

Audit Attestation for

Deutsche Telekom Security GmbH

Reference: AA2021070105

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 findings.

This present Audit Attestation Letter is registered under the unique identifier number "AA2021070105" and consists of 6 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
Reviewer

Matthias Wiedenhorst
Leadauditor

<p>Identification of the conformity assessment body (CAB):</p>	<ul style="list-style-type: none"> • TÜV Informationstechnik GmbH¹, Langemarckstraße 20, 45141 Essen, Germany, registered under HRB 11687, Amtsgericht Essen, Germany • Accredited by DAkkS under registration D-ZE-12022-01² 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.
<p>Identification and qualification of the audit team:</p>	<ul style="list-style-type: none"> • 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 <ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> 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>

	<p>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</p> <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> ○ has acted as auditor in at least three complete TSP audits; ○ has adequate knowledge and attributes to manage the audit process; and ○ 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.
<p>Identification and qualification of the reviewer performing audit quality management:</p>	<ul style="list-style-type: none"> • 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.
<p>Identification of the trust service provider (TSP):</p>	<p>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</p>
<p>Audit Period covered for all policies:</p>	<p>None. This is a Point-in-Time Key Ceremony Audit.</p>

Audit dates:	2021-03-18 (on site)
Audit Location:	Deutsche Telekom Security GmbH, Trust Center & ID Solutions, Untere Industriestr. 20, 57250 Netphen, Germany
Type of audit	<input checked="" type="checkbox"/> Point in time audit <input type="checkbox"/> Period of time, after x month of CA operation <input type="checkbox"/> Period of time, full audit

Standards considered	<p>(Only with regard to key generation and key protection requirements)</p> <p>European Standards:</p> <input checked="" type="checkbox"/> ETSI EN 319 411-2, V2.2.2 (2018-04) <input checked="" type="checkbox"/> ETSI EN 319 411-1, V1.2.2 (2018-04) <input checked="" type="checkbox"/> ETSI EN 319 401, V2.2.1 (2018-04) <p>CA Browser Forum Requirements:</p> <input checked="" type="checkbox"/> EV SSL Certificate Guidelines, version 1.7.4 <input checked="" type="checkbox"/> Baseline Requirements, version 1.7.3 <p>For the Trust Service Provider Conformity Assessment:</p> <input checked="" type="checkbox"/> ETSI EN 319 403 V2.2.2 (2015-08) <input checked="" type="checkbox"/> 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 – Erklärung zum Zertifizierungsbetrieb der Root, Deutsche Telekom Security GmbH, version 13.00 as of 2021-03-15

The root key and root certificate generation ceremony of the aforementioned Root-CA has been covered in this audit. No Sub-CA's have been generated during that ceremony.

No non-conformities have been identified during the audit.

Identification of the audited Root-CA:			
Distinguished Name	C=DE, O=Deutsche Telekom Security GmbH, CN=Telekom Security SMIME RSA Root 2021	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+ (Only with regard to key generation and key protection requirements)
SHA-256 fingerprint	8B8B4C66213F8D70407087DF02D54BFDA6E7BE5251FC7570FB5EFF609354ED52		

Modifications record

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

End of the audit attestation letter.