a Certificate that defines the end of a Certificate's validity period.
Fully-Qualified Domain Name	A Domain Name that includes the Domain Labels of all superior nodes in the Internet Domain Name System.
Government Entity	A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).
High Risk Certificate Request	A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.
Internal Name	A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database.
IP Address	A 32-bit or 128-bit number assigned to a device that uses the Internet Protocol for communication.
IP Address	The person(s) or entity(ies) registered with an IP Address Registration

Contact	Authority as having the right to control how one or more IP Addresses are used.
IP Address Registration Authority	The Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC).
Issuing CA	In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.
Key Compromise	A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, or an unauthorized person has had access to it.
Key Generation Script	A documented plan of procedures for the generation of a CA Key Pair.
Key Pair	The Private Key and its associated Public Key.
LDH Label	From RFC 5890 (http: //tools.ietf.org/html/rfc5890) "A string consisting of ASCII letters, digits, and the hyphen with the further restriction that the hyphen cannot appear at the beginning or end of the string. Like all DNS labels, its total length must not exceed 63 octets."
Legal Entity	An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.
Linting	A process in which the content of digitally signed data such as a Precertificate [RFC 6962], Certificate, Certificate Revocation List, or OCSP response, or data-to-be-signed object such as a tbsCertificate (as described in RFC 5280, Section 4.1.1.1) is checked for conformance with the profiles and requirements defined in these Requirements.
Multi-Perspective Issuance Corroboration	A process by which the determinations made during domain validation and CAA checking by the Primary Network Perspective are corroborated by other Network Perspectives before Certificate issuance.
Network Perspective	Related to Multi-Perspective Issuance Corroboration. A system (e.g., a cloud-hosted server instance) or collection of network components (e.g., a VPN and corresponding infrastructure) for sending outbound Internet traffic associated with a domain control validation method and/or CAA check. The location of a Network Perspective is determined by the point where unencapsulated outbound Internet traffic is typically first handed off to the network infrastructure providing Internet connectivity to that perspective.
Non-Reserved LDH Label	From RFC 5890 (http: //tools.ietf.org/html/rfc5890) "The set of valid LDH labels that do not have '--' in the third and fourth positions."
Object Identifier	A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object 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.
Onion Domain Name	A Fully Qualified Domain Name ending with the RFC 7686 ".onion" Special-Use Domain Name. For example, 2gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkiu3zzui5du4xyclen53wid.onion is an

	Onion Domain Name, whereas torproject.org is not an Onion Domain Name.
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.
Parent Company	A company that Controls a Subsidiary Company.
Pending Prohibition	The use of a behavior described with this label is highly discouraged, as it is planned to be deprecated and will likely be designated as MUST NOT in the future.
Primary Network Perspective	The Network Perspective used by the CA to make the determination of 1) the CA's authority to issue a Certificate for the requested domain(s) or IP address(es) and 2) the Applicant's authority and/or domain authorization or control of the requested domain(s) or IP address(es).
Private Key	The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
Public Key	The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
Public Key Infrastructure	A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.
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.
P-Label	A XN-Label that contains valid output of the Punycode algorithm (as defined in RFC 3492, Section 6.3) from the fifth and subsequent positions.
Qualified Auditor	A natural person or Legal Entity that meets the requirements of Section 8.2.
Random Value	A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.
Registered Domain Name	A Domain Name that has been registered with a Domain Name Registrar.
Registration Authority (RA)	Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of 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	An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and

Data Source	governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.
Reliable Method of Communication	A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.
Relying Party	Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.
Repository	An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.
Request Token	A value, derived in a method specified by the CA which binds this demonstration of control to the certificate request. The CA SHOULD define within its CPS (or a document clearly referenced by the CPS) the format and method of Request Tokens it accepts. The Request Token SHALL incorporate the key used in the certificate request. A Request Token MAY include a timestamp to indicate when it was created. A Request Token MAY include other information to ensure its uniqueness. A Request Token that includes a timestamp SHALL remain valid for no more than 30 days from the time of creation. A Request Token that includes a timestamp SHALL be treated as invalid if its timestamp is in the future. A Request Token that does not include a timestamp is valid for a single use and the CA SHALL NOT re-use it for a subsequent validation. The binding SHALL use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request. **Note** Examples of Request Tokens include, but are not limited to a hash of the public key; or a hash of the Subject Public Key Info [X.509]; or a hash of a PKCS#10 CSR. A Request Token may also be concatenated with a timestamp or other data. If a CA wanted to always use a hash of a PKCS#10 CSR as a Request Token and did not want to incorporate a timestamp and did want to allow certificate key re-use then the applicant might use the challenge password in the creation of a CSR with OpenSSL to ensure uniqueness even if the subject and key are identical between subsequent requests. **Note** This simplistic shell command produces a Request Token which has a timestamp and a hash of a CSR. echo `date -u +%Y%m%d%H%M` `sha256sum <r2.csr` | sed "s/[-]//g" The script outputs 201602251811c9c863405fe7675a3988b97664ea6baf442019e4e52fa335f406f7c5f26cf14f
Required Website Content	Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA.

