SMIME BR Audit Attestation for

Telia Company AB

Reference: DSC.1257-1

"Bremen, 2024-02-14"

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.1257-1" covers multiple Root-CAs and consists of 10 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

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

With best regards,

Dr. Sönke Maseberg
Lead Auditor

Dr. Irene Karper
Reviewer

This attestation is based on the template version 3.1 as of 2023-08-24, 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-Str. 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 “DIN EN ISO/IEC 17065:2013” 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. • 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 2 month of CA operation ☐ Period of time, full audit
Audit period covered for all policies:	2023-09-01 to 2023-10-31
Point in time date:	none, as audit was a period of time audit
Audit dates:	2023-11-01 to 2023-11-02 (on site) 2023-11-08 (on site)
Audit location:	Helsinki, Finland Solna, Sweden Handen, 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 V1.3.1 (2021-05) • ETSI EN 319 401 V2.3.1 (2021-05) CA Browser Forum Requirements: • S/MIME Baseline Requirements, version 1.0.1 Browser Policy Requirements: • Mozilla Root Store Policy, Version 2.9, 2023-09-01 • Apple Root Certificate Program, 2023-08-15 • Microsoft Trusted Root Program, 2023-06-09 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 V1.2.4 (2020-11)

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 Client Certificates, Release 3.8, effective date: 2023-08-31

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

Findings with regard to ETSI EN 319 401:

7.5 Cryptographic controls

Documentation of the quality of subject key pairs generated by the TSP shall be improved.

7.6 Physical and environmental security

Implementation of checks of visitor identity shall be improved.

Findings with regard to ETSI EN 319 411-1:

6.3.4 Certificate acceptance

There is no hint to the terms and conditions or agreement in the user’s application form. Also, with respect to GDPR the user shall be informed about use of personal data, including a hint that the certificate is published to the customer’s AD. In addition, key escrow shall be mentioned, too.

6.5.4 Activation data

Submission of activation data shall be improved.

All non-conformities have been closed before the issuance of this attestation.

To the best of our knowledge, no incidents have occurred within this Root-CA’s hierarchy during the audited period.

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
Note: Cross Certified Subordinate CA Certificate.		
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 = 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
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
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.		

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

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 V1.3.1 (2021-05) • ETSI EN 319 401 V2.3.1 (2021-05) CA Browser Forum Requirements: • S/MIME Baseline Requirements, version 1.0.1 Browser Policy Requirements: • Mozilla Root Store Policy, Version 2.9, 2023-09-01 • Apple Root Certificate Program, 2023-08-15 • Microsoft Trusted Root Program, 2023-06-09 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 V1.2.4 (2020-11)

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 Client Certificates, Release 3.8, effective date: 2023-08-31

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

Findings with regard to ETSI EN 319 401:

7.5 Cryptographic controls

Documentation of the quality of subject key pairs generated by the TSP shall be improved.

7.6 Physical and environmental security

Implementation of checks of visitor identity shall be improved.

Findings with regard to ETSI EN 319 411-1:

6.3.4 Certificate acceptance

There is no hint to the terms and conditions or agreement in the user’s application form. Also, with respect to GDPR the user shall be informed about use of personal data, including a hint that the certificate is published to the customer’s AD. In addition, key escrow shall be mentioned, too.

6.5.4 Activation data

Submission of activation data shall be improved.

All non-conformities have been closed before the issuance of this attestation.

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

- 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.

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 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: 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: 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: EE0343093DF71E364606100164C62A4FB8C4A0F32B1EB47860FFD6C17E94CA54	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 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 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 = 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.		

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

Modifications record

Version	Issuing Date	Changes
Version 1	2024-01-22	Initial attestation
Version 1.1	2024-01-24	Editorial changes after QA
Version 1.2	2024-01-29	Clarification with respect to Bugzilla issues and cross-certified root
Version 1.3	2024-01-30	Further clarifications (cross certificate, CP/CPS, policies)
Version 1.4	2024-02-01	Checksums corrected
Version 1.5	2024-02-14	Certificates in scope added, which did not issue S/MIME certificates but technically could Missing policies added

End of the audit attestation letter.