

SIGNATORIES

Name	Authentication method	Date and time
JOHN GUSTAVSSON	Strong, BankID SE	06.02.2024 10:07:23 UTC+02

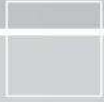


This document package contains:

- Front page (this page)
- The original document(s)
- The electronic signatures. These are not visible in the document, but are electronically integrated



This file is sealed with a digital signature.
The seal is a guarantee for the authenticity
of the document



Telia Company AB

ETSI Audit Report 2023

datenschutz cert GmbH
1. Februar 2024

To the management of Telia Company AB („Telia”)

Scope

datenschutz cert GmbH as an accredited Conformity Assessment Body has been engaged, in a reasonable assurance engagement, to report on Telia management’s assertion that for its Certification Authority (CA) as enumerated in Appendix B, operated by Telia and its affiliates listed in Appendix E, at their locations listed in Appendix C, throughout the period April 1, 2023 to October 31, 2023, Telia has:

- Disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in the applicable versions of its Certification Practice Statements and Certificate Policies in Appendix A.
- Maintained effective controls to provide reasonable assurance that:
 - Telia’s applicable versions of its Certification Practice Statements are consistent with its Certificate Policies as enumerated in Appendix A.
 - Telia provides its services in accordance with applicable versions of its Certificate Policies and Certification Practice Statements as enumerated in Appendix A.
- Maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
 - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
 - subscriber information is properly authenticated (for the registration activities performed by Telia); and
 - subordinate CA certificate requests are accurate, authenticated, and approved.
- Maintained effective controls to provide reasonable assurance that:
 - logical and physical access to CA systems and data is restricted to authorized individuals;
 - the continuity of key and certificate management operations is maintained; and
 - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity.

in accordance with the general requirements for Trust Service Providers (ETSI EN 319 401 V2.3.1), and the policy and security requirements for Trust Service Providers issuing certificates specifically:

- ETSI EN 319 411-1 V1.3.1, NCP;DVCP;OVCP for website authentication certificates (SSL trust bit)
- ETSI TS 119 411-6 V1.1.1, ETSI EN 319 411-1 V1.3.1, NCP for email certificates (email trust bit)

Telia does not escrow its CA keys. Accordingly, our procedures did not extend to controls that would address those criteria.

Certification authority's responsibilities

Telia's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the general requirements for Trust Service Providers (ETSI EN 319 401 V2.3.1), and the policy and security requirements for Trust Service Providers issuing certificates specifically:

- ETSI EN 319 411-1 V1.3.1, NCP; DVCP; OVCP for website authentication certificates (SSL trust bit)
- ETSI TS 119 411-6 V1.1.1, ETSI EN 319 411-1 V1.3.1, NCP for email certificates (email trust bit)

Our independence and quality control

We have complied with the independence and other ethical requirements according to our accreditation under ISO/IEC 17065, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies International Standard on Quality Control 1, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with International Standard Conformity assessment - Requirements for bodies certifying products, processes and services (ISO/IEC 17065), Trust Service Provider Conformity Assessment; Part 1 (ETSI EN 319 403-1), and Trust Service Provider Conformity Assessment; Part 2 (ETSI EN 319 403-2). These standards require that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

1. obtaining an understanding of Telia's key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance and operation of systems integrity;
2. selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business practices;
3. testing and evaluating the operating effectiveness of the controls; and
4. performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Telia's management has disclosed to us the attached comments (Appendix D) that have been posted publicly in the online forums of the Bugzilla site, as well as the online forums of individual internet browsers that comprise the CA/Browser Forum.

We have considered the nature of these comments in determining the nature, timing and extent of our procedures.

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at Telia and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

Because of the nature and inherent limitations of controls, Telia's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

Opinion

In our opinion, throughout the period from April 1, 2023 to October 31, 2023, Telia management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the general requirements for Trust Service Providers (ETSI EN 319 401 V2.3.1), and the policy and security requirements for Trust Service Providers issuing certificates (ETSI EN 319 411-1 V1.3.1, ETSI TS 119 411-6 V1.1.1).

This report does not include any representation as to the quality of Telia's services beyond those covered by the general requirements for Trust Service Providers (ETSI EN 319 401 V2.3.1), and the policy and security requirements for Trust Service Providers issuing certificates (ETSI EN 319 411-1 V1.3.1, ETSI TS 119 411-6 V1.1.1), nor the suitability of any of Telia's services for any customer's intended purpose.