Requirements	The Baseline Requirements found in this document.
Reserved IP Address	An IPv4 or IPv6 address that is contained in the address block of any entry in either of the following IANA registries https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml
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.
Root CA	The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.
Root Certificate	The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.
Short-lived Subscriber Certificate	For Certificates issued on or after 15 March 2024 and prior to 15 March 2026, a Subscriber Certificate with a Validity Period less than or equal to 10 days (864,000 seconds). For Certificates issued on or after 15 March 2026, a Subscriber Certificate with a Validity Period less than or equal to 7 days (604,800 seconds).
Sovereign State	A state or country that administers its own government, and is not dependent upon, or subject to, another power.
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 natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.
Subscriber Agreement	An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.
Subsidiary Company	A company that is controlled by a Parent Company.
Technically Constrained Subordinate CA Certificate	A Subordinate CA certificate which uses a combination of Extended Key Usage and/or Name Constraint extensions, as defined within the relevant Certificate Profiles of this document, to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.
Terms of Use	Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA or is the CA.
Test Certificate	This term is no longer used in TLS Baseline Requirements.

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.
Validation Specialist	Someone who performs the information verification duties specified by these Requirements.
Validity Period	From RFC 5280 (https://datatracker.ietf.org/doc/html/rfc5280) "The period of time from notBefore through notAfter, inclusive."
WHOIS	Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.
Wildcard Certificate	A Certificate containing at least one Wildcard Domain Name in the Subject Alternative Names in the Certificate.
Wildcard Domain Name	A string starting with "*." (U+002A ASTERISK, U+002E FULL STOP) immediately followed by a Fully-Qualified Domain Name.
XN-Label	From RFC 5890 (http: //tools.ietf.org/html/rfc5890) "The class of labels that begin with the prefix "xn--" (case independent), but otherwise conform to the rules for LDH labels."

1.6.2. Acronyms

Acronym	Meaning
AATL	Adobe Approved Trust List
BR	Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DER	Distinguished Encoding Rules
DN	Distinguished Name
DSA	Digital Signature Algorithm
DV	Domain Validation
ETSI	European Telecommunications Standards Institute

Acronym	Meaning
FIPS	Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
OCSP	On-line Certificate Status Protocol
OID	Object Identifier
PDF	Portable Document Format
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509 (IETF Working Group)
PMT	Policy Management Team
RA	Registration Authority
RFC	Request for Comments
RSA	Rivest-Shamir-Adleman asymmetric encryption algorithm
S/MIME	Secure Multipurpose Internet Mail Extension
SHA	Secure Hash Algorithm
TLS	Transport Layer Security
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VPN	Virtua Private Network

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

2.1.1. CPS Repository

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

2.1.2. Revocation Information Repository

Following CRLs are published 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
Telia RSA TLS Root CA v3	http://httpcrl.trust.telia.com/teliarsatlsrootcav3.crl
Telia EC TLS Root CA v3	http://httpcrl.trust.telia.com/teliaectlsrootcav3.crl
TeliaSonera Server CA v2	http://httpcrl.trust.telia.com/teliasoneraservercav2.crl
Telia Server CA v3	http://httpcrl.trust.telia.com/teliaservercav3.crl
Telia RSA OV CA v4	http://httpcrl.trust.telia.com/teliarsaovcav4.crl
Telia Domain Validation CA v3	http://httpcrl.trust.telia.com/teliadomainvalidationcav3.crl
Telia RSA DV CA v4	http://httpcrl.trust.telia.com/teliarsadvcav4.crl
Telia EC DV CA v4	http://httpcrl.trust.telia.com/teliaecdvcav4.crl

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

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

2.4. Access controls on repositories

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

3. 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:

Root CA	commonName, CN (OID 2.5.4.3)	organizationName (O, 2.5.4.10)	countryName (C, OID 2.5.4.6)
TeliaSonera Root CA v1	TeliaSonera Root CA v1	Telia	
Telia Root CA v2	Telia Root CA v2	Telia Finland Oyj	FI
Telia RSA TLS Root CA v3	Telia RSA TLS Root CA v3	Telia Company AB	SE
Telia EC TLS Root CA v3	Telia EC TLS Root CA v3	Telia Company AB	SE

Cross-certified Subordinate CAs for interoperability purposes have the exact same Subject information as the corresponding Self-signed Root CA.

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 organization. The name is either Telia Company AB, Telia Finland Oyj or TeliaSonera
countryName (C, OID 2.5.4.6)	Country where the CA organization 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
commonName (CN, OID 2.5.4.3)	A single host domain name (FQDN) or IP address which is owned or controlled by the Subject and to be associated with the Subject's server. Such server MAY be owned and operated by the Subject or another entity (e.g., a hosting service). The CN value is always one of the values contained in the Certificate's subjectAltName extension.	A single host domain name (FQDN) which is owned or controlled by the Subject and to be associated with the Subject's server. Such server MAY be owned and operated by the Subject or another entity (e.g., a hosting service). The CN value is always one of the values contained in the Certificate's subjectAltName extension.

Attribute	Description – OV TLS	Description – DV TLS
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
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
countryName (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
subjectAltName (OID: 2.5.29.17): 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.
subjectAltName (OID: 2.5.29.17): 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).
jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)	Optional in OV certificates.	Not allowed
businessCategory (OID: 2.5.4.15)	Optional in OV certificates.	Not allowed
serialNumber (OID: 2.5.4.5)	Optional in OV certificates.	Not allowed

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

Attribute	Description – OV TLS
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 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 organizations. However, the CA may issue several certificates to the same organization, 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 Organization and Domain Identity

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.

Telia CA issued certificates will not contain metadata such as '.', '-', and ' ' (whitespace) 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 ("_").

