Audit Attestation for

Deutsche Telekom Security GmbH

Reference: AA2022070107

Essen, 2022-07-01

To whom it may concern,

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

This present Audit Attestation Letter is registered under the unique identifier number “**AA2022070107**” 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	Matthias Wiedenhorst
Reviewer	Lead Auditor

Identification of the conformity assessment body (CAB):	• 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 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 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;

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

	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 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. • 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:	2021-04-22 to 2022-04-07
Point in time date:	None. The audit was a Period-of-Time Audit.
Audit dates:	2022-03-28 to 2022-03-31 (on-site) 2022-04-04 to 2022-04-07 (on-site)
Audit location:	57250 Netphen, Germany 60484 Frankfurt, Germany 60388 Frankfurt, Germany

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: ☐ EV SSL Certificate Guidelines, version 1.7.8 ☒ Baseline Requirements, version 1.8.2 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 02.00 as of 2022-03-01, valid from 2022-03-02, Deutsche Telekom Security GmbH
2. Certification Practice Statement Root, Version 15.00 as of 2022-02-18, valid from 2022-03-01, Deutsche Telekom Security GmbH
3. CPS Server.ID (TeleSec ServerPass), Version 19.00 as of 2022-03-01, Deutsche Telekom Security GmbH
4. Certification Practice Statement (CPS), Business.ID (Shared-Business-CA), Version 16.00 as of 2022-02-16, valid from 2022-02-18, Deutsche Telekom Security GmbH
5. Deutsche Telekom Corporate PKI (DTAG cPKI), Certificate Policy (CP) & Certificate Practice Statement (CPS), Version 11.00 as of 2022-02-16, valid from 2022-02-17, Deutsche Telekom Security GmbH
6. Trust Center Certificate Practice Statement Public, Version 02.00 as of 2022-03-15, Deutsche Telekom Security GmbH

No non-conformities have been identified during the audit.

This Audit Attestation also covers the following incidents as documented under

- Bug 1703528, Telekom Security: Key Encipherment in two ECC SAN TLS certificates: https://bugzilla.mozilla.org/show_bug.cgi?id=1703528
- Bug 1711432, Telekom Security: Certificate with invalid FQDN: https://bugzilla.mozilla.org/show_bug.cgi?id=1711432

The remediation measures taken by Deutsche Telekom Security GmbH as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident. The long-term effectiveness of the measures will be rechecked at the next regular audit.

Identification of the audited Root-CA:		
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 V.1.3.1, LCP ETSI EN 319 411-1 V.1.3.1, NCP ETSI EN 319 411-1 V.1.3.1, DVCP ETSI EN 319 411-1 V.1.3.1, OVCP

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.

Identification of the audited Sub-CAs			
Distinguished Name	**SHA-256 fingerprint**	**Applied policy**	**EKU**
C=DE, O=Deutsche Telekom AG, CN=Deutsche Telekom AG secure email CA E03	38CBC81860C904BDF18046CD0FB7754E44D569398DD14FBF09F72AA20FC35CCF	ETSI EN 319 411-1 V.1.3.1, LCP	id-kp-emailProtection (1.3.6.1.5.5.7.3.4) szOID_KP_CA_EXCHANGE (1.3.6.1.4.1.311.21.5)
C=DE, O=Deutsche Telekom Security GmbH, CN=Telekom Security DV RSA CA 21	956FF9CC914874D9CAF9655BCCB696C1BE49A25BF928D5C41C0F5395A135D8B8	ETSI EN 319 411-1 V.1.3.1, DVCP	id-kp-serverAuth (1.3.6.1.5.5.7.3.1)
C=DE, O=Deutsche Telekom Security GmbH, CN=Telekom Security DV RSA CA 22	938E52642501DD16E23D8AEBFB97EB3C3B2562F50C324144C390946B29684A7E	ETSI EN 319 411-1 V.1.3.1, DVCP	id-kp-clientAuth (1.3.6.1.5.5.7.3.2) id-kp-serverAuth (1.3.6.1.5.5.7.3.1)
C=DE, O=T-Systems International GmbH, OU=T-Systems Trust Center, CN=TeleSec Business CA 1	44EBF0123E27FF1DB0497BD2DAE18155B2A414E6BCD9C6C8FB8F48398449B9E9	ETSI EN 319 411-1 V.1.3.1, NCP ETSI EN 319 411-1 V.1.3.1, OVCP	not defined
C=DE, O=Deutsche Telekom Security GmbH, CN=TeleSec Business CA 2021	7732599AAF35853E0351E49F8057BBF5321777E83603C38570065056A56FA68B	ETSI EN 319 411-1 V.1.3.1, 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)

C=DE, O=Deutsche Telekom Security GmbH, CN=TeleSec Business CA 21	06B58F124B45E9417708F60CDDAEB6F39B72206FE4BD40EE2E20E628DDFDD33D	ETSI EN 319 411-1 V.1.3.1, 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)
C=DE, O=Deutsche Telekom Security GmbH, CN=TeleSec Business TLS-CA 2021	A712E2126EA4CAC6A5EE860D2F3E0CE03CDFD232A9E7911B7CFE2C4B12A228FA	ETSI EN 319 411-1 V.1.3.1, OVCP	id-kp-serverAuth (1.3.6.1.5.5.7.3.1)
C=DE, O=Deutsche Telekom Security GmbH, CN=TeleSec Business TLS-CA 21	F00E616B59ED06E6CC9717D039F7A1A70CB3D08E0B6AD74653670CCE448C61F3	ETSI EN 319 411-1 V.1.3.1, OVCP	id-kp-serverAuth (1.3.6.1.5.5.7.3.1)
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 V.1.3.1, OVCP	not defined

Table 2: 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 1.0	2022-07-01	Initial attestation

End of the audit attestation letter.