

SBR Audit Attestation for

Deutsche Telekom Security GmbH

Reference: AA2025061801-SBR

Essen, 2025-06-18

To whom it may concern,

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

This present Audit Attestation Letter is registered under the unique identifier number “AA2025061801-SBR”, covers multiple Root-CAs and consists of 11 pages.

Kindly find here-below the details accordingly.

In case of any question, please contact:

TÜV NORD CERT GmbH
Business Entity IT
Am TÜV 1
45307 Essen, Germany
E-Mail: info.tncert@tuev-nord.de

With best regards,

Dr. Bernd Kirsig
Lead Auditor

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

Headquarters
TÜV NORD CERT GmbH

Am TÜV 1
45307 Essen, Germany

Tel.: 0201 825-0
Fax: 0201 825-2517
info.tncert@tuev-nord.de
tuev-nord-cert.en

Director
Dipl.-Ing. Wolfgang Wielpütz
Dipl.-Oec. Sandra Gerhartz

Registration Office
Amtsgericht Essen
HRB 9976
VAT ID No.: DE 811389923
Tax No.: 111/5706/2193

Deutsche Bank AG, Essen
BIC (SWIFT-Code): DEUTDE33XXX
IBAN-Code: DE26 3607 0050 0607 8950 00

General audit information

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor

- TÜV NORD CERT GmbH, Am TÜV 1, 45307 Essen, Germany, registered under HRB 9976, Amtsgericht Essen, Germany
- Accredited by DAkkS under registration D-ZE-12007-01-12¹ 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
- 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;
 - e) general knowledge of regulatory requirements relevant to TSPs; and

¹ <https://www.dakks.de/en/accredited-body.html?id=D-ZE-12007-01-12>

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, Friedrich-Ebert-Allee 71-77, 53113 Bonn, Germany, registered under "HRB 15241" at Amtsgericht Bonn, Germany
Postal address: Deutsche Telekom Security GmbH, Koblenzer Str. 87-89, 57072 Siegen, Germany

Type of audit:

- Point in time audit
- Period of time, after 13 month of CA operation
- Period of time, full audit

Audit period covered for all policies:

2024-04-08 to 2025-04-03

Point in time date:

none, as audit was a period of time audit

Audit dates:

2025-03-10 to 2025-03-13 (on-site)
2025-03-31 to 2025-04-03 (on-site)

Audit location:

57072 Siegen, Germany

Root 1: Telekom Security SMIME ECC Root 2021

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:

- Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.9
- Network and Certificate System Security Requirements, version 2.0.4

For the Trust Service Provider Conformity Assessment:

- 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:

- Deutsche Telekom Security GmbH, Trust Center Certificate Policy, Version 6.0 as of 2025-01-15, Deutsche Telekom Security GmbH
- Deutsche Telekom Security GmbH, Certification Practice Statement Public, Version 8.00 as of 2025-03-01, Deutsche Telekom Security GmbH

No non-conformities have been identified during the audit.

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 SMIME ECC Root 2021	3AE6DF7E0D637A65A8C81612EC6F9A142F85A16834C10280D88E707028518755	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) ETSI EN 319 411-1 V1.3.1, NCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)

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 SMIME ECC CA 23	EA45DD36FD0CA91706080F68F7213D55E658249A20C81AFDD34E80CC5EC3E349	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) ETSI EN 319 411-1 V1.3.1, NCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)
C = DE, O = Deutsche Telekom Security GmbH, CN = Telekom Security SMIME ECC CA 24	F33B1859C34A063E941DC7D8F3F5378833C4770D48B7454EE1CDCD9A8194935A	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) ETSI EN 319 411-1 V1.3.1, NCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)
C = DE, O = Deutsche Telekom Security GmbH, CN = Deutsche Telekom AG SMIME ECC CA 24	5F8CD9D54A0C2F83C86B999F34C448A4608DC75C4377978A4CC3669B5718BF36	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)

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 SMIME RSA Root CA 2023

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:

- Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.9
- Network and Certificate System Security Requirements, version 2.0.4

For the Trust Service Provider Conformity Assessment:

- 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:

- Deutsche Telekom Security GmbH, Trust Center Certificate Policy, Version 6.0 as of 2025-01-15, Deutsche Telekom Security GmbH
- Deutsche Telekom Security GmbH, Certification Practice Statement Public, Version 8.00 as of 2025-03-01, Deutsche Telekom Security GmbH

No major or minor non-conformities have been identified during the audit.

