

TLS BR Audit Attestation for Telia Company AB

Reference: DSC.1257-5

“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.1257-5” covers multiple Root-CAs and consists of 17 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,

A handwritten signature in purple ink, appearing to read 'Alvilis Švēde'.

Dr. Alvilis Švēde
Lead Auditor

A handwritten signature in black ink, appearing to read 'Sönke Maseberg'.

Dr. Sönke Maseberg
Reviewer

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

<p>e) general knowledge of regulatory requirements relevant to TSPs; and f) knowledge of security policies and controls.</p> <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> 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

<ul style="list-style-type: none"> • 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.

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

<p>Type of audit:</p>	<p><input type="checkbox"/> Point in time audit <input type="checkbox"/> Period of time, after n month of CA operation <input checked="" type="checkbox"/> Period of time, full audit</p>
<p>Audit period covered for all policies:</p>	<p>2023-11-01 to 2024-10-31</p>
<p>Point in time date:</p>	<p>none, as audit was a period of time audit</p>
<p>Audit dates:</p>	<p>2024-11-12 to 2024-11-14 (on site)</p>
<p>Audit location:</p>	<p>Helsinki, Finland Solna, Sweden</p>

Root 1: TeliaSonera Root CA v1

Standards considered:	<p>European Standards:</p> <ul style="list-style-type: none">• 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) <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none">• Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, Version 2.0.8• Network and Certificate System Security Requirements, version 1.7 <p>Browser Policy Requirements:</p> <ul style="list-style-type: none">• 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 <p>For the Trust Service Provider Conformity Assessment:</p> <ul style="list-style-type: none">• 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

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

Findings with regard to ETSI EN 319 401:

None.

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]

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 1859314, Telia: TLS certificates issued in violation of TLS BR v2.0.1
https://bugzilla.mozilla.org/show_bug.cgi?id=1859314
- 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 Note: Cross Certified Subordinate CA Certificate.	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP, LCP
Complete subject DN: CN=TeliaSonera Server CA v2, O=TeliaSonera, C=FI Note: After 2023-03-31 this CA has renewed the test certificates required by CA/B Forum TLS BR in June 2023, only, no other certificates issued.	SHA-256 fingerprint of the certificate: D721110388CA6F20BBA9FD1A8DBA4EFB8C16392A3DEBAD97C553EEAF0ACACAAC	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 Domain Validation CA v2, O=Telia Finland Oyj, C=FI Note: After 2023-03-31 this CA has renewed the test certificates required by CA/B Forum TLS BR in June 2023, only, no other certificates issued.	SHA-256 fingerprint of the certificate: 5B312B7E11B70D07C14E0AB99F08D00748966098C52AA85A06A0822BBE59A02C	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=TeliaSonera Class 1 CA v2, O=TeliaSonera, C=FI Note: This CA has not been used for TLS issuance during the audit period.	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

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN=TeliaSonera Class 2 CA v2, O=TeliaSonera, C=FI	SHA-256 fingerprint of the certificate: 092829433D231949F4A9BC666CBF54B3AA27D7BEBCA048D75E59093E15A72EA5 Note: This CA has not been used for TLS issuance during the audit period.	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP, LCP
Complete subject DN: CN=TeliaSonera Email CA v4, O=TeliaSonera, C=SE	SHA-256 fingerprint of the certificate: D1F2656AC8382739A3B087C47AB5CAB945A32F162B6149C308783C7E06AF8AE8 Note: This CA has not been used for TLS issuance during the audit period.	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP, LCP

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:	<p>European Standards:</p> <ul style="list-style-type: none">• 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) <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none">• Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, Version 2.0.8• Network and Certificate System Security Requirements, version 1.7 <p>Browser Policy Requirements:</p> <ul style="list-style-type: none">• 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 <p>For the Trust Service Provider Conformity Assessment:</p> <ul style="list-style-type: none">• 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

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

Findings with regard to ETSI EN 319 401:
None.

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]

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 1859314, Telia: TLS certificates issued in violation of TLS BR v2.0.1
https://bugzilla.mozilla.org/show_bug.cgi?id=1859314
- 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 RSA TLS Root CA v3, O=Telia Company AB, C=SE	SHA-256 fingerprint of the certificate: 6DD4E12B751849BA3E1AD90AC48674C2474C772182F3500C85C2DF4DB7F48866 Note: Cross Certified Subordinate CA Certificate.	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=Telia EC TLS Root CA v3, O=Telia Company AB, C=SE	SHA-256 fingerprint of the certificate: 07E5866107E24AE69A9679668F916AA1B3B39DC3554781E3AE9ABAA44B5A7BC4 Note: Cross Certified Subordinate CA Certificate.	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP, LCP

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:	<p>European Standards:</p> <ul style="list-style-type: none">• 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) <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none">• Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, Version 2.0.8• Network and Certificate System Security Requirements, version 1.7 <p>Browser Policy Requirements:</p> <ul style="list-style-type: none">• 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 <p>For the Trust Service Provider Conformity Assessment:</p> <ul style="list-style-type: none">• 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

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

Findings with regard to ETSI EN 319 401:

None.

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]

Audit Attestation "DSC.1257-5", issued to "Telia Company AB"

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 1859314, Telia: TLS certificates issued in violation of TLS BR v2.0.1
https://bugzilla.mozilla.org/show_bug.cgi?id=1859314
- 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 Note: This CA has been used only to issue required test certificates for the new TLS root.	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 RSA OV CA v4, O = Telia Company AB, C = SE	SHA-256 fingerprint of the certificate: F07D383827E264326C5D0DBE257AA82108409F25246F81EE36C8AF222B5A1E43 Note: This CA has been used only to issue required test certificates for the new TLS root.	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP, OVCP, LCP

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

Root 4: Telia EC TLS Root CA v3

Standards considered:	<p>European Standards:</p> <ul style="list-style-type: none">• 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) <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none">• Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, Version 2.0.8• Network and Certificate System Security Requirements, version 1.7 <p>Browser Policy Requirements:</p> <ul style="list-style-type: none">• 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 <p>For the Trust Service Provider Conformity Assessment:</p> <ul style="list-style-type: none">• 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

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

Findings with regard to ETSI EN 319 401:

None.

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]

Audit Attestation "DSC.1257-5", issued to "Telia Company AB"

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 1859314, Telia: TLS certificates issued in violation of TLS BR v2.0.1
https://bugzilla.mozilla.org/show_bug.cgi?id=1859314
- 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 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 EC DV CA v4, O = Telia Company AB, C = SE	SHA-256 fingerprint of the certificate: 26D742741BA428394F904E4410ED6DA92F4D0C55521F1EDE2B29797F866C955C Note: This CA has been used only to issue required test certificates for the new TLS root.	ETSI EN policy that this Intermediate CA has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP, DVCP, LCP

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

Modifications record

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

End of the audit attestation letter.