Audit Attestation for

Deutsche Telekom Security GmbH

Reference: AA2021070109

Essen, 2021-07-01

To whom it may concern,

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

This present Audit Attestation Letter is registered under the unique identifier number “**AA2021070109**” and consists of 10 pages.

Kindly find here-below the details accordingly.

In case of any question, please contact:

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Certification Body
Langemarckstr. 20
45141 Essen, Germany
E-Mail: certuvit@tuvit.de
Phone: +49 (0) 201 / 8999-9

With best regards,

Dr. Silke Keller	Matthias Wiedenhorst
Reviewer	Leadauditor

Identification of the conformity assessment body (CAB):	• TÜV Informationstechnik GmbH[1], Langemarckstraße 20, 45141 Essen, Germany, registered under HRB 11687, Amtsgericht Essen, Germany • Accredited by DAkkS under registration D-ZE-12022-01[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 • 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 o has acted as auditor in at least three complete TSP audits; o has adequate knowledge and attributes to manage the audit process; and o 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 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

Audit Period covered for all policies:	2020-05-10 until 2021-04-21

Audit dates:	2021-04-12 until 2021-04-15 (remote) 2021-04-20 until 2021-04-21 (onsite)
Audit Location:	Deutsche Telekom Security GmbH, Trust Center & ID Solutions, Untere Industriestr. 20, 57250 Netphen, Germany Due to COVID-19 / Sars-CoV-2 influences, the 2 data centre locations have not been inspected in person, but the physical security concept was discussed during the audit. Both data centres maintain active certifications according to ISO/IEC 27001 and TÜViT Trusted Site Infrastructure.
Type of audit	☐ Point in time audit ☐ Period of time, after x month of CA operation ☒ Period of time, full audit

Standards considered	(Only with regard to key generation and key protection requirements) European Standards: ☐ ETSI EN 319 411-2, V2.2.2 (2018-04) ☒ ETSI EN 319 411-1, V1.2.2 (2018-04) ☒ ETSI EN 319 401, V2.2.1 (2018-04) CA Browser Forum Requirements: ☐ EV SSL Certificate Guidelines, version 1.7.5 ☒ Baseline Requirements, version 1.7.4 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 TSP:

1. Deutsche Telekom Security GmbH – Trust Center Certificate Policy, Deutsche Telekom Security GmbH, version 01.00 as of 2021-03-15
2. Deutsche Telekom Security GmbH – Root Certificate Practice Statement, Deutsche Telekom Security GmbH, version 13.00 as of 2021-03-15
3. CPS TeleSec ServerPass, Deutsche Telekom Security GmbH, version 16.00 as of 2021-04-30
4. Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) der Shared-Business-CA, Deutsche Telekom Security GmbH, version 13.00 as of 2021-04-30
5. Deutsche Telekom PKS – Certificate Practice Statement (CPS), Zertifizierungsrichtlinie für den Deutsche Telekom Security GmbH Public Key Service, Deutsche Telekom Security GmbH, version 08.00 as of 2021-04-30

6. Deutsche Telekom Corporate PKI (DTAG cPKI) – Certificate Policy (CP) & Certificate Practice Statement (CPS) – Zertifizierungsrichtlinie und Erklärung zum Zertifikatsbetrieb, Deutsche Telekom Security GmbH, Version 10.00 as of 2021-04-30

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

This Audit Attestation also covers the following incidents as documented under

- Bug 1649941, T-Systems: Incorrect OCSP Delegated Responder Certificate: https://bugzilla.mozilla.org/show_bug.cgi?id=1649941
- Bug 1651487, Telekom Security: Delayed Revocations of Sub-CA certificates: https://bugzilla.mozilla.org/show_bug.cgi?id=1651487
- Bug 1651611, Telekom Security: Finding in 2020 ETSI-Audit regarding weekly review of changes to configurations: https://bugzilla.mozilla.org/show_bug.cgi?id=1651611
- Bug 1655698, Telekom Security: CRL also contained unrevoked certificates: https://bugzilla.mozilla.org/show_bug.cgi?id=1655698
- Bug 1675314, Telekom Security: Wrong jurisdiction entries in certificates: https://bugzilla.mozilla.org/show_bug.cgi?id=1675314
- Bug 1703528, Telekom Security: Key Encipherment in two ECC SAN TLS certificates: https://bugzilla.mozilla.org/show_bug.cgi?id=1703528

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	C=DE, O=T-Systems Enterprise Services GmbH, OU=T-Systems Trust Center, CN=T-TeleSec GlobalRoot Class 2	Applied policy	ETSI EN 319 411-1 V1.2.2, LCP ETSI EN 319 411-1 V1.2.2, NCP ETSI EN 319 411-1 V1.2.2, NCP+ ETSI EN 319 411-1 V1.2.2, DVCP ETSI EN 319 411-1 V1.2.2, OVCP
SHA-256 fingerprint	91E2F5788D5810EBA7BA58737DE1548A8ECACD014598BC0B143E041B17052552		