February 1, 2024
datenschutz cert GmbH
Represented by

Dr. Sönke Maseberg, CEO

Appendix A – Certification Practice Statements (CPS) and Certificate Policies (CP) in Scope

CP/CPS for Server Certificates

- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 4.8, effective date: 2022-12-30
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 4.9, effective date: 2023-04-07
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.0, effective date: 2023-06-29

CP/CPS for Client Certificates

- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 3.5, effective date: 2022-12-30
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 3.6, effective date: 2023-04-07
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 3.7, effective date: 2023-06-29
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 3.8, effective date: 2023-08-31

Appendix B – Root and Intermediate CAs in scope

For some CAs a note was added to put emphasis on a certain detail.

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN = TeliaSonera Root CA v1 O = TeliaSonera	SHA-256 fingerprint of the certificate: DD6936FE21F8Fo77C123A1A521C12224F72255B73Eo3A726o693E8A24BoFA389	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP

Table 1: Root-CA 1 in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN=Telia Root CA v2, O=Telia Finland Oyj, C=FI	SHA-256 fingerprint of the certificate: EF6F29F636F62BDD4753122F41F3419EE7C2877587BE4A98o7ADF58946458E7F Note: Cross Certified Subordinate CA Certificate.	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN=TeliaSonera Server CA v2, O=TeliaSonera, C=FI	SHA-256 fingerprint of the certificate: D721110388CA6F2oBBA9FD1A8DBA4EFB8C16392A3DEBAD97C553EEAFoACACAAC Note: After 2023-03-31 this CA has renewed the test certificates required by CA/B Forum TLS BR in June 2023, only, no other certificates issued.	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP, OVCP

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN=Telia Domain Validation CA v2, O=Telia Finland Oyj, C=FI Note: After 2023-03-31 this CA has renewed the test certificates required by CA/B Forum TLS BR in June 2023, only, no other certificates issued.	SHA-256 fingerprint of the certificate: 5B312B7E11B70Do7C14EoAB99Fo8Doo748966098C52AA85Ao6Ao822BBE59Ao2C	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP, DVCP
Complete subject DN: CN=TeliaSonera Class 1 CA v2, O=Te- liaSonera, C=FI Note: During the period of 2023-04-01 – 2023-08-31 this CA was used for client issuance only and has not been used for issuance after 2023-08-31.	SHA-256 fingerprint of the certificate: B95AE54F838E3ABFoB57ACCC1B1266DC68C7A3FA774015FA128D6oCDD1AAE28o	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN=TeliaSonera Class 1 CA v2, O=Te- liaSonera, C=FI	SHA-256 fingerprint of the certificate: F6EoD3o06465585AA276E4o8619451o2B266o7o8399879o62FD53A2o4oEB5B31	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN=TeliaSonera Class 2 CA v2, O=Te- liaSonera, C=SE Note: During the period of 2023-04-01 – 2023-08-31 this CA was used for client issuance only and has not been used for issuance after 2023-08-31.	SHA-256 fingerprint of the certificate: o92829433D231949F4A9BC666CBF54B3AA27D7BEBCAo48D75E59o93E15A72EA5	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN=TeliaSonera Class 2 CA v2, O=Te- liaSonera, C=SE	SHA-256 fingerprint of the certificate: 1oDo81A9541BFoB388818447A2A754658o9AA5FB9A3DF3756o2472E873432AC1	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN=TeliaSonera Email CA v4, O=TeliaSonera, C=SE Note: During the period of 2023-04-01 – 2023-08-31 this CA was used for client issuance only and has not been used for issuance after 2023-08-31.	SHA-256 fingerprint of the certificate: D1F2656AC8382739A3B087C47AB5CAB945A32F162B6149C308783C7E06AF8AE8	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN=TeliaSonera Email CA v4, O=TeliaSonera, C=SE	SHA-256 fingerprint of the certificate: 77D82B83905D4465A3EB6B62E42081A7C273632F7D6CDA33A1E366987420AD12	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN = Ericsson NL Individual CA v3, O = Ericsson, C = SE	SHA-256 fingerprint of the certificate: 63ED95B17FFDCB7AE30FEAC6A874653099264E21B268D836D957966FoBo4BE43 Note: This CA has not been used for issuance during the audit period.	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN = Telia Class 3 CA v2, O = Telia Company AB, C = SE	SHA-256 fingerprint of the certificate: 5E343F2432BBFoECC7062F4237110581DFFD638CC3689D50D5864174C9DC011D Note: This CA has not been used for issuance during the audit period.	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP

Table 2: Sub-CA's issued by the Root-CA 1 or its Sub-CA's in scope of the audit

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN=Telia Root CA v2, O=Telia Finland Oyj, C=FI	SHA-256 fingerprint of the certificate: 242B69742FCB1E5B2ABF98898B94572187544E5B4D9911786573621F6A74B82C	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP

Table 3: Root-CA 2 in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN=Telia Domain Validation CA v3 O=Telia Finland Oyj, C=FI	SHA-256 fingerprint of the certificate: A7E83056E9B3D9DDB1816B95518F6A5E5A1DFDFA28F60533B1C850855EAA4263	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP, DVCP
Complete subject DN: CN=Telia Server CA v3, O=Telia Finland Oyj, C=FI	SHA-256 fingerprint of the certificate: 1281AD8FABE883F209E9636448D1A80C373DAA7686C813A270FAD48F5F5E589A	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP, OVCP
Complete subject DN: CN = Telia Document Signing CA v3, O = Telia Finland Oyj, C = FI	SHA-256 fingerprint of the certificate: 6924A4DD82948DA53F6FB933E895A0F6581C8DBDEBABB36FC11CAC25E9Co335A	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN = Telia Class 3 CA v1, O = Telia Company AB, C = SE	SHA-256 fingerprint of the certificate: E734oDC9475E87C4E5A4572C82604C5EFF9BF6oB231C5486943173B26A4CAFCC	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN = Telia Class 1 CA v3, O = Telia Finland Oyj, C = FI	SHA-256 fingerprint of the certificate: 2E459B4B2F4C24D3BCF6D357E21DC74286C8891o4888267E2BACA75C78D1A615 Note: This CA has not issued certificates after 2023-08-31.	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN = Telia Class 1 CA v3, O = Telia Finland Oyj, C = FI	SHA-256 fingerprint of the certificate: E85BA26F89FEB67oA2638E1E293o54DE1A955DD19o9AoAFD5o8B1F87Fo61o4A9	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN = Telia Class 2 CA v3, O = Telia Company AB, C = SE	SHA-256 fingerprint of the certificate: E5F6844EABECA374B597295671CD12C37D7CDBBFE75529C4D61E5BA2BD32BB11 Note: This CA has not issued certificates after 2023-08-31.	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN = Telia Class 2 CA v3, O = Telia Company AB, C = SE	SHA-256 fingerprint of the certificate: 96FD4A9ED8E28B9o1D5E93E265992A9D411D49DC228oB5CF89398A862B7E26EC	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN = Telia Email CA v5, O = Telia Company AB, C = SE	SHA-256 fingerprint of the certificate: 8BB1BA521951077143A02CDB409D200B954F4684E59C67682A14852EF7B3EB44 Note: This CA has not issued certificates after 2023-08-31.	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN = Telia Email CA v5, O = Telia Company AB, C = SE	SHA-256 fingerprint of the certificate: E26BA792CDF9E21B6402044DD9A61E2E1537D5FFD22EE2478979408E3233310A	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN = Ericsson NL Individual CA v4, O = Ericsson, C = SE	SHA-256 fingerprint of the certificate: 800707B1F57FCDF95CFB047B387C6F48142DA885B7DC1FED28C5F87FoC712AD4 Note: This CA has not issued certificates after 2023-08-31.	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN = Ericsson NL Individual CA v4, O = Ericsson, C = SE	SHA-256 fingerprint of the certificate: EE0343093DF71E364606100164C62A4FB8C4AoF32B1EB4786oFFD6C17E94CA54	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP

Table 4: Sub-CA's issued by the Root-CA 2 or its Sub-CA's in scope of the audit

Appendix C – Locations audited

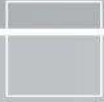
Operational management of the CA, Helsinki, Finland
Datacenter 1, Hosting of infrastructure and CA issuing systems, Helsinki, Finland
Datacenter 2, Hosting of infrastructure and CA issuing systems, Helsinki, Finland
Operational management of the CA, Solna, Sweden
Datacenter, Handen, Sweden

Appendix D - Publicly disclosed incidents

- Bug 1859314, Telia: TLS certificates issued in violation of TLS BR v2.o.1
https://bugzilla.mozilla.org/show_bug.cgi?id=1859314.
- Bug 1856591, Telia: S/MIME certificates issued in violation of S/MIME BR v1.o.1
https://bugzilla.mozilla.org/show_bug.cgi?id=1856591.

