Standard Audit Attestation for

Telia Company AB

Reference: DSC.1257-4

"Bremen, 2024-12-13"

To whom it may concern,

This is to confirm that "datenschutz cert GmbH" has audited the CAs of the "Telia Company AB" without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number "DSC.1257-4" covers multiple Root-CAs and consists of 41 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

datenschutz cert GmbH
Konsul-Smidt-Straße 88a
28217 Bremen, Germany
E-Mail: office@datenschutz-cert.de
Phone: +49 421 69 66 32 550

With best regards,

Dr. Alvils Švēde
Lead Auditor

Dr. Sönke Maseberg
Reviewer

This attestation is based on the template version 3.3 as of 2024-10-08, that was approved for use by ACAB-c.

General audit information

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor
• datenschutz cert GmbH, Konsul-Smidt-Straße 88a, 28217 Bremen, Germany, registered under HRB 26787 HB at Amtsgericht Bremen • Accredited by Deutsche Akkreditierungsstelle GmbH under registration https://www.dakks.de/files/data/as/pdf/D-ZE-16077-01-00.pdf[1] for the certification of trust services according to “EN ISO/IEC 17065:2012” and “ETSI EN 319 403 V2.2.2 (2015-08)” / “ETSI EN 319 403-1 V2.3.1 (2020-06)”. • Insurance Carrier (BRG section 8.2): ERGO Versicherung AG • Third-party affiliate audit firms involved in the audit: None.
Identification and qualification of the audit team
• Number of team members: 3 • Academic qualifications of team members: All team members have formal academic qualifications or professional training or extensive experience indicating general capability to carry out audits based on the knowledge given below and at least four years full time practical workplace experience in information technology, of which at least two years have been in a role or function relating to relevant trust services, public key infrastructure, information security including risk assessment/management, network security and physical security. • Additional competences of team members: • All team members have knowledge of 1) audit principles, practices and techniques in the field of CA/TSP audits gained in a training course of at least five days; 2) the issues related to various areas of trust services, public key infrastructure, information security including risk assessment/management, network security and physical security; 3) the applicable standards, publicly available specifications and regulatory requirements for CA/TSPs and other relevant publicly available specifications including standards for IT product evaluation; and 4) the Conformity Assessment Body's processes. Furthermore, all team members have language skills appropriate for all organizational levels within the CA/TSP organization; note-taking, report-writing, presentation, and interviewing skills; and relevant personal attributes: objective, mature, discerning, analytical, persistent and realistic. • Professional training of team members: See “Additional competences of team members” above. Apart from that are all team members trained to demonstrate adequate competence in: a) knowledge of the CA/TSP standards and other relevant publicly available specifications; b) understanding functioning of trust services and information security including network security issues; c) understanding of risk assessment and risk management from the business perspective; d) technical knowledge of the activity to be audited;

[1] URL to the accreditation certificate hosted by the national accreditation body

e) general knowledge of regulatory requirements relevant to TSPs; and f) knowledge of security policies and controls. • Types of professional experience and practical audit experience: The CAB ensures, that its personnel performing audits maintains competence on the basis of appropriate education, training or experience; that all relevant experience is current and prior to assuming responsibility for performing as an auditor, the candidate has gained experience in the entire process of CA/TSP auditing. This experience shall have been gained by participating under supervision of lead auditors in a minimum of four TSP audits for a total of at least 20 days, including documentation review, on-site audit and audit reporting. • Additional qualification and experience Lead Auditor: On top of what is required for team members (see above), the Lead Auditor a) has acted as auditor in at least three complete TSP audits; b) has adequate knowledge and attributes to manage the audit process; and c) has the competence to communicate effectively, both orally and in writing. • Special skills or qualifications employed throughout audit: None. • Special Credentials, Designations, or Certifications: All members are qualified and registered assessors within the accredited CAB. <<< add info if necessary for this audit or delete this text >>> • Auditors code of conduct incl. independence statement: Code of Conduct as of Annex A, ETSI EN 319 403 or ETSI EN 319 403-1 respectively.
Identification and qualification of the reviewer performing audit quality management
• Number of Reviewers/Audit Quality Managers involved independent from the audit team: 1 • The reviewer fulfils the requirements as described for the Audit Team Members above and has acted as an auditor in at least three complete CA/TSP audits.

Identification of the CA / Trust Service Provider (TSP):	Telia Company AB, Stjärntorget 1, 16994 Solna, Sweden, registered under 556103-4249

Type of audit:	☐ Point in time audit ☐ Period of time, after x month of CA operation ☒ Period of time, full audit
Audit period covered for all policies:	2023-11-01 to 2024-10-31
Point in time date:	none, as audit was a period of time audit
Audit dates:	2024-11-12 to 2024-11-14 (on site)
Audit location:	Helsinki, Finland Solna, Sweden

Root 1: TeliaSonera Root CA v1

Standards considered:	European Standards: • ETSI TS 119 411-6 V1.1.1 (2023-08) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.1 (2024-06) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, Version 2.0.8 • Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.6 • Network and Certificate System Security Requirements, version 1.7 Browser Policy Requirements: • Mozilla Root Store Policy, Version 2.9, 2023-09-01 • Apple Root Certificate Program, 2023-08-15 • Chrome Root Program Policy, Version 1.5, 2024-01-16 • Microsoft Trusted Root Program, 2024-10-29 For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403 V2.2.2 (2015-08) • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.3.1 (2023-03)

The audit was based on the following policy and practice statement documents of the CA / TSP:

- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.0, effective date: 2023-06-29
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.1, effective date: 2023-11-07
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.2, effective date: 2023-12-08
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.3, effective date: 2024-02-05
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.4, effective date: 2024-03-22
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.5, effective date: 2024-04-30
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.6, effective date: 2024-06-14
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.7, effective date: 2024-10-04
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 3.8, effective date: 2023-08-31

- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 3.9, effective date: 2023-11-07
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.0, effective date: 2023-12-08
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.1, effective date: 2024-03-22
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.2, effective date: 2024-04-30
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.3, effective date: 2024-06-14
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.4, effective date: 2024-09-18
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.5, effective date: 2024-10-14

In the following areas, non-conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:

7.7 Operation security

Test documentation for Cygate secure mail, and software acceptance process shall be improved. [REQ-7.7-03, REQ-7.7-04]

Findings with regard to ETSI EN 319 411-1:

6.6.3 OCSP profile

OCSP service monitoring shall be improved. [OVR-6.6.3-03]

6.3.12 Key escrow and recovery

The security of any duplicated subject's private keys shall be improved. [SDP-6.3.12-02]

All major non-conformities have been closed before the issuance of this attestation. For all minor non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.
Clarification: No major non-conformities detected during the audit, see also page 1 of this AL.

This Audit Attestation also covers the following incidents as described in the following.

- Bug 1896108, Telia: Certificates Issued with lower case value in subject:countryName
  https://bugzilla.mozilla.org/show_bug.cgi?id=1896108
- 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
- Bug 1859314, Telia: TLS certificates issued in violation of TLS BR v2.0.1
  https://bugzilla.mozilla.org/show_bug.cgi?id=1859314
- Bug 1920659, Telia: S/MIME Certificate issued to expired domain
  https://bugzilla.mozilla.org/show_bug.cgi?id=1920659

- Bug 1896553, Telia: Delayed revocation of seven (7) certificates related to incident 1896108
  https://bugzilla.mozilla.org/show_bug.cgi?id=1896553

The remediation measures taken by Telia Company AB as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident.

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	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP, LCP
Note: Cross Certified Subordinate CA Certificate.		
Complete subject DN: CN=TeliaSonera Server CA v2, O=TeliaSonera, C=FI	SHA-256 fingerprint of the certificate: D721110388CA6F20BBA9FD1A8DBA4EFB8C16392A3DEBAD97C553EEAF0ACACAAC	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP, OVCP, LCP
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.		
Complete subject DN: CN=Telia Domain Validation CA v2, O=Telia Finland Oyj, C=FI	SHA-256 fingerprint of the certificate: 5B312B7E11B70D07C14E0AB99F08D00748966098C52AA85A06A0822BBE59A02C	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP, DVCP, LCP
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.		
Complete subject DN: CN=TeliaSonera Class 1 CA v2, O=TeliaSonera, C=FI	SHA-256 fingerprint of the certificate: B95AE54F838E3ABF0B57ACCC1B1266DC68C7A3FA774015FA128D60CDD1AAE280	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP, LCP
Note: This CA has not been used for TLS issuance during the audit period.		

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN=TeliaSonera Class 1 CA v2, O=TeliaSonera, 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, LCP
Complete subject DN: CN=TeliaSonera Class 2 CA v2, O=TeliaSonera, C=SE	SHA-256 fingerprint of the certificate: 092829433D231949F4A9BC666CBF54B3AA27D7BEBCA048D75E59093E15A72EA5	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP, LCP
Note: This CA has not been used for TLS issuance during the audit period.		
Complete subject DN: CN=TeliaSonera Class 2 CA v2, O=TeliaSonera, 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, LCP
Complete subject DN: CN=TeliaSonera Email CA v4, O=TeliaSonera, C=SE	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, LCP
Note: This CA has not been used for TLS issuance during the audit period.		
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
Note: This CA has not been used for issuance during the audit period.		
Complete subject DN: CN = Ericsson NL Individual CA v3, O = Ericsson, C = SE	SHA-256 fingerprint of the certificate: 63ED95B17FFDCB7AE30FEAC6A874653099264E21B268D836D957966F0B04BE43	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Note: This CA has not been used for issuance during the audit period.		
Complete subject DN: CN = Telia Class 3 CA v2, O = Telia Company AB, C = SE	SHA-256 fingerprint of the certificate: 5E343F2432BBF0ECC7062F4237110581DFFD638CC3689D50D5864174C9DC011D	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Note: This CA has not been used for issuance during the audit period.		

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN=Telia Class 3 CA v3, O=Telia Company AB, C=SE	SHA-256 fingerprint of the certificate: D20E08A8F9E16DF94A4CD7E052B382C339880B47931B78CC7DF404C063E49852	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

Root 2: Telia Root CA v2

Standards considered:	European Standards: • ETSI TS 119 411-6 V1.1.1 (2023-08) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.1 (2024-06) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, Version 2.0.8 • Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.6 • Network and Certificate System Security Requirements, version 1.7 Browser Policy Requirements: • Mozilla Root Store Policy, Version 2.9, 2023-09-01 • Apple Root Certificate Program, 2023-08-15 • Chrome Root Program Policy, Version 1.5, 2024-01-16 • Microsoft Trusted Root Program, 2024-10-29 For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403 V2.2.2 (2015-08) • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.3.1 (2023-03)

The audit was based on the following policy and practice statement documents of the CA / TSP:

- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.0, effective date: 2023-06-29
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.1, effective date: 2023-11-07
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.2, effective date: 2023-12-08
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.3, effective date: 2024-02-05
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.4, effective date: 2024-03-22
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.5, effective date: 2024-04-30
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.6, effective date: 2024-06-14
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.7, effective date: 2024-10-04
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 3.8, effective date: 2023-08-31

- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 3.9, effective date: 2023-11-07
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.0, effective date: 2023-12-08
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.1, effective date: 2024-03-22
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.2, effective date: 2024-04-30
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.3, effective date: 2024-06-14
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.4, effective date: 2024-09-18
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.5, effective date: 2024-10-14

In the following areas, non-conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:
7.7 Operation security
Test documentation for Cygate secure mail, and software acceptance process shall be improved. [REQ-7.7-03, REQ-7.7-04]

Findings with regard to ETSI EN 319 411-1:
6.6.3 OCSP profile
OCSP service monitoring shall be improved. [OVR-6.6.3-03]
6.3.12 Key escrow and recovery
The security of any duplicated subject's private keys shall be improved. [SDP-6.3.12-02]

All major non-conformities have been closed before the issuance of this attestation. For all minor non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.
Clarification: No major non-conformities detected during the audit, see also page 1 of this AL.

This Audit Attestation also covers the following incidents as described in the following.

- Bug 1896108, Telia: Certificates Issued with lower case value in subject:countryName
  https://bugzilla.mozilla.org/show_bug.cgi?id=1896108
- 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
- Bug 1859314, Telia: TLS certificates issued in violation of TLS BR v2.0.1
  https://bugzilla.mozilla.org/show_bug.cgi?id=1859314
- Bug 1920659, Telia: S/MIME Certificate issued to expired domain
  https://bugzilla.mozilla.org/show_bug.cgi?id=1920659

- Bug 1896553, Telia: Delayed revocation of seven (7) certificates related to incident 1896108
  https://bugzilla.mozilla.org/show_bug.cgi?id=1896553

The remediation measures taken by Telia Company AB as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident.

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, LCP
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, LCP
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
Complete subject DN: CN = Telia Class 1 CA v3, O = Telia Finland Oyj, C = FI	SHA-256 fingerprint of the certificate: 2E459B4B2F4C24D3BCF6D357E21DC74286C889104888267E2BACA75C78D1A615	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Note: This CA has not issued certificates after 2023-08-31.		

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: 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	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Note: This CA has not issued certificates after 2023-08-31.		
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	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Note: This CA has not issued certificates after 2023-08-31.		
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	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Note: This CA has not issued certificates after 2023-08-31.		
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

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN=Telia RSA TLS Root CA v3, O=Telia Company AB, C=SE	SHA-256 fingerprint of the certificate: 6DD4E12B751849BA3E1AD90AC48674C2474C772182F3500C85C2DF4DB7F48866	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP, LCP
Note: Cross Certified Subordinate CA Certificate.		
Complete subject DN: CN=Telia RSA Email Root CA v3, O=Telia Company AB, C=SE	SHA-256 fingerprint of the certificate: D46F8990078A9B2AE08F3C50E9CB1A07373D574003A66BB72EC3A99CBE2A3382	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Note: Cross Certified Subordinate CA Certificate.		
Complete subject DN: CN=Telia RSA Client Root CA v3, O=Telia Company AB, C=SE	SHA-256 fingerprint of the certificate: 81B837B929D1E854DFE8A368F264C6E7D928CA1E4A205BA258E17A0C7516E2F1	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Note: Cross Certified Subordinate CA Certificate.		
Complete subject DN: CN=Telia RSA Signing Root CA v3, O=Telia Company AB, C=SE	SHA-256 fingerprint of the certificate: 8CEF3433AB3C3F4A3C5D395B82B4EAA250E9BF647BC6095ECF0B57620F5DA9BF	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Note: Cross Certified Subordinate CA Certificate.		
Complete subject DN: CN=Telia EC TLS Root CA v3, O=Telia Company AB, C=SE	SHA-256 fingerprint of the certificate: 07E5866107E24AE69A9679668F916AA1B3B39DC3554781E3AE9ABAA44B5A7BC4	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP, LCP
Note: Cross Certified Subordinate CA Certificate.		
Complete subject DN: CN=Telia EC Email Root CA v3, O=Telia Company AB, C=SE	SHA-256 fingerprint of the certificate: 18C2FC38AFD8E668A89A6FC1E8A924C8D5C6BD1A70089FDDE56361CDA92EF445	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Note: Cross Certified Subordinate CA Certificate.		

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN=Telia EC Client Root CA v3, O=Telia Company AB, C=SE	SHA-256 fingerprint of the certificate: 708E7E73BC638B90F14bAAB634B5CBFBF8FFE1BD1B24B1744612E49167CA7731	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Note: Cross Certified Subordinate CA Certificate.		
Complete subject DN: CN=Telia EC Signing Root CA v3, O=Telia Company AB, C=SE	SHA-256 fingerprint of the certificate: 622F1C188A0E818C222E9A5674980D6E77197E580FC476C6F741DC0606FF538A	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Note: Cross Certified Subordinate CA Certificate.		

