TLS BR Audit Attestation for

Deutsche Telekom Security GmbH

Reference: AA2024062101

Essen, 2024-07-09

To whom it may concern,

This is to confirm that “TÜV Informationstechnik GmbH” has audited the CAs of “Deutsche Telekom Security GmbH” without open critical findings.

This present Audit Attestation Letter is registered under the unique identifier number “**AA2024062101**” covers multiple Root-CAs and consists of 14 pages.

Kindly find here-below the details accordingly.

In case of any question, please contact:

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Certification Body
Am TÜV 1
45307 Essen, Germany
E-Mail: certuvit@tuvit.de
Phone: +49 (0) 201 / 8999-9

With best regards,

Dr. Silke Keller	Wolfgang Thöne
Reviewer	Lead Auditor

This attestation is based on the template version 3.2 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

- TÜV Informationstechnik GmbH[1], TÜV NORD GROUP, Am TÜV 1, 45307 Essen, Germany, registered under HRB 11687, Amtsgericht Essen, Germany
- Accredited by DAkkS under registration D-ZE-12022-01-01[2] for the certification of trust services according to “DIN EN ISO/IEC 17065:2013” and “ETSI EN 319 403-1 V2.3.1 (2020-06)”.
- Insurance Carrier (BRG section 8.2):
  Allianz Global Corporate & Specialty SE
- Third-party affiliate audit firms involved in the audit:
  None.

Identification and qualification of the audit team

- Number of team members: 1 Lead Auditor, 1 Auditor, 2 Trainee Auditor
- 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] In the following termed shortly „TÜVIT“
[2] https://www.dakks.de/en/accredited-body.html?id=D-ZE-12022-01-01

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 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 Reviewer
- 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):

Deutsche Telekom Security GmbH, Bonner Talweg 100, 53113 Bonn, Germany, registered under “HRB 15241” at Amtsgericht Bonn, Germany

Postal address: Deutsche Telekom Security GmbH, Trust Center & ID Solutions, Untere Industriestr. 20, 57250 Netphen, Germany

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:

2023-04-08 to 2024-04-07

Point in time date:

none, as audit was a period of time audit

Audit dates:

2024-03-11 to 2024-03-14 (on-site)
2024-04-08 to 2024-04-11 (on-site)
2024-04-18 (on-site)
2024-05-24 (remote)

Audit location:

57250 Netphen, Germany
60388 Frankfurt, Germany
60484 Frankfurt, Germany

Root 1: Telekom Security TLS ECC Root 2020

Standards considered

European Standards:
- ETSI EN 319 411-1 V1.3.1 (2021-05)
- ETSI EN 319 401 V2.3.1 (2021-05)

CA Browser Forum Requirements:
- Guidelines for the Issuance and Management of Extended Validation Certificates, version 1.8.0
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.0.2
- Network and Certificate System Security Requirements, version 1.7

For the Trust Service Provider Conformity Assessment:
- 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:

- Deutsche Telekom Security GmbH Trust Center Certificate Policy, Version 4.0 as of 2023-08-28, Deutsche Telekom Security GmbH
- Deutsche Telekom Security GmbH Certification Practice Statement Public, Version 7.0 as of 2024-03-22, Deutsche Telekom Security GmbH

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

Findings with regard to ETSI EN 319 401:

7.1 Internal organization

Documentation and implementation of subcontractor management shall be improved. [REQ-7.1.1-07, REQ-7.1.1-08]

Documentation and implementation of the role appointment and access right process shall be improved. [REQ-7.1.2-01]

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
C=DE, O=Deutsche Telekom Security GmbH, CN=Telekom Security TLS ECC Root 2020	578AF4DED0853F4E5998DB4AEAF9CBEA8D945F60B620A38D1A3C13B2BC7BA8E1	ETSI EN 319 411-1 V1.3.1, EVCP