3.2.2.1. Identity

In case of OV, Telia CA verifies the organization name (O) of a new Subscriber by checking the existence of the company, its legal name, business identity code and other relevant organization 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 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.

3.2.2.2. DBA/Tradename

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).

Same authentication practice is applied for DBA/Tradename as for Identity (3.2.2.1).

3.2.2.3. Verification of Country

Same authentication practice is applied for Country as for Identity (3.2.2.1).

3.2.2.4. Validation of Domain Authorization or Control

Telia verifies that the Applicant has registered all domain(s) and/or IP address/addresses referenced in the certificate or has been authorized by the domain registrant to act on their behalf. Validation shall be done in accordance with the methods documented in section 3.2.2.4 of the CA/Browser Forum Baseline Requirements and implemented as listed herein below.

Each validation performed and recorded in accordance with this section contain the method identifier and then current Baseline Requirements version number.

3.2.2.4.1 Validating the Applicant as a Domain Contact

NOT allowed.

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

NOT allowed.

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 and if re-sent Telia CA ensures that the message is sent in its original content and unchanged.

3.2.2.4.5 Domain Authorization Document

NOT allowed.

3.2.2.4.6 Agreed-Upon Change to Website

NOT allowed.

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 by one of the following methods:

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.

This method is NOT ALLOWED to validate Wildcard Domain Names.

3.2.2.4.9 Test Certificate

NOT allowed.

3.2.2.4.10 TLS Using a Random Number

NOT allowed.

3.2.2.4.11 Any other method

NOT allowed.

3.2.2.4.12 Validating Applicant as a Domain Contact

If the CA is also the Domain Name Registrar, may be used on case-by-case basis upon prior approval of Telia CA Security Board and supervised by assigned Telia CA Security Board member.

3.2.2.4.13 Email to DNS CAA Contact

Following validation procedure is used.

- Unique random value is generated to be included in the email sent DNS CAA Email contact.
- Unique random value shall be unique for each email.
- CAA Resource Record is verified in accordance with RFC 8659 Section 3

- Messages may be re-sent in its entirety and if re-sent Telia CA ensures that the message is sent in its original content and unchanged.
- Random value is valid for a maximum lifetime of 30 days.
- The CAA contactemail property takes an email address as its parameter. The entire parameter value MUST be a valid email address as defined in RFC 6532, Section 3.2, with no additional padding or structure, or it cannot be used.

Each email MAY confirm control of multiple FQDNs, provided that each email address is a DNS CAA Email Contact for each Authorization Domain Name being validated.

3.2.2.4.14 Email to DNS TXT Contact

Following validation procedure is used.

- Unique random value is generated to be included in the email sent DNS TXT Record Email contact for the Authorization Domain Name selected to validate the Fully Qualified Domain Name.
- Unique random value shall be unique for each email.
- Messages may be re-sent in its entirety and if re-sent Telia CA ensures that the message is sent in its original content and unchanged.
- Random value is valid for a maximum lifetime of 30 days.
- The DNS TXT record MUST be placed on the "validation-contactemail" subdomain of the domain being validated. The entire RDATA value of this TXT record MUST be a valid email address as defined in RFC 6532, Section 3.2, with no additional padding or structure, or it cannot be used.

Each email MAY confirm control of multiple FQDNs, provided that each email address is a DNS TXT Email Contact for each Authorization Domain Name being validated.

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.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

May be used on case-by-case basis upon prior approval of Telia CA Security Board and supervised by assigned Telia CA Security Board member.

In case this method is used, following validation procedure is used under supervision:

- Performing direct call to the number defined in the DNS CAA Phone Contact (Record) for the Authorized Domain Name.
    - Telia CA does not accept calls knowingly transferred or requested to be transferred to the number provided by the said Record.
- The Contact MUST be reached directly from the number defined by the Record.
- Telia CA SHALL NOT use random values for this validation method.

Performed validation is documented and logged in accordance with this CP/CPS.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

May be used on case-by-case basis upon prior approval of Telia CA Security Board and supervised by assigned Telia CA Security Board member.

In case this method is used, following validation procedure is used under supervision:

- Performing direct call to the number defined in the relevant DNS CAA Resource Record (Record) found using algorithm defined in RFC 8659 Section 3.
    - Telia CA does not accept calls knowingly transferred or requested to be transferred to the number provided by the said Record.
- The Contact MUST be reached directly from the number defined by the Record.
- Telia CA SHALL NOT use random values for this validation method.

Performed validation is documented and logged in accordance with this CP/CPS.

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.

For each FQDN Telia CA performs separate validation using authorized method in this CP/CPS.

This method is NOT ALLOWED for validation of Wildcard Domain Names.

3.2.2.4.20 TLS Using ALPN

NOT allowed.

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 performing validation with one of the methods listed herein below.

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 ("_").

Each validation performed and recorded in accordance with this section contain the method identifier and then current Baseline Requirements version number.

3.2.2.5.1 Agreed-Upon Change to Website

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 the requirements set forth in BR Section 3.2.2.5.1.

3.2.2.5.2 Email, Fax, SMS, or Postal Mail to IP Address Contact

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 the requirements set forth in BR Section 3.2.2.5.2.

3.2.2.5.3 Reverse Address Lookup

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 Any Other Method

NOT allowed.

3.2.2.5.5 Phone Contact with IP Address Contact

Confirming the Applicant’s control over the IP Address by calling the IP Address Contact’s phone number, as identified by the IP Address Registration Authority, and obtaining a response confirming the Applicant’s request for validation of the IP Address, performed in accordance with the requirements set forth in BR Section 3.2.2.5.5.