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

Root 3: Telia RSA TLS Root CA v3

Standards considered:	European Standards: • ETSI TS 119 411-6 V1.1.1 (2023-08) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.1 (2024-06) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, Version 2.0.8 • Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.6 • Network and Certificate System Security Requirements, version 1.7 Browser Policy Requirements: • Mozilla Root Store Policy, Version 2.9, 2023-09-01 • Apple Root Certificate Program, 2023-08-15 • Chrome Root Program Policy, Version 1.5, 2024-01-16 • Microsoft Trusted Root Program, 2024-10-29 For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403 V2.2.2 (2015-08) • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.3.1 (2023-03)

The audit was based on the following policy and practice statement documents of the CA / TSP:

- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.2, effective date: 2023-12-08
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.3, effective date: 2024-02-05
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.4, effective date: 2024-03-22
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.5, effective date: 2024-04-30
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.6, effective date: 2024-06-14
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.7, effective date: 2024-10-04
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.0, effective date: 2023-12-08
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.1, effective date: 2024-03-22
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.2, effective date: 2024-04-30

- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.3, effective date: 2024-06-14
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.4, effective date: 2024-09-18
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.5, effective date: 2024-10-14

In the following areas, non-conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:
7.7 Operation security
Test documentation for Cygate secure mail, and software acceptance process shall be improved. [REQ-7.7-03, REQ-7.7-04]

Findings with regard to ETSI EN 319 411-1:
6.6.3 OCSP profile
OCSP service monitoring shall be improved. [OVR-6.6.3-03]
6.3.12 Key escrow and recovery
The security of any duplicated subject's private keys shall be improved. [SDP-6.3.12-02]

All major non-conformities have been closed before the issuance of this attestation. For all minor non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.
Clarification: No major non-conformities detected during the audit, see also page 1 of this AL.

This Audit Attestation also covers the following incidents as described in the following.
- Bug 1896108, Telia: Certificates Issued with lower case value in subject:countryName
  https://bugzilla.mozilla.org/show_bug.cgi?id=1896108
- 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
- Bug 1859314, Telia: TLS certificates issued in violation of TLS BR v2.0.1
  https://bugzilla.mozilla.org/show_bug.cgi?id=1859314
- Bug 1920659, Telia: S/MIME Certificate issued to expired domain
  https://bugzilla.mozilla.org/show_bug.cgi?id=1920659
- Bug 1896553, Telia: Delayed revocation of seven (7) certificates related to incident 1896108
  https://bugzilla.mozilla.org/show_bug.cgi?id=1896553

The remediation measures taken by Telia Company AB as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident.

These are Telia CA’s new root CA and subordinate CA certificates that are first time in audit and not yet included in any Root program.

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN=Telia RSA TLS Root CA v3, O=Telia Company AB, C=SE	SHA-256 fingerprint of the certificate: D13DB1294C45EBC6FC86C6BBF69FA29BDFE692DFF7C713C243C7A956C6A2284C	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP

Table 5: Root-CA 3 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 RSA DV CA v4, O = Telia Company AB, C = SE	SHA-256 fingerprint of the certificate: A67F3E67CB1DF2EACF3A404EAFF179374E5E3F4BA0D82E91405DAEADFB0F337D	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP, DVCP, LCP
Note: This CA has been used only to issue required test certificates for the new TLS root.		
Complete subject DN: CN = Telia RSA OV CA v4, O = Telia Company AB, C = SE	SHA-256 fingerprint of the certificate: F07D383827E264326C5D0DBE257AA82108409F25246F81EE36C8AF222B5A1E43	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP, OVCP, LCP
Note: This CA has been used only to issue required test certificates for the new TLS root.		

Table 6: Sub-CA’s issued by the Root-CA 3 or its Sub-CA’s in scope of the audit

Root 4: Telia RSA Email Root CA v3

Standards considered:	European Standards: • ETSI TS 119 411-6 V1.1.1 (2023-08) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.1 (2024-06) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, Version 2.0.8 • Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.6 • Network and Certificate System Security Requirements, version 1.7 Browser Policy Requirements: • Mozilla Root Store Policy, Version 2.9, 2023-09-01 • Apple Root Certificate Program, 2023-08-15 • Chrome Root Program Policy, Version 1.5, 2024-01-16 • Microsoft Trusted Root Program, 2024-10-29 For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403 V2.2.2 (2015-08) • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.3.1 (2023-03)

The audit was based on the following policy and practice statement documents of the CA / TSP:

- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.2, effective date: 2023-12-08
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.3, effective date: 2024-02-05
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.4, effective date: 2024-03-22
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.5, effective date: 2024-04-30
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.6, effective date: 2024-06-14
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.7, effective date: 2024-10-04
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.0, effective date: 2023-12-08
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.1, effective date: 2024-03-22
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.2, effective date: 2024-04-30

- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.3, effective date: 2024-06-14
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.4, effective date: 2024-09-18
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.5, effective date: 2024-10-14

In the following areas, non-conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:
7.7 Operation security
Test documentation for Cygate secure mail, and software acceptance process shall be improved. [REQ-7.7-03, REQ-7.7-04]

Findings with regard to ETSI EN 319 411-1:
6.6.3 OCSP profile
OCSP service monitoring shall be improved. [OVR-6.6.3-03]
6.3.12 Key escrow and recovery
The security of any duplicated subject's private keys shall be improved. [SDP-6.3.12-02]

All major non-conformities have been closed before the issuance of this attestation. For all minor non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.
Clarification: No major non-conformities detected during the audit, see also page 1 of this AL.

This Audit Attestation also covers the following incidents as described in the following.

- Bug 1896108, Telia: Certificates Issued with lower case value in subject:countryName
  https://bugzilla.mozilla.org/show_bug.cgi?id=1896108
- 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
- Bug 1859314, Telia: TLS certificates issued in violation of TLS BR v2.0.1
  https://bugzilla.mozilla.org/show_bug.cgi?id=1859314
- Bug 1920659, Telia: S/MIME Certificate issued to expired domain
  https://bugzilla.mozilla.org/show_bug.cgi?id=1920659
- Bug 1896553, Telia: Delayed revocation of seven (7) certificates related to incident 1896108
  https://bugzilla.mozilla.org/show_bug.cgi?id=1896553

The remediation measures taken by Telia Company AB as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident.