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
C=DE, O=Deutsche Telekom Security GmbH, CN=Telekom Security EV ECC CA 21	D7A8A9947C31806C1B4625F82FCBCCA7CC2090E58DB215B8E4D88BA9C60D3166	ETSI EN 319 411-1 V1.3.1, EVCP

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

Root 2: Telekom Security TLS RSA Root 2023

Standards considered

European Standards:
- ETSI EN 319 411-2 V2.4.1 (2021-11)
- ETSI EN 319 411-1 V1.3.1 (2021-05)
- ETSI EN 319 401 V2.3.1 (2021-05)

CA Browser Forum Requirements:
- Guidelines for the Issuance and Management of Extended Validation Certificates, version 1.8.0
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.0.2
- Network and Certificate System Security Requirements, version 1.7

For the Trust Service Provider Conformity Assessment:
- 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:

- Deutsche Telekom Security GmbH Trust Center Certificate Policy, Version 4.0 as of 2023-08-28, Deutsche Telekom Security GmbH
- Deutsche Telekom Security GmbH Certification Practice Statement Public, Version 7.0 as of 2024-03-22, Deutsche Telekom Security GmbH

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

Findings with regard to ETSI EN 319 401:

7.1 Internal organization

Documentation and implementation of subcontractor management shall be improved. [REQ-7.1.1-07, REQ-7.1.1-08]

Documentation and implementation of the role appointment and access right process shall be improved. [REQ-7.1.2-01]

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
C=DE, O=Deutsche Telekom Security GmbH, CN=Telekom Security TLS RSA Root 2023	EFC65CADBB59ADB6EFE84DA22311B35624B71B3B1EA0DA8B6655174EC8978646	ETSI EN 319 411-2 V2.4.1, QEVCP-w ETSI EN 319 411-1 V1.3.1, EVCP

Table 7: 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
C=DE, O=Deutsche Telekom Security GmbH, CN=Telekom Security EV RSA CA 23	9A6FC4AB4DB1EA6F6663507EDC1D008F091AE88FAB6F3AE56A84A4090529EF58	ETSI EN 319 411-2 V2.4.1, QEVCP-w ETSI EN 319 411-1 V1.3.1, EVCP

Table 8: Sub-CA's issued by the Root-CA 2 or its Sub-CA's in scope of the audit

Root 3: T-TeleSec GlobalRoot Class 2

Standards considered

European Standards:
- ETSI EN 319 411-1 V1.3.1 (2021-05)
- ETSI EN 319 401 V2.3.1 (2021-05)
- ETSI TS 119 411-6 V1.1.1 (2023-08)

CA Browser Forum Requirements:
- Guidelines for the Issuance and Management of Extended Validation Certificates, version 1.8.0
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.0.2
- Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.2
- Network and Certificate System Security Requirements, version 1.7

For the Trust Service Provider Conformity Assessment:
- 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:

- Deutsche Telekom Security GmbH Trust Center Certificate Policy, Version 4.0 as of 2023-08-28, Deutsche Telekom Security GmbH
- Deutsche Telekom Security GmbH Certification Practice Statement Public, Version 7.0 as of 2024-03-22, Deutsche Telekom Security GmbH

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

Findings with regard to ETSI EN 319 401:

7.1 Internal organization

Documentation and implementation of subcontractor management shall be improved. [REQ-7.1.1-07, REQ-7.1.1-08]

Documentation and implementation of the role appointment and access right process shall be improved. [REQ-7.1.2-01]

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 1825780: “Telekom Security: Improper use of a domain validation method”: https://bugzilla.mozilla.org/show_bug.cgi?id=1825780
- Bug 1875820: “Telekom Security: TLS certificates with basicConstraints not marked as critical”: https://bugzilla.mozilla.org/show_bug.cgi?id=1875820

- Bug 1877388: “Telekom Security: Revocation delay for TLS certificates with basicConstraints not marked as critical”: https://bugzilla.mozilla.org/show_bug.cgi?id=1877388