The Contact MUST be reached directly from one single number identified by IP Address Registration Authority as the IP Address Contact.

Telia CA SHALL NOT use voicemail and random values for this validation method.

3.2.2.5.6 ACME “http-01” method for IP Addresses

Confirming the Applicant’s control over the IP Address by implementing “http-01” challenge in ACME service performed in accordance with BR Section 3.2.2.5.6 for the Applicant’s request for validation of the IP Address.

3.2.2.5.7 ACME “tls-alpn-01” method for IP Addresses

NOT allowed.

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.

3.2.2.8. CAA Records

Telia CA verifies CAA record for each dNSName in the subjectAltName extension of the Certificate to be issued, according to the procedure described in section 4.2.4 and complying with the requirements set forth in BR Section 3.2.2.8.

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

No stipulation.

3.2.5. Validation of authority

OV order via public web form or via using self-service software	Telia CA verifies that the administrative contact person defined in the certificate application is employed by the Subscriber. This is verified by calling the contact person via the Subscriber PBX number or by making a phone call to other verified number(s) in the organization, which is looked up from a directory maintained by a trusted party. Authorization of the administrative and technical contact persons may also be based on attorney letter or FullTLS agreement from the actual Subscriber. In that case CA will verify the origin of the authorization document by verification phone call. CA will always verify that the Subscriber's administrative contact person approves the subscriber agreement at least once including information about Subscriber responsibilities, Company details, authorised Certificate Approvers and all relevant subject or domain values allowed in the TLS certificates. In online service the agreement details are available to him/her online in the CA web pages so that the agreement can be modified at any time. In non-authenticated TLS web order all order details are verified each time by CA. In online mode the authenticated administrative contact person may be authorised by CA to approve further additions to the TLS contract (e.g. who can be Certificate Requester or Certificate Approver in the Company or if new domains are requested from CA). All authenticated and authorised contact persons are allowed to make TLS certificates but only in the limits of the pre-verified values and individual role. Data expiration time limits specified by CA/Browser Forum are utilized in all pre-verified values. Authentication is based on secure combination of SMS-OTP and weblinks with unique hash values. In internal Telia requests the authorization may be based on Employee register and authentication may be based on Telia email accounts Telia employees. Admistrative contact MUST be Telia Employee and technical contact may be Telia employee or Contingent worker found in Telia HR register. Technical contact, if contingent worker, may use his/her company email address. CA verifies that both technical and administrative contact persons are using approved Applicant company email addresses/domains and administrative contact persons are active employees of Telia Group and technical contact persons are active employees of Telia Group or contingent workers according to the Telia Group employee register.
DV order via public web form or via using self-service software.	Telia verifies host domain name/IP address ownership or control of those by using methods listed in the BR.

For 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

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

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

3.3. 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

3.4.1. 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 organization, who has additionally the rights of a Revocation Officer. The Revocation Officer in the Subscriber Organization 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 Organization is verified based on strong authentication method.

3.4.2. Revocation by the Revocation Service of the CA

The Subscriber or Registration Officer in a Subscriber Organization 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.

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

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.

3.4.3. Revocation of CAs

The authorised CA personnel can request revocation of a CA certificate. The Policy Management Team in the CA is responsible for the verification of the authenticity and authorisation of the request to revoke the certificate.

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

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

OV order via public web form	Manually processed Certificate application can be submitted by a representative of the Organization, which possesses or will possess the Device or service to which the certificate is applied. If the application is submitted by a different organization from the organization that owns the service, domain name or the IP address (e.g. by an IT service provider), the application must be authorised by the organization 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 organization 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 refuses to issue certificates to organizations registered in countries where Telia cannot reliably validate information to be included in the certificate.

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

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

DV and OV order using Telia's self-service software	A person in a Subscriber Organization 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. If the order includes new values or order is originated from a new person the subscriber's administrative contact must approve the new values or persons to be added to Subscriber's TLS contract. Then CA will verify that the Subscriber is allowed to use the new values before the certificate is created and the new values get pre-approved status for further orders. Only Telia Registration Officers may add new allowed Domain Name or Organization Name values for Subscriber that act as the RA role. New values are always verified according to 3.2. The Subscriber is bound through an TLS Service Agreement with Telia. The Registration Officers also accept Subscriber Responsibilities when they logon to Telia's self-service application for the first time.

4.2. Certificate application processing

4.2.1. Performing identification and authentication functions

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

Telia may use its previously documented validation data, provided that validation data is maximum 825 days old for OV and DV certificate applications. Validation data reuse period for FQDN and IP Address is maximum 398 days.

Old verification data including organization name, address components, Parent/Subsidiary/name change relationships, authorisation documents and domain/IP ownership are stored related to organization's registration number if available.

Telia CA maintains documented process and procedures to detect possible High Risk Certificate Requests to the reasonable extent possible to be able to perform duly verification of such requests.

4.2.2. Approval or rejection of certificate applications

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

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

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

4.2.3. Time to process certificate applications

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

4.2.4. Certificate Authority Authorization (CAA)

Telia CA supports requirements set forth in RFC 8659 (DNS Certification Authority Authorization (CAA) Resource Record) and RFC 8657 (Certification Authority Authorization (CAA) Record Extensions for Account URI and Automatic Certificate Management Environment (ACME) Method Binding.