These are Telia CA’s new root CA and subordinate CA certificates that are first time in audit and not yet included in any Root program.

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN=Telia RSA Email Root CA v3, O=Telia Company AB, C=SE	SHA-256 fingerprint of the certificate: 5B0C502A7D963BA55217396FDA9B3DC78171000AEEFF42CECC3A20A7938163E8	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP

Table 7: Root-CA 4 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 RSA Email CA v6, O = Telia Company AB, C = SE	SHA-256 fingerprint of the certificate: BD6E7EDCEBE62E4571F180001568F861DE2AA7AF6D98E7C338D426F54123785B	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Note: This CA has not issued certificates during the audit period.		
Complete subject DN: CN = Ericsson NL Individual CA v5, O = Ericsson AB, C = SE	SHA-256 fingerprint of the certificate: B974D221C073DF439FE2918845D9783D7E4762C5A9D777DF2DECCBDBDCC1C1CC	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Note: This CA has not issued certificates during the audit period.		

Table 8: Sub-CA’s issued by the Root-CA 4 or its Sub-CA’s in scope of the audit

Root 5: Telia RSA Client Root CA v3

Standards considered:	European Standards: • ETSI TS 119 411-6 V1.1.1 (2023-08) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.1 (2024-06) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, Version 2.0.8 • Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.6 • Network and Certificate System Security Requirements, version 1.7 Browser Policy Requirements: • Mozilla Root Store Policy, Version 2.9, 2023-09-01 • Apple Root Certificate Program, 2023-08-15 • Chrome Root Program Policy, Version 1.5, 2024-01-16 • Microsoft Trusted Root Program, 2024-10-29 For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403 V2.2.2 (2015-08) • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.3.1 (2023-03)

The audit was based on the following policy and practice statement documents of the CA / TSP:

- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.2, effective date: 2023-12-08
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.3, effective date: 2024-02-05
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.4, effective date: 2024-03-22
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.5, effective date: 2024-04-30
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.6, effective date: 2024-06-14
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.7, effective date: 2024-10-04
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.0, effective date: 2023-12-08
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.1, effective date: 2024-03-22
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.2, effective date: 2024-04-30

- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.3, effective date: 2024-06-14
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.4, effective date: 2024-09-18
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.5, effective date: 2024-10-14

In the following areas, non-conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:
7.7 Operation security
Test documentation for Cygate secure mail, and software acceptance process shall be improved. [REQ-7.7-03, REQ-7.7-04]

Findings with regard to ETSI EN 319 411-1:
6.6.3 OCSP profile
OCSP service monitoring shall be improved. [OVR-6.6.3-03]
6.3.12 Key escrow and recovery
The security of any duplicated subject's private keys shall be improved. [SDP-6.3.12-02]

All major non-conformities have been closed before the issuance of this attestation. For all minor non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.
Clarification: No major non-conformities detected during the audit, see also page 1 of this AL.

This Audit Attestation also covers the following incidents as described in the following.

- Bug 1896108, Telia: Certificates Issued with lower case value in subject:countryName
  https://bugzilla.mozilla.org/show_bug.cgi?id=1896108
- 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
- Bug 1859314, Telia: TLS certificates issued in violation of TLS BR v2.0.1
  https://bugzilla.mozilla.org/show_bug.cgi?id=1859314
- Bug 1920659, Telia: S/MIME Certificate issued to expired domain
  https://bugzilla.mozilla.org/show_bug.cgi?id=1920659
- Bug 1896553, Telia: Delayed revocation of seven (7) certificates related to incident 1896108
  https://bugzilla.mozilla.org/show_bug.cgi?id=1896553

The remediation measures taken by Telia Company AB as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident.

These are Telia CA’s new root CA and subordinate CA certificates that are first time in audit and not yet included in any Root program.

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN=Telia RSA Client Root CA v3, O=Telia Company AB, C=SE	SHA-256 fingerprint of the certificate: 6485F6E060934AF413EC54B9C65F87BD231929ECFA11DE522BAD8DC64F001571	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP

Table 9: Root-CA 5 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 RSA Client 1 CA v4, O = Telia Company AB, C = SE	SHA-256 fingerprint of the certificate: 814EB66B02E73A4DA67FCC6099246C264E610B48AAD08ED0A22D705FABC717E0	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Note: This CA has not issued certificates during the audit period.		
Complete subject DN: CN = Telia RSA Client 2 CA v4, O = Telia Company AB, C = SE	SHA-256 fingerprint of the certificate: 1F520582132CD60D8566B8F14D0502A26456BB2E3B9811AAAEE768CCF51774CB	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Note: This CA has not issued certificates during the audit period.		
Complete subject DN: CN = Telia RSA Client 3 CA v4, O = Telia Company AB, C = SE	SHA-256 fingerprint of the certificate: 945DF0B4A36132746BBA9310841461B4FE42BA05ED35DA0405B5FDBA750F560D	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP
Note: This CA has not issued certificates during the audit period.		