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 SMIME RSA Root 2023	78A656344F947E9CC0F734D9053D32F6742086B6B9CD2CAE4FAE1A2E4EFDE048	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) ETSI EN 319 411-1 V1.3.1, NCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)

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
C = DE, O = Deutsche Telekom Security GmbH, CN = Telekom Security SMIME RSA CA 23	EB48699C89C702DAC2C05F483396489BBBF71AA0ACAC0F52596A5DE97CEBD913	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) ETSI EN 319 411-1 V1.3.1, NCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)
C = DE, O = Deutsche Telekom Security GmbH, CN = Telekom Security SMIME RSA CA 24	0E2CFE3B15D2A754BD86DDDA077AC4A3DF961A9FA6B59278DD72098024D04567	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) ETSI EN 319 411-1 V1.3.1, NCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)
C = DE, O = Deutsche Telekom Security GmbH, CN = Deutsche Telekom AG SMIME RSA CA 24	0CE1DAB9D12CD1D587AEF1B7B50B33D682D539F45DF809643A53B6A84935B47B	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)

Table 4: 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:

- Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.9
- Network and Certificate System Security Requirements, version 2.0.4

For the Trust Service Provider Conformity Assessment:

- 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:

- Deutsche Telekom Security GmbH, Trust Center Certificate Policy, Version 6.0 as of 2025-01-15, Deutsche Telekom Security GmbH
- Deutsche Telekom Security GmbH, Certification Practice Statement Public, Version 8.00 as of 2025-03-01, Deutsche Telekom Security GmbH

No major or minor non-conformities have been identified during the audit.

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

- [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
- [Bug 1914383] Telekom Security: CRL entries with wrong CRL reason codes
https://bugzilla.mozilla.org/show_bug.cgi?id=1914383.

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 2	91E2F5788D5810EBA7BA58737DE1548A8ECACD014598BC0B143E041B17052552	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) ETSI EN 319 411-1 V1.3.1, NCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)

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
C=DE, O=Deutsche Telekom AG, CN=Deutsche Telekom AG secure email CA E03	38CBC81860C904BDF18046CD0FB7754E44D569398DD14FBBF09F72AA20FC35CCF	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 (2023-08)
C = DE. O = Deutsche Telekom Security GmbH, CN = TeleSec Business CA 21	06B58F124B45E9417708F60CDDAEB6F39B72206FE4BD40EE2E20E628DDFDD33D	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) ETSI EN 319 411-1 V1.3.1, NCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)
C = DE, O = Deutsche Telekom Security GmbH, CN = Telekom Security BusinessID SMIME CA 2023	6F25BD0E9E7492D15375089EB97C1C0747537336BB0FA82543BD2A485BE61A00	ETSI EN 319 411-1 V1.3.1, LCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08) ETSI EN 319 411-1 V1.3.1, NCP amended by ETSI TS 119 411-6 V1.1.1 (2023-08)

C = DE. O = Deutsche Telekom
Security GmbH, CN = Telekom Security
SMIME CA 25

BE096522370C4BABCA86876B3060A94FC3D157613C3500606A9E5691DA7D11E7

ETSI EN 319 411-1 V1.3.1, LCP
amended by ETSI TS 119 411-6
V1.1.1 (2023-08)
ETSI EN 319 411-1 V1.3.1, NCP
amended by ETSI TS 119 411-6
V1.1.1 (2023-08)

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



Modifications record

Version	Issuing Date	Changes
Version 1	2025-06-18	Initial attestation

End of the audit attestation letter.