CAA Resource records (RR) are verified for each dNSName in the subjectAltName extension of the Certificate to be issued, according to the procedures defined in RFC 8659 and RFC 8657 respectively.

Recognized authorized CAA domain names for non-ACME in Telia CA are:

- "telia.com"
- "telia.fi"
- "telia.se"
- "trust.telia.com"

Recognized authorized CAA domain names for ACME in Telia CA are:

- "acme.trust.telia.com"

Processing of CAA RR property tags are supported in accordance with requirements set forth in this section and 3.2.2.8. Telia CA processes following CAA RR property tags:

- Issue
- Issuewild
- Iodef

Recognized and supported CAA RR property tag parameters are:

- Critical Flag
- accounturi (only for ACME recognized CAA domains)
- validationmethods (only for ACME recognized CAA domains)

During validation Telia queries DNS for the existence of a CAA RR set. If CAA RRset exists, CAA property tags are processed and if Telia CA is not authorised by the CAA RRset, Telia will not issue the certificate.

Telia CA documents prevented issuances when CAA record did not authorize Telia CA to issue certificate.

4.3. Certificate issuance

Telia verifies certificate's structure and compliance with external requirements before enrolment to detect possible issues prior certificate is issued using industry best-practice linting tools and applications. Industry best-practice and recommended certificate linting tools are used to verify all issued TLS certificates in daily batch processing and output of daily run is verified the next day for any issues.

Any issue in pre-enrolment verification will prevent certificate to be issued and any issue identified in daily Lint verification shall result in revocation according to this CP/CPS by the CA.

4.3.1. CA actions during certificate issuance

4.3.1.1. CA certificate issuance

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 certificate is created by the CA according to the information contained in the certificate request and configured for the Subscriber. The CA may replace or remove information requested in the certificate request to ensure certificate compliance with this CP/CPS and other relevant requirements.

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

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

4.4. Certificate acceptance

By accepting a certificate, the Subscriber:

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

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

4.4.1. Conduct constituting certificate acceptance

The Subscriber is considered to have accepted the certificate when:

- The subscriber 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 within 7 days of issuance.

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.

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.
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	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. Subscriber Certificate Requester is responsible to ensure that the certificate information is still valid and that there are no other obstacles to the renewal. CA will verify the renewal request like it was a new request.

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 within 7 days of issuance.

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 as before.

4.7.1. Circumstance for certificate re-key

When old certificate is about to expire the subscriber may re-key the certificate. The key pairs are generated by the Subscriber, to Certificate Signing Request format (CSR) and given to CA. If Subscriber is also changing subject or SAN values the process reverts to Certificate modification described in section 4.8.

4.7.2. Who may request certification of a new public key
Authorized Subscriber's representative able to manage the certificate with permission to create new certificate.

4.7.3. Processing certificate re-keying requests
Certificate re-key requests are processed as certificate modification described in section 4.8 only supplying new key in the request. 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). Certificate re-key is sub-function to certificate modification only changing Subscriber's public key (certificate re-key).

4.8.1. Circumstance for certificate modification
When old certificate needs any kind of update a modification is required. Subscribers may do certificate modification in Telia CA certificate management portal.

Subscriber may change following certificate properties:

- Certificate type DV or OV
- Modify Subject Alternative Name (SAN) list (DNS)
- Add or modify subject:organizationName, subject:localityName and/or subject:countryName

CA may use the stored data of previous validations if available and such data is not expired. Any new data that requires validation shall be validated as described in section 3 and its sub-sections.

4.8.2. Who may request certificate modification
Authorized Subscriber's representative able to manage the certificate with permission to create new certificate.

4.8.3. Processing certificate modification requests
Certificate modification requests are processed as initial certificate requests as described in sections 4.1 – 4.4.

4.8.4. Notification of new certificate issuance to subscriber
Certificate modification notifications are generated like initial certificate notifications as described in section 4.3.2.

4.8.5. Conduct constituting acceptance of modified certificate
Certificate modification acceptance is done like initial certificate acceptance as described in section 4.4.1.

4.8.6. Publication of the modified certificate by the CA
Certificate publication is done like initial certificate publication as described in section 4.4.2.

4.8.7. Notification of certificate issuance by the CA to other entities
Certificate modification notifications are generated like initial certificate notifications as described in section 4.4.3.

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 by trustworthy means of communication (written request, phone call etc.)
2. The Subordinate CA notifies the Telia CA that the original certificate request was not authorised and does not retroactively grant authorisation
3. The Telia CA obtains evidence that the Subordinate CA's private key corresponding to the public key in the certificate suffered a key compromise or no longer complies with the 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

With the exception of Short-lived Subscriber Certificates, Telia CA will revoke a Subscriber certificate within 24 hours if one or more of the following occurs:

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

With the exception of Short-lived Subscriber Certificates, 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 RA or Telia CA

3. Owner of the server or device that possesses the certificate.
4. Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing the issuing CA of reasonable cause to revoke 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.

4.9.3.1. 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.

4.9.3.2. 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 as soon as possible 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 as soon as possible, 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

No stipulation.

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

All OCSP responses will be signed.

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

The OCSP service is using near-real-time CA database information. The OCSP responder may use the previous status value for a certificate if it is fresher than two hours old (refresh time). In rare circumstances where the connection between OCSP and CA is broken the status information may be up to 48 hours old (grace period).