Table 10: Sub-CA’s issued by the Root-CA 5 or its Sub-CA’s in scope of the audit

Root 6: Telia RSA Signing Root CA v3

Standards considered:	European Standards: • ETSI TS 119 411-6 V1.1.1 (2023-08) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.1 (2024-06) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, Version 2.0.8 • Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.6 • Network and Certificate System Security Requirements, version 1.7 Browser Policy Requirements: • Mozilla Root Store Policy, Version 2.9, 2023-09-01 • Apple Root Certificate Program, 2023-08-15 • Chrome Root Program Policy, Version 1.5, 2024-01-16 • Microsoft Trusted Root Program, 2024-10-29 For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403 V2.2.2 (2015-08) • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.3.1 (2023-03)

The audit was based on the following policy and practice statement documents of the CA / TSP:

- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.2, effective date: 2023-12-08
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.3, effective date: 2024-02-05
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.4, effective date: 2024-03-22
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.5, effective date: 2024-04-30
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.6, effective date: 2024-06-14
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.7, effective date: 2024-10-04
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.0, effective date: 2023-12-08
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.1, effective date: 2024-03-22
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.2, effective date: 2024-04-30

- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.3, effective date: 2024-06-14
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.4, effective date: 2024-09-18
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.5, effective date: 2024-10-14

In the following areas, non-conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:
7.7 Operation security
Test documentation for Cygate secure mail, and software acceptance process shall be improved. [REQ-7.7-03, REQ-7.7-04]

Findings with regard to ETSI EN 319 411-1:
6.6.3 OCSP profile
OCSP service monitoring shall be improved. [OVR-6.6.3-03]
6.3.12 Key escrow and recovery
The security of any duplicated subject's private keys shall be improved. [SDP-6.3.12-02]

All major non-conformities have been closed before the issuance of this attestation. For all minor non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.
Clarification: No major non-conformities detected during the audit, see also page 1 of this AL.

This Audit Attestation also covers the following incidents as described in the following.

- Bug 1896108, Telia: Certificates Issued with lower case value in subject:countryName
  https://bugzilla.mozilla.org/show_bug.cgi?id=1896108
- 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
- Bug 1859314, Telia: TLS certificates issued in violation of TLS BR v2.0.1
  https://bugzilla.mozilla.org/show_bug.cgi?id=1859314
- Bug 1920659, Telia: S/MIME Certificate issued to expired domain
  https://bugzilla.mozilla.org/show_bug.cgi?id=1920659
- Bug 1896553, Telia: Delayed revocation of seven (7) certificates related to incident 1896108
  https://bugzilla.mozilla.org/show_bug.cgi?id=1896553

The remediation measures taken by Telia Company AB as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident.

These are Telia CA’s new root CA and subordinate CA certificates that are first time in audit and not yet included in any Root program.

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN=Telia RSA Signing Root CA v3, O=Telia Company AB, C=SE	SHA-256 fingerprint of the certificate: C2FB44D8DEF85126D84FC41FBE667BC811F0D633411CAC26D13FBD95EA5BE603	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP

Table 11: Root-CA 6 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 RSA qSeal CA v4, O = Telia Company AB, organizationIdentifier = NTRSE-556103-4249, C = SE	SHA-256 fingerprint of the certificate: 709F4003B93F46F1653B76728C9EDE739DAD5095FBE87A80362A856BC840B96A	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP, DVCP
Note: This CA has not issued certificates during the audit period.		

Table 12: Sub-CA’s issued by the Root-CA 6 or its Sub-CA’s in scope of the audit

Root 7: Telia EC TLS Root CA v3

Standards considered:	European Standards: • ETSI TS 119 411-6 V1.1.1 (2023-08) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.1 (2024-06) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, Version 2.0.8 • Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.6 • Network and Certificate System Security Requirements, version 1.7 Browser Policy Requirements: • Mozilla Root Store Policy, Version 2.9, 2023-09-01 • Apple Root Certificate Program, 2023-08-15 • Chrome Root Program Policy, Version 1.5, 2024-01-16 • Microsoft Trusted Root Program, 2024-10-29 For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403 V2.2.2 (2015-08) • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.3.1 (2023-03)

The audit was based on the following policy and practice statement documents of the CA / TSP:

- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.2, effective date: 2023-12-08
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.3, effective date: 2024-02-05
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.4, effective date: 2024-03-22
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.5, effective date: 2024-04-30
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.6, effective date: 2024-06-14
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.7, effective date: 2024-10-04
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.0, effective date: 2023-12-08
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.1, effective date: 2024-03-22
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.2, effective date: 2024-04-30

- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.3, effective date: 2024-06-14
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.4, effective date: 2024-09-18
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.5, effective date: 2024-10-14

In the following areas, non-conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:
7.7 Operation security
Test documentation for Cygate secure mail, and software acceptance process shall be improved. [REQ-7.7-03, REQ-7.7-04]

Findings with regard to ETSI EN 319 411-1:
6.6.3 OCSP profile
OCSP service monitoring shall be improved. [OVR-6.6.3-03]
6.3.12 Key escrow and recovery
The security of any duplicated subject's private keys shall be improved. [SDP-6.3.12-02]

All major non-conformities have been closed before the issuance of this attestation. For all minor non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.
Clarification: No major non-conformities detected during the audit, see also page 1 of this AL.

This Audit Attestation also covers the following incidents as described in the following.
- Bug 1896108, Telia: Certificates Issued with lower case value in subject:countryName
  https://bugzilla.mozilla.org/show_bug.cgi?id=1896108
- 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
- Bug 1859314, Telia: TLS certificates issued in violation of TLS BR v2.0.1
  https://bugzilla.mozilla.org/show_bug.cgi?id=1859314
- Bug 1920659, Telia: S/MIME Certificate issued to expired domain
  https://bugzilla.mozilla.org/show_bug.cgi?id=1920659
- Bug 1896553, Telia: Delayed revocation of seven (7) certificates related to incident 1896108
  https://bugzilla.mozilla.org/show_bug.cgi?id=1896553

The remediation measures taken by Telia Company AB as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident.