The remediation measures taken by Deutsche Telekom Security 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
C=DE, O=T-Systems Enterprise Services GmbH, OU=T-Systems Trust Center, CN=T-TeleSec GlobalRoot Class 2	91E2F5788D5810EBA7BA58737DE1548A8ECACD014598BC0B143E041B17052552	ETSI EN 319 411-1 V1.3.1, OVCP ETSI EN 319 411-1 V1.3.1, DVCP ETSI EN 319 411-1 V1.3.1, NCP ETSI EN 319 411-1 V1.3.1, NCP amended by ETSI TS 119 411-6 V1.1.1, NCP ETSI EN 319 411-1 V1.3.1, LCP ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1, LCP

Table 1: 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
C=DE, O=Deutsche Telekom AG, CN=Deutsche Telekom AG secure email CA E03	38CBC81860C904BDF18046CD0FB7754E44D569398DD14FBF09F72AA20FC35CCF	ETSI EN 319 411-1 V1.3.1, LCP
C=DE, O=Deutsche Telekom AG, CN=Deutsche Telekom AG secure email CA E05	1AB8A68FCBBA644D5C6D2627FE6D943CE4FD3E58619B3B087F3CF4EFA838C46A	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1, LCP
C=DE, O=Deutsche Telekom Security GmbH, CN=Telekom Security BusinessID SMIME CA 2023	6F25BD0E9E7492D15375089EB97C1C0747537336BB0FA82543BD2A485BE61A00	ETSI EN 319 411-1 V1.3.1, NCP amended by ETSI TS 119 411-6 V1.1.1, NCP
C=DE, O=Deutsche Telekom Security GmbH, CN=Telekom Security DV RSA CA 21	956FF9CC914874D9CAF9655BCCB696C1BE49A25BF928D5C41C0F5395A135D8B8	ETSI EN 319 411-1 V1.3.1, DVCP
C=DE, O=Deutsche Telekom Security GmbH, CN=Telekom Security DV RSA CA 22	938E52642501DD16E23D8AEBFB97EB3C3B2562F50C324144C390946B29684A7E	ETSI EN 319 411-1 V1.3.1, DVCP
C=DE, O=Deutsche Telekom Security GmbH, CN=Telekom Security OV RSA CA 22	D5D9445EEAA5576081DDF2E6C0904091BBC79BA10915E5215C8A2A7D87915FFD	ETSI EN 319 411-1 V1.3.1, OVCP

C=DE, O=Deutsche Telekom Security GmbH, CN=Telekom Security ServerID OV Class 2 CA	944ACE961DB316BEB694E01C302C46FED40DC0291729E7DAF58550C3CB55E791	ETSI EN 319 411-1 V1.3.1, OVCP
C=DE, O=T-Systems International GmbH, OU=T-Systems Trust Center, CN=TeleSec Business CA 1	44EBF0123E27FF1DB0497BD2DAE18155B2A414E6BCD9C6C8FB8F48398449B9E9	ETSI EN 319 411-1 V1.3.1, OVCP ETSI EN 319 411-1 V1.3.1, NCP
C=DE, O=Deutsche Telekom Security GmbH, CN=TeleSec Business CA 21	06B58F124B45E9417708F60CDDAEB6F39B72206FE4BD40EE2E20E628DDFDD33D	ETSI EN 319 411-1 V1.3.1, NCP amended by ETSI TS 119 411-6 V1.1.1, NCP
C=DE, O=Deutsche Telekom Security GmbH, CN=TeleSec Business TLS-CA 2022	A3F2A10A366AFF774CBB4E6EC4C8A8EF707C03E932B4C46E5078767AACF1ED60	ETSI EN 319 411-1 V1.3.1, OVCP
C=DE, O=Deutsche Telekom Security GmbH, CN=TeleSec Business TLS-CA 21	F00E616B59ED06E6CC9717D039F7A1A70CB3D08E0B6AD74653670CCE448C61F3	ETSI EN 319 411-1 V1.3.1, OVCP
C=DE, O=T-Systems International GmbH, OU=T-Systems Trust Center, ST=Nordrhein Westfalen, PostalCode=57250, L=Netphen, STREET=Untere Industriestr. 20, CN=TeleSec ServerPass Class 2 CA	AC1EC556318E3EA70F8F04E03A0F2633BFE73992359A810145FFDF1A427396EE	ETSI EN 319 411-1 V1.3.1, OVCP