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

4.9.10.1. Status of Subscriber Certificates

For the status of subscriber certificates following applies:

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

4.9.10.2. Status of Subordinate CA Certificates

For the status of subordinate CA certificates following applies:

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

4.9.10.3. Other information

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

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

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

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

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

4.9.11. Other forms of revocation advertisements available
Not applicable.

4.9.12. Special requirements regarding key compromise
In case of CA private key compromise, the procedures defined in 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
Telia CA does not support suspension.

4.9.14. Who can request suspension
Telia CA does not support suspension.

4.9.15. Procedure for suspension request
Telia CA does not support suspension.

4.9.16. Limits on suspension period
Telia CA does not support suspension.

4.10. Certificate status services

4.10.1. Operational characteristics

Revocation information on a CRL or OCSP Response are not removed until after the expiry date of revoked certificates. Telia CA ensures integrity and authenticity of the status information using strong security mechanisms. CRLs are digitally signed using the CA’s private key. OCSP 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.

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

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

5. FACILITIES, MANAGEMENT, AND OPERATIONAL CONTROLS

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

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

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

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

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

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

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

5.1. Physical controls

5.1.1. Site location and construction

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

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

5.1.1.1. CA Site location and construction

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

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

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

5.1.1.2. RA Site location and construction

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

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

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.

5.1.2. Physical access

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

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

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

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

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

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

5.1.2.1. CA Site Physical access

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

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

5.1.2.2. RA Site Physical access

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

5.1.3. Power and air conditioning

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

5.1.4. Water exposures

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

.

5.1.5. Fire prevention and protection

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

5.1.6. Media storage

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

5.1.7. Waste disposal

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

5.1.8. Off-site backup

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

5.2. Procedural controls

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

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

5.2.1. Trusted roles

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

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

Trusted Roles include, but are not limited to:

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

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

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

Typical duties which may be administered by the CAA include:

a. creating CA certificates
b. personalising cards

c. generating CA and central RA keys
d. configuration of CA and RA applications
e. generating revocation lists
f. Checking the certificate issue log

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

Typical duties which may be administered by the SA include:

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

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

5.2.1.4. Registration Officer: RA Office and Customer Service staff of the CA. Subscriber RA's Registration Officers are not Trusted Roles.

Typical duties of the Registration Officer include processing and approving certificate applications and submitting certificate requests to the CA system that issues and signs the certificates. Registration Officers also create new Subscriber accounts, privileges, and values to enable Telia's self-service software for 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 presence of and/or actions by multiple authorized Trusted Role individuals (Dual Control).

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

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

a. Each administrative login or physical access to critical servers or environments is causing alarm to be inspected by security supervisors. If alarm is caused by a security supervisor only another security supervisor can inspect and accept the alarm.
b. Each operation and command entered by operator is logged on the separate log server.
c. All operational remote access to critical systems is done only via secure management hosts.

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

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

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

5.2.3. Identification and authentication for each role

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

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

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

Each of these certificates and accounts shall be:

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

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

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

Identification of the RA roles takes place within the CA and RA system applications, and it is based on strong authentication either using personal operator cards or other two

factor authentication mechanisms depending on the policy requirements of the applicable CA.

5.2.4. Roles requiring separation of duties

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

5.3. Personnel controls

5.3.1. Qualifications, experience, and clearance requirements

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

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

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

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

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

5.3.2. Background check procedures

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

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

- Confirmation of previous employment

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

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

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

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

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

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

5.3.3. Training requirements

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

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

- Basic PKI concepts
- Telia CA's operational requirements and policies (e.g. CP/CPS, internal guidelines and instructions)
- Telia security and operational policies and procedures
- Use and operation of deployed hardware and software
- Incident and Compromise reporting and handling
- Common security and vulnerability awareness trainings and updates
- Global PKI community updates and trainings (e.g. CA/Browser forum updates)
- Role and occupation dependent training (e.g. Registration Officer)
- Individually tailored training programs

All personnel responsible for performance of certificate data validation (Validation Specialists in Baseline Requirements) are required on annual basis to complete and pass an exam to show proof of their validation skills in relation to this CP/CPS and consequently underlying Baseline Requirements.

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

5.3.5. Job rotation frequency and sequence
Not applicable.

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

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

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

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

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

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

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

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

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

4. All Log entries include the following elements:
    1. Date and time of event
    2. Identity of the person making the journal record
    3. Description of the event

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

5.4.2. Frequency of processing log

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

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

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

5.4.3. Retention period for audit log

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

5.4.4. Protection of audit log

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

5.4.5. Audit log backup procedures

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

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

5.4.6. Audit collection system (internal vs. external)

Automated audit data is generated and recorded at the application, network, and operating system level.

Manually generated audit data is recorded by Telia personnel.

5.4.7. Notification to event-causing subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, 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 cases where the archived information constitutes a digitally signed volume of information, the necessary information required for verifying the signature during the stated archiving time is also archived.

5.5.2. Retention period for archive

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

5.5.3. Protection of archive

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

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

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

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

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

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, using the following procedure:

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

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

a. A new subordinate CA key pair is created
b. A new subordinate CA certificate is issued for the new public CA key by the superior CA on the next level of the hierarchy

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

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

5.7. Compromise and disaster recovery

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

5.7.1. Incident and compromise handling procedures

Telia has implemented detailed change and incident management procedures to allow for controlled and accountable handling of incidents and recovery from system and application disasters. Regarding disaster recovery at the site level Telia has implemented disaster recovery plans. 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 comprised key or keys certified using the compromised key. This means that all associated revocation lists are removed from their assigned locations
c. Inform all key holders and all parties with which Telia has a relationship

that the CA's private key has been compromised and how new CA certificates can be obtained
d. In the event that Telia has cross certified the compromised CA key with another operational CA key, revoke any such cross certificates

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

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

Information will be made available to relying parties, who are clearly informed that the use of the affected certificates and the CA's issuer certificate has been revoked.