Table 1: Root-CA in scope of this attestation

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	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	Applied policy	ETSI EN 319 411-1 V1.2.2, OVCP	EKU	not defined
SHA-256 fingerprint	AC1EC556318E3EA70F8F04E03A0F2633BFE73992359A810145FFDF1A427396EE				

Distinguished Name	C=DE, O=T-Systems International GmbH, OU=T-Systems Trust Center, CN=TeleSec Business CA 1	Applied policy	ETSI EN 319 411-1 V1.2.2, NCP ETSI EN 319 411-1 V1.2.2, OVCP	EKU	not defined
SHA-256 fingerprint	44EBF0123E27FF1DB0497BD2DAE18155B2A414E6BCD9C6C8FB8F48398449B9E9				
Distinguished Name	C=DE, O=Deutsche Telekom AG, CN=Deutsche Telekom AG secure email CA E03	Applied policy	ETSI EN 319 411-1 V1.2.2, LCP	EKU	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)
SHA-256 fingerprint	38CBC81860C904BDF18046CD0FB7754E44D569398DD14FBF09F72AA20FC35CCF				
Distinguished Name	C=DE, O=Deutsche Telekom Security GmbH, CN=Telekom Security DV RSA CA 21	Applied policy	ETSI EN 319 411-1 V1.2.2, DVCP	EKU	id-kp-serverAuth (1.3.6.1.5.5.7.3.1)
SHA-256 fingerprint	956FF9CC914874D9CAF9655BCCB696C1BE49A25BF928D5C41C0F5395A135D8B8				
Distinguished Name	C=DE, O=T-Systems International GmbH, OU=T-Systems Trust Center, CN=TeleSec PKS CA 8	Applied policy	ETSI EN 319 411-1 V1.2.2, NCP+	EKU	id-kp-clientAuth (1.3.6.1.5.5.7.3.2) id-kp-emailProtection (1.3.6.1.5.5.7.3.4) id-kp-OCSPSigning (1.3.6.1.5.5.7.3.9) Smartcard logon (1.3.6.1.4.1.311.20.2.2)
SHA-256 fingerprint	D486BFA3F00D165EE2CF6270FDA7D00817E58CDA2DF4FA256E0F2EB122CF8F02				

Distinguished Name	C=DE, O=Deutsche Telekom AG, OU=Trust Center, CN=Deutsche Telekom AG Issuing CA 01	Applied policy	ETSI EN 319 411-1 V1.2.2, LCP	EKU	id-kp-emailProtection (1.3.6.1.5.5.7.3.4) id-kp-OCSPSigning (1.3.6.1.5.5.7.3.9) szOID_KP_CA_EXCHANGE (1.3.6.1.4.1.311.21.5)
SHA-256 fingerprint	C6193077C6189D1DFBBF813B87DC7CBF0498ACF727887BC7EC54320906DE9BC8				
Distinguished Name	C=DE, O=Deutsche Telekom AG, OU=Trust Center, CN=Deutsche Telekom AG secure email CA	Applied policy	ETSI EN 319 411-1 V1.2.2, LCP	EKU	id-kp-emailProtection (1.3.6.1.5.5.7.3.4) id-kp-OCSPSigning (1.3.6.1.5.5.7.3.9) szOID_KP_CA_EXCHANGE (1.3.6.1.4.1.311.21.5)
SHA-256 fingerprint	D0805A3E6A628E9405613023DE87827A76118DC116B64903D3E75B9DDF4BDB97				
Distinguished Name	C=DE, O=Deutsche Telekom AG, OU=Trust Center, CN=Deutsche Telekom AG secure email CA	Applied policy	ETSI EN 319 411-1 V1.2.2, LCP	EKU	id-kp-emailProtection (1.3.6.1.5.5.7.3.4) id-kp-OCSPSigning (1.3.6.1.5.5.7.3.9) szOID_KP_CA_EXCHANGE (1.3.6.1.4.1.311.21.5)
SHA-256 fingerprint	1ACF28AA8C5303EFE5C30118623936B6F501F94D3BB7AD35B810B764345F4F01				

Distinguished Name	C=DE, O=Deutsche Telekom AG, CN=Deutsche Telekom AG secure email CA E02	Applied policy	ETSI EN 319 411-1 V1.2.2, LCP	EKU	id-kp-emailProtection (1.3.6.1.5.5.7.3.4) id-kp-OCSPSigning (1.3.6.1.5.5.7.3.9) szOID_KP_CA_EXCHANGE (1.3.6.1.4.1.311.21.5)
SHA-256 fingerprint	029379118E5775226C54D7182A367A240B51770F5011BB35177CFD17D9B2445A				

Table 2: Sub-CA’s issued by the Root-CA or its Sub-CA’s

Modifications record

Version	Issuing Date	Changes
Version 1.0	2021-07-01	Initial attestation

End of the audit attestation letter.