



## Audit Attestation for

### *T-Systems International GmbH*

**Reference: AA2020012301**

Essen, 2020-01-24

To whom it may concern,

This is to confirm that "TÜV Informationstechnik GmbH" has successfully audited the CAs of the "**T-Systems International GmbH**" without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number "**AA2020012301**" 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](mailto:certuvit@tuvit.de)  
Phone: +49 (0) 201 / 8999-9

With best regards,

---

**Dr. Silke Keller**  
Reviewer

---

**Matthias Wiedenhorst**  
Leadauditor

**TÜV Informationstechnik GmbH – Member of TÜV NORD GROUP**

Langemarckstrasse 20  
45141 Essen, Germany  
Phone: +49 201 8999-9  
Fax: +49 201 8999-888  
[info@tuvit.de](mailto:info@tuvit.de)  
[www.tuvit.de](http://www.tuvit.de)

Court of jurisdiction:  
Essen HRB 11687  
VAT ID.: DE 176132277  
Tax No.: 111/57062251

Commerzbank AG  
SWIFT/BIC Code: DRES DEFF 360  
IBAN: DE47 3608 0080 0525 4851 00

Management Board  
Dirk Kretzschmar

Identification of the conformity assessment body (CAB):	TÜV Informationstechnik GmbH <sup>1</sup> , Langemarckstraße 20, 45141 Essen, Germany registered under HRB 11687, Amtsgericht Essen, Germany Accredited by DAkKS under registration D-ZE-12022-01 <sup>2</sup> for the certification of trust services according to “DIN EN ISO/IEC 17065:2013” and “ETSI EN 319 403 V2.2.2 (2015-08)”.
---	---

Identification of the trust service provider (TSP):	T-Systems International GmbH, Untere Industriestraße 20, 57250 Netphen, Germany, registered under “HRB 55933” at Amtsgericht Frankfurt am Main, Germany.
---	---

Identification of the audited Root-CA:	T-TeleSec GlobalRoot Class 2	
	Distinguished Name	CN=T-TeleSec GlobalRoot Class 2 OU=T-Systems Trust Center O=T-Systems Enterprise Services GmbH C=DE
	SHA-256 fingerprint	91E2F5788D5810EBA7BA58737DE1548 A8ECACD014598BC0B143E041B170525 52
	Certificate Serial number	01
	Applied policy	ETSI EN 319 411-1 V1.2.2, LCP

<sup>1</sup> In the following termed shortly „TÜViT“

<sup>2</sup> <http://www.dakks.de/en/content/accredited-bodies-dakks?Regnr=D-ZE-12022-01-01>

The audit was performed as full period of time audit at the TSP's location in Netphen, Germany. It took place from 2019-04-08 until 2019-04-11 as well as on 2019-11-27 and covered the period from 2018-11-28 until 2019-11-27. The audit was performed according to the European Standards "ETSI EN 319 411-1, V1.2.2 (2018-04)" and "ETSI EN 319 401, V2.2.1 (2018-04)" as well as CA Browser Forum Requirements "Baseline Requirements, version 1.6.3" considering the requirements of the "ETSI EN 319 403, V2.2.2 (2015-08)" for the Trust Service Provider Conformity Assessment.

The audit was based on the following policy and practice statement documents of the TSP:

1. Deutsche Telekom Corporate PKI (DTAG cPKI) – Certificate Policy (CP) & Certificate Practice Statement (CPS) – Zertifizierungsrichtlinie und Erklärung zum Zertifikatsbetrieb, Version 05.00 as of 2019-11-08

The Sub-CAs that have been issued by the aforementioned Root-CA and that have been covered by this audit are listed in table 1 below. The TSP assured that all non-revoked Sub-CA's that are technically capable of issuing server or email certificates and that have been issued by this Root-CA are in the scope of regular audits.

The CA "Deutsche Telekom AG Issuing CA 01" has stopped the issuance of certificates on 2018-04-18. During the audit, it was verified that this CA is issuing revocation status information but not any new end entity certificates.

In the following areas, non-conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:

7.9 Incident management

Documentation and implementation of the processes regarding logging functions shall be improved. [ETSI EN 319 401, REQ-7.9-04]

Findings with regard to ETSI EN 319 411-1/2:

6.5.2 Private key protection and cryptographic module engineering controls

Documentation and implementation of processes regarding HSM management shall be improved. [ETSI EN 319 411-1, GEN-6.5.2-06]

All non-conformities have been closed before the issuance of this attestation.

This Audit Attestation also covers the following incidents as documented under

- Bug 1455137, T-Systems: Undisclosed Intermediate certificate:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=1455137](https://bugzilla.mozilla.org/show_bug.cgi?id=1455137)
- Bug 1536082, T-Systems: Insufficient serial number entropy:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=1536082](https://bugzilla.mozilla.org/show_bug.cgi?id=1536082)

The remediation measures taken by T-Systems as described on Bugzilla (see link above) have been accompanied by the auditors and showed to properly address the incident. The long-term effectiveness of the measures will be rechecked at the next regular audit.

This template (version 2.2 as of 2019-05-28) was approved for use by ACAB-c.

Identification of the Sub-CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number	Applied policy	Service	EKU	Validity
Deutsche Telekom AG Issuing CA 01	C=DE, O=Deutsche Telekom AG, OU=Trust Center, CN=Deutsche Telekom AG Issuing CA 01	C6193077C6189 D1DFBBF813B87 DC7CBF0498ACF 727887BC7EC54 320906DE9BC8	EEDB860E523B2 E43	LCP	Signature, encryption	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)	2016-07-13 until 2026-07-13
Deutsche Telekom AG secure email CA	C=DE, O=Deutsche Telekom AG, OU=Trust Center, CN=Deutsche Telekom AG secure email CA	D0805A3E6A628 E9405613023DE8 7827A76118DC11 6B64903D3E75B 9DDF4BDB97	1531B1A1347C85 A97A37F60EBB5 0FD86	LCP	Signature, encryption	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)	2019-04-09 until 2029-04-09
Deutsche Telekom AG secure email CA	C=DE, O=Deutsche Telekom AG, OU=Trust Center, CN=Deutsche Telekom AG secure email CA	1ACF28AA8C530 3EFE5C30118623 936B6F501F94D3 BB7AD35B810B7 64345F4F01	7581AA9F9830A3 ABBF5BB69F84D 856	LCP	Signature, encryption	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)	2018-01-18 until 2028-01-18

**Table 1: Sub-CA's issued by the Root-CA**

**Modifications record**

<b>Version</b>	<b>Issuing Date</b>	<b>Changes</b>
Version 1.0	2020-01-23	Initial attestation
Version 1.1	2020-01-24	Editorial corrections

**End of the audit attestation letter.**

