Audit Attestation for

Deutsche Telekom Security GmbH

Reference: AA2023042801

Essen, 2023-04-28

To whom it may concern,

This is to confirm that “TÜV Informationstechnik 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 “**AA2023042801**”, it covers multiple Root-CAs and consists of 8 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
Reviewer

Matthias Wiedenhorst
Lead Auditor

General audit information

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor
• TÜV Informationstechnik GmbH[1], 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 V2.2.2 (2015-08)”. • Insurance Carrier (BRG section 8.2): HDI Global 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 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; e) general knowledge of regulatory requirements relevant to TSPs; and

[1] In the following termed shortly „TÜViT“
[2] https://www.dakks.de/en/accredited-body.html?id=D-ZE-12022-01-01

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 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:	none, as audit was a point in time audit
Point in time date:	2023-03-28
Audit dates:	2023-03-28
Audit location:	57250 Netphen, Germany

Root 1: Telekom Security SMIME RSA Root 2023

Standards considered:	European Standards: ☒ ETSI EN 319 411-1 V1.3.1 (2021-05) ☒ ETSI EN 319 401 V2.4.1 (2021-11) CA Browser Forum Requirements: ☒ Baseline Requirements, version 1.8.6 For the Trust Service Provider Conformity Assessment: ☒ ETSI EN 319 403 V2.2.2 (2015-08) ☒ 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:

1. Trust Center Certificate Policy, Version 3.0 as of 2023-01-24, Deutsche Telekom Security GmbH
2. Certification Practice Statement Public, Version 04.00 as of 2023-01-10, Deutsche Telekom Security GmbH

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

Distinguished Name	SHA-256 fingerprint	Applied policy and OID
C=DE, O=Deutsche Telekom Security GmbH, CN=Telekom Security SMIME RSA Root 2023	78A656344F947E9CC0F734D9053D32F6742086B6B9CD2CAE4FAE1A2E4EFDE048	ETSI EN 319 411-1 V1.3.1, NCP

Table 1: Root-CA 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 and OID	EKU
C=DE, O=Deutsche Telekom Security GmbH, CN=Telekom Security SMIME RSA CA 23	EB48699C89C702DAC2C05F483396489BBBF71AA0ACAC0F52596A5DE97CEBD913	ETSI EN 319 411-1 V1.3.1, NCP	id-kp-clientAuth (1.3.6.1.5.5.7.3.2) id-kp-emailProtection (1.3.6.1.5.5.7.3.4)

Table 2: Sub-CA’s issued by the Root-CA 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 V2.3.1 (2021-05) ☒ ETSI EN 319 411-1 V1.3.1 (2021-05) ☒ ETSI EN 319 401 V2.4.1 (2021-11) CA Browser Forum Requirements: ☒ EV SSL Certificate Guidelines, version 1.8.0 ☒ Baseline Requirements, version 1.8.6 For the Trust Service Provider Conformity Assessment: ☒ ETSI EN 319 403 V2.2.2 (2015-08) ☒ 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:

1. Trust Center Certificate Policy, Version 3.0 as of 2023-01-24, Deutsche Telekom Security GmbH
2. Certification Practice Statement Public, Version 04.00 as of 2023-01-10, Deutsche Telekom Security GmbH

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

Distinguished Name	SHA-256 fingerprint	Applied policy and OID
C=DE, O=Deutsche Telekom Security GmbH, CN=Telekom Security TLS RSA Root 2023	EFC65CADBB59ADB6EFE84DA22311B35624B71B3B1EA0DA8B6655174EC8978646	ETSI EN 319 411-2 V2.3.1, QEVCP-w ETSI EN 319 411-1 V1.3.1, EVCP

Table 3: Root-CA 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 and OID	EKU
C=DE, O=Deutsche Telekom Security GmbH, CN=Telekom Security EV RSA CA 23	9A6FC4AB4DB1EA6F6663507EDC1D008F091AE88FAB6F3AE56A84A4090529EF58	ETSI EN 319 411-2 V2.3.1, QEVCP-w ETSI EN 319 411-1 V1.3.1, EVCP	id-kp-clientAuth (1.3.6.1.5.5.7.3.2) id-kp-serverAuth (1.3.6.1.5.5.7.3.1)

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

Modifications record

Version	Issuing Date	Changes
Version 1	2023-04-28	Initial attestation

End of the audit attestation letter.