Table 2: Sub-CA's issued by the Root-CA 3 or its Sub-CA's in scope of the audit

Root 4: T-TeleSec GlobalRoot Class 3

Standards considered

European Standards:
- ETSI EN 319 411-2 V2.4.1 (2021-11)
- ETSI EN 319 411-1 V1.3.1 (2021-05)
- ETSI EN 319 401 V2.3.1 (2021-05)

CA Browser Forum Requirements:
- Guidelines for the Issuance and Management of Extended Validation Certificates, version 1.8.0
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.0.2
- Network and Certificate System Security Requirements, version 1.7

For the Trust Service Provider Conformity Assessment:
- 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:

- Deutsche Telekom Security GmbH Trust Center Certificate Policy, Version 4.0 as of 2023-08-28, Deutsche Telekom Security GmbH
- Deutsche Telekom Security GmbH Certification Practice Statement Public, Version 7.0 as of 2024-03-22, Deutsche Telekom Security GmbH

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

Findings with regard to ETSI EN 319 401:

7.1 Internal organization

Documentation and implementation of subcontractor management shall be improved. [REQ-7.1.1-07, REQ-7.1.1-08]

Documentation and implementation of the role appointment and access right process shall be improved. [REQ-7.1.2-01]

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
C=DE, O=T-Systems Enterprise Services GmbH, OU=T-Systems Trust Center, CN=T-TeleSec GlobalRoot Class 3	FD73DAD31C644FF1B43BEF0CCDDA96710B9CD9875ECA7E31707AF3E96D522BBD	ETSI EN 319 411-2 V2.4.1, QEVCP-w ETSI EN 319 411-1 V1.3.1, EVCP

Table 11: 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
C=DE, O=Deutsche Telekom Security GmbH, CN=Telekom Security EV RSA CA 22	86DB1D597419BC0FDDF2A6129DE46AF537752683A49CB9435C855F53637CFE13	ETSI EN 319 411-1 V1.3.1, EVCP
C=DE, O=Deutsche Telekom Security GmbH, CN=Telekom Security EV RSA CA 23A	82FBE865DA22D1F25ADF94BBD809D3F516125849E792DB7BB18452304C2ECC43	ETSI EN 319 411-2 V2.4.1, QEVCP-w ETSI EN 319 411-1 V1.3.1, EVCP
C=DE, O=Deutsche Telekom Security GmbH, CN=Telekom Security ServerID EV Class 3 CA	5092CE0E3F70F2FD9561C34623B546F7D333EF1B633C147D1290E28DE986A230	ETSI EN 319 411-2 V2.4.1, QEVCP-w ETSI EN 319 411-1 V1.3.1, EVCP
C=DE, O=T-Systems International GmbH, OU=T-Systems Trust Center, ST=Nordrhein Westfalen, PostalCode=57250, L=Netphen, STREET=Untere Industriestr. 20, CN=TeleSec ServerPass Extended Validation Class 3 CA	8A0ADDAE4F2CF9D2C24D7A49EED5C86C8B1DF1C85BA73DE5C477CB14FA0D13E9	ETSI EN 319 411-2 V2.4.1, QEVCP-w ETSI EN 319 411-1 V1.3.1, EVCP

Table 12: 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	2024-06-21	Initial attestation
Version 2	2024-07-04	Correction of errors
Version 3	2024-09-09	TLS-EV CAs added to this TLS-BR attestation

End of the audit attestation letter.