These are Telia CA’s new root CA and subordinate CA certificates that are first time in audit and not yet included in any Root program.

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN=Telia EC TLS Root CA v3, O=Telia Company AB, C=SE	SHA-256 fingerprint of the certificate: 098E08A91DBBF77478B96CCEB89B1413A5DA37B7C862606A955DEB07179F4326	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP

Table 13: Root-CA 7 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 EC DV CA v4, O = Telia Company AB, C = SE	SHA-256 fingerprint of the certificate: 26D742741BA428394F904E4410ED6DA92F4D0C55521F1EDE2B29797F866C955C	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP, DVCP, LCP
Note: This CA has been used only to issue required test certificates for the new TLS root.		

Table 14: Sub-CA’s issued by the Root-CA 7 or its Sub-CA’s in scope of the audit

Root 8: Telia EC Email Root CA v3

Standards considered:	European Standards: • ETSI TS 119 411-6 V1.1.1 (2023-08) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.1 (2024-06) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, Version 2.0.8 • Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.6 • Network and Certificate System Security Requirements, version 1.7 Browser Policy Requirements: • Mozilla Root Store Policy, Version 2.9, 2023-09-01 • Apple Root Certificate Program, 2023-08-15 • Chrome Root Program Policy, Version 1.5, 2024-01-16 • Microsoft Trusted Root Program, 2024-10-29 For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403 V2.2.2 (2015-08) • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.3.1 (2023-03)

The audit was based on the following policy and practice statement documents of the CA / TSP:

- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.2, effective date: 2023-12-08
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.3, effective date: 2024-02-05
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.4, effective date: 2024-03-22
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.5, effective date: 2024-04-30
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.6, effective date: 2024-06-14
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.7, effective date: 2024-10-04
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.0, effective date: 2023-12-08
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.1, effective date: 2024-03-22
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.2, effective date: 2024-04-30

- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.3, effective date: 2024-06-14
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.4, effective date: 2024-09-18
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.5, effective date: 2024-10-14

In the following areas, non-conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:
7.7 Operation security
Test documentation for Cygate secure mail, and software acceptance process shall be improved. [REQ-7.7-03, REQ-7.7-04]

Findings with regard to ETSI EN 319 411-1:
6.6.3 OCSP profile
OCSP service monitoring shall be improved. [OVR-6.6.3-03]
6.3.12 Key escrow and recovery
The security of any duplicated subject's private keys shall be improved. [SDP-6.3.12-02]

All major non-conformities have been closed before the issuance of this attestation. For all minor non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.
Clarification: No major non-conformities detected during the audit, see also page 1 of this AL.

This Audit Attestation also covers the following incidents as described in the following.

- Bug 1896108, Telia: Certificates Issued with lower case value in subject:countryName
  https://bugzilla.mozilla.org/show_bug.cgi?id=1896108
- 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
- Bug 1859314, Telia: TLS certificates issued in violation of TLS BR v2.0.1
  https://bugzilla.mozilla.org/show_bug.cgi?id=1859314
- Bug 1920659, Telia: S/MIME Certificate issued to expired domain
  https://bugzilla.mozilla.org/show_bug.cgi?id=1920659
- Bug 1896553, Telia: Delayed revocation of seven (7) certificates related to incident 1896108
  https://bugzilla.mozilla.org/show_bug.cgi?id=1896553

The remediation measures taken by Telia Company AB as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident.

This is a Telia CA’s new root CA certificate that are first time in audit and not yet included in any Root program.

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN=Telia EC Email Root CA v3, O=Telia Company AB, C=SE	SHA-256 fingerprint of the certificate: 3682228D7D678B571440CF1CB34E69FB4135FD6C2A1BE38E14163B711E02AE01	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP

Table 15: Root-CA 8 in scope of the audit

No Sub-CAs have been issued by the aforementioned Root-CA during the audit period.

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN:	SHA-256 fingerprint of the certificate:	ETSI EN policy that this Intermediate CA has been assessed against:

Table 16: Sub-CA’s issued by the Root-CA 8 or its Sub-CA’s in scope of the audit

Root 9: Telia EC Client Root CA v3

Standards considered:	European Standards: • ETSI TS 119 411-6 V1.1.1 (2023-08) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.1 (2024-06) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, Version 2.0.8 • Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.6 • Network and Certificate System Security Requirements, version 1.7 Browser Policy Requirements: • Mozilla Root Store Policy, Version 2.9, 2023-09-01 • Apple Root Certificate Program, 2023-08-15 • Chrome Root Program Policy, Version 1.5, 2024-01-16 • Microsoft Trusted Root Program, 2024-10-29 For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403 V2.2.2 (2015-08) • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.3.1 (2023-03)

The audit was based on the following policy and practice statement documents of the CA / TSP:

- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.2, effective date: 2023-12-08
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.3, effective date: 2024-02-05
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.4, effective date: 2024-03-22
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.5, effective date: 2024-04-30
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.6, effective date: 2024-06-14
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.7, effective date: 2024-10-04
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.0, effective date: 2023-12-08
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.1, effective date: 2024-03-22
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.2, effective date: 2024-04-30

- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.3, effective date: 2024-06-14
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.4, effective date: 2024-09-18
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.5, effective date: 2024-10-14

In the following areas, non-conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:
7.7 Operation security
Test documentation for Cygate secure mail, and software acceptance process shall be improved. [REQ-7.7-03, REQ-7.7-04]

Findings with regard to ETSI EN 319 411-1:
6.6.3 OCSP profile
OCSP service monitoring shall be improved. [OVR-6.6.3-03]
6.3.12 Key escrow and recovery
The security of any duplicated subject's private keys shall be improved. [SDP-6.3.12-02]

All major non-conformities have been closed before the issuance of this attestation. For all minor non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.
Clarification: No major non-conformities detected during the audit, see also page 1 of this AL.