Appendix E – Legal entities operating the CA services

1. Telia Company AB, Sweden
2. Telia Finland Oyj, Finland
3. Cygate AB, Sweden



datenschutz cert GmbH

Hauptsitz Bremen

Konsul-Smidt-Straße 88a

28217 Bremen

Tel.: 0421 69 66 32 50

office@datenschutz-cert.de

www.datenschutz-cert.de

datenschutz
■ ■ ■ cert

Telia's Management's Assertion

Telia Company AB ("Telia") and affiliates listed in [Appendix E](#) operate the Certification Authority (CA) services as disclosed in [Appendix B](#) and provide the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subscriber key generation and management
- Subordinate CA [cross-]certification

The management of Telia is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to Telia's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Telia's management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in Telia's management's opinion, in providing its Certification Authority (CA) operations at its locations as detailed in [Appendix C](#), throughout the period April 1, 2023 to October 31, 2023, Telia has:

- Disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management and CA Environment Control practices in the applicable versions of its Certification Practice Statement and Certificate Policy, as enumerated in [Appendix A](#).
- Maintained effective controls to provide reasonable assurance that:
 - Telia's applicable versions of its Certification Practice Statements are consistent with its Certificate Policies as enumerated in [Appendix A](#)
 - Telia provides its services in accordance with applicable versions of its Certificate Policies and Certification Practice Statements as enumerated in [Appendix A](#)
- Maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and certificates it manages was established and protected throughout their lifecycles;
 - the integrity of subscriber keys and certificates it manages was established and protected throughout their lifecycles;
 - subscriber information was properly authenticated (for the registration activities

- performed by Telia); and
- subordinate CA certificate requests were accurate, authenticated, and approved
- Maintained effective controls to provide reasonable assurance that:
 - logical and physical access to CA systems and data was restricted to authorized individuals;
 - the continuity of key and certificate management operations was maintained; and
 - CA systems development, maintenance, and operations were properly authorized and performed to maintain CA systems integrity
- Disclosed the attached comments ([Appendix D](#)) that have been posted publicly in the online forums of the Bugzilla site, as well as the online forums of individual internet browsers that comprise the CA/Browser Forum.

in accordance with the general requirements for Trust Service Providers ([ETSI EN 319 401 V2.3.1](#)), and the policy and security requirements for Trust Service Providers issuing certificates specifically:

- [ETSI EN 319 411-1 V1.3.1](#), NCP;DVCP;OVCP for website authentication certificates (SSL trust bit)
- [ETSI EN 319 411-1 V1.3.1](#), [ETSI TS 119 411-6 V1.1.1](#), NCP for email certificates (email trust bit)

These requirements cover the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management

- Certificate Policy Management
- Certification Practice Statement Management
- CP and CPS Consistency

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise

- CA Cryptographic Hardware Lifecycle Management

Subscriber Key Lifecycle Management Controls

- CA-Provided Subscriber Key Generation Services
- CA-Provided Subscriber Key Storage and Recovery Services
- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

Telia does not escrow its CA keys. Accordingly, our assertion does not extend to controls that would address those criteria.

Telia Company AB
Helsinki, Sweden

John Gustavsson
Function: Head of Trust Services

February 06, 2024

Appendix A – Certification Practice Statements and Certificate Policies in Scope

Telia Server certificates		
Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates	Begin Effective Date	End Effective Date
Release 4.8	December 30, 2022	April 7, 2023
Release 4.9	April 7, 2023	June 29, 2023
Release 5.0	June 29, 2023	November 7, 2023

Telia Client certificates		
Certification Practice Statement and Certificate Policy	Begin Effective Date	End Effective Date
Release 3.5	December 30, 2022	April 7, 2023
Release 3.6	April 7, 2023	June 29, 2023
Release 3.7	June 29, 2023	August 31, 2023
Release 3.8	August 31, 2023	November 7, 2023

Appendix B – Root and Intermediate CAs in scope

For some CAs a note was added to put emphasis on a certain detail.