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

5.7.4. Business continuity capabilities after a disaster

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

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

5.8. CA or RA termination

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

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

a. Ensure that any disruption caused by the termination of an Issuing CA is minimized as much as possible
b. Provision of notice to parties affected by the termination, such as Subscribers Relying Parties, and Supervisory bodies and informing them of the status of the CA
c. Make public announcement in the CA repository at least three months in advance that operations will cease for the CA
d. Revoke all active Certificates before the end of the three months' notice period
e. Destroy private keys, including backup copies, in a manner such that the private

keys cannot be retrieved

f. Cease all revocation checking services relating to certificates issued using the CA keys of which use will cease. This means that all associated revocation lists are removed from their assigned locations and that no new revocation lists are issued to replace those that are removed
g. Terminate all rights for subcontractors to act in the name of the CA which will cease to operate
h. Ensure that all archive records of the issuing CA are retained
i. Prior terminating the CA services - if applicable depending on the agreed contracts, Telia may transfer provision of the CA services for its existing Subscribers to another CA successor entity
j. Notify relevant parties such as auditors, CA root programs and CCADB

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

6. TECHNICAL SECURITY CONTROLS

6.1. Key pair generation and installation

6.1.1. Key pair generation

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

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

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

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

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

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

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.

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

Telia CA never create Subscriber private keys.

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, or RA key pairs are generated by Telia, this requirement is not applicable.

The public key is delivered digitally signed in a CSR file and using an encrypted connection.

6.1.4. CA public key delivery to relying parties

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

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

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

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

No other key sizes or algorithms are permitted.

6.1.5.1. CA key pairs

Allowed key sizes and algorithms for CA key pairs are:

- RSA algorithm (rsaEncryption (OID: 1.2.840.113549.1.1.1) with a minimum key length of 4096 bits and restricted to either 4096 or 8192 bits for a CA key pair.
- ECDSA algorithm, NIST P-384, namedCurve secp384r1 (OID: 1.3.132.0.34)

6.1.5.2. Subscriber key pairs

Allowed key sizes and algorithms for Subscriber key pairs are:

- RSA algorithm (rsaEncryption (OID: 1.2.840.113549.1.1.1)
    - Minimum key length of 2048 bits and restricted to one (1) of the following key lengths: 2048, 3072, 4096 or 8192 bits for a subscriber certificate key pair.
- ECDSA algorithm (id-ecPublicKey (OID: 1.2.840.10045.2.1)
    - P-256, namedCurve secp256r1 (OID: 1.2.840.10045.3.1.7)
    - P-384, namedCurve secp384r1 (OID: 1.3.132.0.34)

6.1.6. Public key parameters generation and quality checking

Telia uses a HSM device that conforms to FIPS 186-2 and provides random number

generation and on-board generation of up to 8192 bit RSA Public Keys and a wide range of ECC curves.

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

Telia verifies the quality of keys before accepting the certificate request in accordance with the requirements set forth in Baseline Requirements section 6.1.6.

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.

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

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

- Signing of self-signed Certificate to represent the Root CA itself
- Signing of subordinate CA certificates and Cross Certificates by the Root CA
- Signing of OCSP response verification certificates

6.2. Private key protection and cryptographic module engineering controls

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

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

6.2.1. Cryptographic module standards and controls

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

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

The Subscriber private keys are generated by the Subscribers and private keys are protected and stored by the Subscriber.

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

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

operations.

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

6.2.3. Private key escrow

Telia CA does not escrow Subscriber private keys.

6.2.4. Private key backup

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

No backups are made of Subscriber private keys.

See section 4.12. for a more detailed description.

6.2.5. Private key archival

RA or CA private keys will be archived by Telia CA for disaster recovery purposes.

Telia CA does not archive Subscriber private keys.

6.2.6. Private key transfer into or from a cryptographic module

Telia CA generates CA key pairs on the hardware cryptographic modules in which the keys will be used. Where CA key pairs are transferred to another hardware cryptographic module for clustering reasons such key pairs are transported between modules in encrypted form using private networks dedicated for Telia CA.

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

6.2.7. Private key storage on cryptographic module

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

6.2.8. Method of activating private key

CA keys:

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

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

requires the use of activation data as described in section 6.4.

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

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

6.2.9. Method of deactivating private key

CA keys:

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

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

Software keys:

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

Smart Cards and USB tokens:

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

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. Physical destruction is used when destroying the media.

When the Subscriber's certificate becomes expired and it is not renewed, related private key 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.

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

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

Certificate type	Key pair usage period	Certificate term
Publicly Trusted Root CA	25 years	Maximum 25 years
Publicly Trusted Cross-Certified Subordinate CA	25 years	Maximum 25 years
Publicly Trusted Subordinate CA	25 years	Maximum 25 years
Subscriber Domain Validated certificates	Maximum 397 days	Maximum 397 days
Subscriber Organization Validated certificates	Maximum 397 days	Maximum 397 days

Subscriber certificates issued in accordance with this CPS are issued for both new keys and for existing keys.