This Audit Attestation also covers the following incidents as described in the following.

- Bug 1896108, Telia: Certificates Issued with lower case value in subject:countryName
  https://bugzilla.mozilla.org/show_bug.cgi?id=1896108
- 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
- Bug 1859314, Telia: TLS certificates issued in violation of TLS BR v2.0.1
  https://bugzilla.mozilla.org/show_bug.cgi?id=1859314
- Bug 1920659, Telia: S/MIME Certificate issued to expired domain
  https://bugzilla.mozilla.org/show_bug.cgi?id=1920659
- Bug 1896553, Telia: Delayed revocation of seven (7) certificates related to incident 1896108
  https://bugzilla.mozilla.org/show_bug.cgi?id=1896553

The remediation measures taken by Telia Company AB as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident.

This is a Telia CA’s new root CA certificate that are first time in audit and not yet included in any Root program.

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN=Telia EC Client Root CA v3, O=Telia Company AB, C=SE	SHA-256 fingerprint of the certificate: CCF6A7C3881928CFB1DBEBD74EABA50D3BC69633C106274D2C221ECCEE697E87	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP

Table 17: Root-CA 9 in scope of the audit

No Sub-CAs have been issued by the aforementioned Root-CA during the audit period.

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN:	SHA-256 fingerprint of the certificate:	ETSI EN policy that this Intermediate CA has been assessed against:

Table 18: Sub-CA’s issued by the Root-CA 9 or its Sub-CA’s in scope of the audit

Root 10: Telia EC Signing Root CA v3

Standards considered:	European Standards: • ETSI TS 119 411-6 V1.1.1 (2023-08) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.1 (2024-06) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, Version 2.0.8 • Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.6 • Network and Certificate System Security Requirements, version 1.7 Browser Policy Requirements: • Mozilla Root Store Policy, Version 2.9, 2023-09-01 • Apple Root Certificate Program, 2023-08-15 • Chrome Root Program Policy, Version 1.5, 2024-01-16 • Microsoft Trusted Root Program, 2024-10-29 For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403 V2.2.2 (2015-08) • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.3.1 (2023-03)

The audit was based on the following policy and practice statement documents of the CA / TSP:

- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.2, effective date: 2023-12-08
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.3, effective date: 2024-02-05
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.4, effective date: 2024-03-22
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.5, effective date: 2024-04-30
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.6, effective date: 2024-06-14
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Server Certificates, Release 5.7, effective date: 2024-10-04
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.0, effective date: 2023-12-08
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.1, effective date: 2024-03-22
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.2, effective date: 2024-04-30

- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.3, effective date: 2024-06-14
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.4, effective date: 2024-09-18
- Telia Company AB, Certificate Policy and Certification Practice Statement for Telia Client Certificates, Release 4.5, effective date: 2024-10-14

In the following areas, non-conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:
7.7 Operation security
Test documentation for Cygate secure mail, and software acceptance process shall be improved. [REQ-7.7-03, REQ-7.7-04]

Findings with regard to ETSI EN 319 411-1:
6.6.3 OCSP profile
OCSP service monitoring shall be improved. [OVR-6.6.3-03]
6.3.12 Key escrow and recovery
The security of any duplicated subject's private keys shall be improved. [SDP-6.3.12-02]

All major non-conformities have been closed before the issuance of this attestation. For all minor non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.
Clarification: No major non-conformities detected during the audit, see also page 1 of this AL.

This Audit Attestation also covers the following incidents as described in the following.

- Bug 1896108, Telia: Certificates Issued with lower case value in subject:countryName
  https://bugzilla.mozilla.org/show_bug.cgi?id=1896108
- 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
- Bug 1859314, Telia: TLS certificates issued in violation of TLS BR v2.0.1
  https://bugzilla.mozilla.org/show_bug.cgi?id=1859314
- Bug 1920659, Telia: S/MIME Certificate issued to expired domain
  https://bugzilla.mozilla.org/show_bug.cgi?id=1920659
- Bug 1896553, Telia: Delayed revocation of seven (7) certificates related to incident 1896108
  https://bugzilla.mozilla.org/show_bug.cgi?id=1896553

The remediation measures taken by Telia Company AB as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident.

This is a Telia CA’s new root CA certificate that are first time in audit and not yet included in any Root program.

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN=Telia EC Signing Root CA v3, O=Telia Company AB, C=SE	SHA-256 fingerprint of the certificate: 2C4E9B0F8D0FCDC308C077E30DD2349DAF871FB3A37214859C486189A9F80ADB	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP

Table 19: Root-CA 10 in scope of the audit

No Sub-CAs have been issued by the aforementioned Root-CA during the audit period.

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN:	SHA-256 fingerprint of the certificate:	ETSI EN policy that this Intermediate CA has been assessed against:

Table 20: Sub-CA’s issued by the Root-CA 10 or its Sub-CA’s in scope of the audit

Modifications record

Version	Issuing Date	Changes
Version 1	2024-12-03	Initial attestation
Version 1.1	2024-12-06	Hashes and misprints corrected
Version 1.2	2024-12-11	Correction due to ALV test
Version 1.3	2024-12-13	Misprints (version numbers of ETSI standards) corrected, clarification added

End of the audit attestation letter.