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN=TeliaSonera Root CA v1, O=TeliaSonera	SHA-256 fingerprint of the certificate: DD6936FE21F8F077C123A1A521C12224F72255B73E03A7260693E8A24B0FA389	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP

Table 1: Root-CA 1 in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN=Telia Root CA v2, O=Telia Finland Oyj, C=FI	SHA-256 fingerprint of the certificate: EF6F29F636F62BDD4753122F41F3419EE7C2877587BE4A9807ADF58946458E7F Note: Cross Certified Subordinate CA Certificate.	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN=TeliaSonera Server CA v2, O=TeliaSonera, C=FI	SHA-256 fingerprint of the certificate: D721110388CA6F20BBA9FD1A8DBA4EFB8C16392A3DEBAD97C553EEAF0ACACAAC Note: After 2023-03-31 this CA has renewed the test certificates required by CA/B Forum TLS BR in June 2023, only, no other certificates issued.	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP, OVCP
Complete subject DN: CN=Telia Domain Validation CA v2, O=Telia Finland Oyj, C=FI	SHA-256 fingerprint of the certificate: 5B312B7E11B70D07C14E0AB99F08D00748966098C52AA85A06A0822BBE59A02C Note: After 2023-03-31 this CA has renewed the test certificates required by CA/B Forum TLS BR in June 2023, only, no other certificates issued.	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP, DVCP
Complete subject DN: CN=TeliaSonera Class 1 CA v2, O=TeliaSonera, C=FI	SHA-256 fingerprint of the certificate: B95AE54F838E3ABF0B57ACCC1B1266DC68C7A3FA774015FA128D60CDD1AAE280 Note: During the period of 2023-04-01 – 2023-08-31 this CA was used for client issuance only and has not been used for issuance after 2023-08-31.	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN=TelioSonera Class 1 CA v2, O=TelioSonera, C=FI	SHA-256 fingerprint of the certificate: F6E0D3006465585AA276E40861945102B2660708399879062FD53A2040EB5B31	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN=TelioSonera Class 2 CA v2, O=TelioSonera, C=SE	SHA-256 fingerprint of the certificate: 092829433D231949F4A9BC666CBF54B3AA27D7BEBCA048D75E59093E15A72EA5 Note: During the period of 2023-04-01 – 2023-08-31 this CA was used for client issuance only and has not been used for issuance after 2023-08-31.	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN=TelioSonera Class 2 CA v2, O=TelioSonera, C=SE	SHA-256 fingerprint of the certificate: 10D081A9541BF0B388818447A2A75465809AA5FB9A3DF375602472E873432AC1	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN=TelioSonera Email CA v4, O=TelioSonera, C=SE	SHA-256 fingerprint of the certificate: D1F2656AC8382739A3B087C47AB5CAB945A32F162B6149C308783C7E06AF8AE8 Note: During the period of 2023-04-01 – 2023-08-31 this CA was used for client issuance only and has not been used for issuance after 2023-08-31.	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN=TelioSonera Email CA v4, O=TelioSonera, C=SE	SHA-256 fingerprint of the certificate: 77D82B83905D4465A3EB6B62E42081A7C273632F7D6CDA33A1E366987420AD12	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN = Ericsson NL Individual CA v3, O = Ericsson, C = SE	SHA-256 fingerprint of the certificate: 63ED95B17FFDCB7AE30FEAC6A874653099264E21B268D836D957966F0B04BE43 Note: This CA has not been used for issuance during the audit period.	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN = Telia Class 3 CA v2, O = Telia Company AB, C = SE	SHA-256 fingerprint of the certificate: 5E343F2432BBF0ECC7062F4237110581DFFD638CC3689D50D5864174C9DC011D Note: This CA has not been used for issuance during the audit period.	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP

Distinguished Name	SHA-256 fingerprint	Applied policy
--------------------	---------------------	----------------

Table 2: Sub-CA's issued by the Root-CA 1 or its Sub-CA's in scope of the audit

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN=Telia Root CA v2, O=Telia Finland Oyj, C=FI	SHA-256 fingerprint of the certificate: 242B69742FCB1E5B2ABF98898B94572187544E5B4D9911786573621F6A74B82C	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP

Table 3: Root-CA 2 in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN=Telia Domain Validation CA v3, O=Telia Finland Oyj, C=FI	SHA-256 fingerprint of the certificate: A7E83056E9B3D9DDB1816B95518F6A5E5A1DFDFA28F60533B1C850855EAA4263	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP, DVCP
Complete subject DN: CN=Telia Server CA v3, O=Telia Finland Oyj, C=FI	SHA-256 fingerprint of the certificate: 1281AD8FABE883F209E9636448D1A80C373DAA7686C813A270FAD48F5F5E589A	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP, OVCP
Complete subject DN: CN = Telia Document Signing CA v3, O = Telia Finland Oyj, C = FI	SHA-256 fingerprint of the certificate: 6924A4DD82948DA53F6FB933E895A0F6581C8DBDEBABB36FC11CAC25E9C0335A	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN = Telia Class 3 CA v1, O = Telia Company AB, C = SE	SHA-256 fingerprint of the certificate: E7340DC9475E87C4E5A4572C82604C5EFF9BF60B231C5486943173B26A4CAFCC	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN = Telia Class 1 CA v3, O = Telia Finland Oyj, C = FI	SHA-256 fingerprint of the certificate: 2E459B4B2F4C24D3BCF6D357E21DC74286C889104888267E2BACA75C78D1A615 Note: This CA has not issued certificates after 2023-08-31.	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN = Telia Class 1 CA v3, O = Telia Finland Oyj, C = FI	SHA-256 fingerprint of the certificate: E85BA26F89FEB670A2638E1E293054DE1A955DD1909A0AFD508B1F87F06104A9	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN = Telia Class 2 CA v3, O = Telia Company AB, C = SE	SHA-256 fingerprint of the certificate: E5F6844EABECA374B597295671CD12C37D7CDBBFE75529C4D61E5BA2BD32BB11 Note: This CA has not issued certificates after 2023-08-31.	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN = Telia Class 2 CA v3, O = Telia Company AB, C = SE	SHA-256 fingerprint of the certificate: 96FD4A9ED8E28B901D5E93E265992A9D411D49DC2280B5CF89398A862B7E26EC	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN = Telia Email CA v5, O = Telia Company AB, C = SE	SHA-256 fingerprint of the certificate: 8BB1BA521951077143A02CDB409D200B954F4684E59C67682A14852EF7B3EB44 Note: This CA has not issued certificates after 2023-08-31.	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN = Telia Email CA v5, O = Telia Company AB, C = SE	SHA-256 fingerprint of the certificate: E26BA792CDF9E21B6402044DD9A61E2E1537D5FFD22EE2478979408E3233310A	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Complete subject DN: CN = Ericsson NL Individual CA v4, O = Ericsson, C = SE	SHA-256 fingerprint of the certificate: 800707B1F57FCDF95CFB047B387C6F48142DA885B7DC1FED28C5F87F0C712AD4 Note: This CA has not issued certificates after 2023-08-31.	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN = Ericsson NL Individual CA v4, O = Ericsson, C = SE	SHA-256 fingerprint of the certificate: EE0343093DF71E364606100164C62A4FB8C4A0F32B1EB47860FFD6C17E94CA54	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP

Table 4: Sub-CA's issued by the Root-CA 2 or its Sub-CA's in scope of the audit.

Appendix C – Locations

#	Country	City	Type
1	Finland	Helsinki	Operational management of the CA
2	Finland	Helsinki	Datacenter 1, Hosting of infrastructure and CA issuing systems
3	Finland	Helsinki	Datacenter 2, Hosting of infrastructure and CA issuing systems
4	Sweden	Stockholm	Operational management of the CA
5	Sweden	Handen	Datacenter

Appendix D – Publicly disclosed incidents

#	Disclosure	Publicly Disclosed Link
1	Bug 1859314, Telia: TLS certificates issued in violation of TLS BR v2.0.1	https://bugzilla.mozilla.org/show_bug.cgi?id=1859314.
2	Bug 1856591, Telia: S/MIME certificates issued in violation of S/MIME BR v1.0.1	https://bugzilla.mozilla.org/show_bug.cgi?id=1856591.

Appendix E – Legal entities operating the CA services

#	Name	Location
1	Telia Company AB	Sweden
2	Telia Finland Oyj	Finland
3	Cygate AB	Sweden