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

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

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

For calculations, a day is measured as 86,400 seconds. Any amount of time greater than this, including fractional seconds and/or leap seconds, represents an additional day. For purposes of calculating time periods in this document, increments are rounded down subject to the imposed maximum requirements.

6.4. Activation data

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

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

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

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

6.4.1. Activation data generation and installation

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 RAs 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.

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.

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 organizations 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.

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 updated to the staging system. The acceptance test is performed in the test system before the changes are taken into production.

All the changes in the system 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 Guidelines[3].

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

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

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/

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 guaranteeing non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG..
Signature algorithm	The signature algorithm is the set of mathematical rules according to which the CA software executes the signing of the certificate. Identifiers have been allocated for the algorithms that are generally used. The identifier of the algorithm used for the signing of the certificate is given in this field. The signature cannot be verified if the algorithm used is not known. The algorithm that is used for the signing of the certificates is one of the following sha256RSA/ECDSA, sha384RSA/ECDSA or sha512RSA
Issuer	This field states the name of the Issuer of the certificate. The Issuer name in the certificates of each CA has been described in section 1.3.1. 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".

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

Extension	Criticality	Extension description and contents	In Root CA
Authority key identifier OID: 2.5.29.35	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 OID: 2.5.29.14	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 OID: 2.5.29.32	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 OID: 2.5.29.31	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 OID: 2.5.29.15	critical	The key usage purposes of the public key contained in the certificate are given in this extension. Within Telia PKI the key usage purposes of the public key of the CA are: - Certificate signing (KeyCertSign) - CRL signing (CRLSign)	Yes
Basic constraints OID: 2.5.29.19	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 OID: 1.3.6.1.5.5.7.1.1	non-critical	This extension may contain two values: a. The URL to CA-certificate b. OCSP service address as defined by RFC6960 Typically, all subordinate CA certificates include both listed values.	No

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

Extension	Authority	Extension description and contents
Authority key identifier OID: 2.5.29.35	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 OID: 2.5.29.14	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 OID: 2.5.29.32	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 OID: 2.5.29.31	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 OID: 2.5.29.15	CA	The key usage purposes of the public key contained in the certificate are given in this extension. The CA is not responsible for use other than the given key usage purposes. The key usage extension is optional for Telia server certificates. Purposes KeyCertSign and cRLSign are never set. The key usage purposes of the public keys contained in the OV and DV certificates typically include: Digital Signature, Key Encipherment. Key usage may include Data Encipherment in OV certificates.

Extension	Authority	Extension description and contents
Extended key usage OID: 2.5.29.37	CA	This extension contains other key usage purposes of the public key except those contained in the "Key usage" extension. A key usage purpose given in this extension may be generally known or privately defined for a certain application. The extended key usage purposes of the public keys contained in the OV and DV certificates include: Server authentication and Client authentication
Subject alternative name OID: 2.5.29.17	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 Information Access OID: 1.3.6.1.5.5.7.1.1	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.

If Basic Constraints extension is set in Subscriber Certificate, the cA flag is always set to FALSE.

Other extensions may be used in Subscriber certificates, if agreed with Telia or added to CSR and CA is aware of a reason for including the data in the certificate. Telia CA SHALL ensure before accepting any value to be set in Subscriber certificate, that the Subscriber certificate contents comply with Baseline Requirements section 7.1.2 and adequate documentation supporting and explaining the authorization to use such extensions.

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.

Precertificates are issued by the issuing CA directly and contain the Precertificate Poison extension (OID: 1.3.6.1.4.1.11129.2.4.3) extnValue OCTET STRING which is exactly the hexencoded bytes 0500, the encoded representation of the ASN.1 NULL value, as specified in RFC 6962, Section 3.1.

Telia constructs and signs a Precertificate corresponding to the Certificate, for purposes of submitting to Certificate Transparency Logs and Signed Certificate Timestamps added to the Certificate's extensions field in accordance with TLS BR 7.1.2.11.3 and as permitted by the relevant subscriber certificate profile, prior to signing the Certificate.

7.1.3. Algorithm object identifiers

7.1.3.1. SubjectPublicKeyInfo

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

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

No other encodings are permitted.

7.1.3.2. SignatureAlgorithmIdentifier

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

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

No other encodings are permitted.

7.1.4. Name forms

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

7.1.5. Name constraints

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

7.1.6. Certificate policy object identifier

The 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 issues CRLs compliant with RFC 5280.

7.2.1. Version number(s)
All issued CRL's are X.509 version 2 CRL's in accordance with the RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and 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 OID: 2.5.29.35	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 OID: 2.5.29.20	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
Reason Code of the CRL Entry OID: 2.5.29.21	For CRL Entries of Root CA, Subordinate CA and Cross-Certifier Subordinate CA reasonCode is always present. For Certificates not capable of issuing certificates reasonCode is present unless reasonCode is "unspecified (0)" reasonCodes shall be used in accordance to Baseline Requirements 7.2.2 and this CP/CPS

7.3. OCSP profile
Telia CA supports OCSP in accordance with section 7.3 of the Baseline Requirements, 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.

The singleExtensions (if present) of an OCSP response does not contain reasonCode (OID 2.5.29.21) CRL entry extension.

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 organizational 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 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2 (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.

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 organization.

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/en/articles/privacy#telia-company-privacy-policy

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

9.6.2. RA representations and warranties

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

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

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

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

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

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

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

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

9.12.1. Procedure for amendment

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.

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

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

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

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

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

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

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

9.16.5. Force Majeure

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

9.17. Other provisions

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

Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the 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.