# Audit Attestation for

# T-Systems International GmbH

## Reference: AA2019072605

Essen, 26.07.2019

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 "**AA2019072605**" and consist 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. Anja Wiedemann | Matthias Wiedenhorst |
| Reviewer | Leadauditor |

| Identification of the conformity assessment body (CAB): | TÜV Informationstechnik GmbH[1], Langemarckstraße 20, 45141 Essen, Germany<br>registered under HRB 11687, Amtsgericht Essen, Germany<br>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)". | |
|---|---|---|

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

| Identification of the audited Root-CA: | TeleSec GlobalRoot Class 3 G2 | |
|---|---|---|
| | Distinguished Name | CN = TeleSec GlobalRoot Class 3 G2<br>OU = T-Systems Trust Center<br>O = T-Systems International GmbH<br>C = DE |
| | SHA-256 fingerprint | A9 8F 81 D0 76 0A 62 D0 C3 E7 C1 C5 CF EF 2F 19 AC C5 58 03 57 6F 0F CB 5B 79 03 B8 07 AE 76 6C |
| | Certificate Serial number | 2C 87 1D 8E A0 07 19 FE |
| | Applied policy | EVCP of ETSI EN 319 411-1<br>QCP-w of ETSI EN 319 411-2 |

---

[1] In the following termed shortly „TÜViT"

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

This template (version 2 as of 2018-03-05) was approved for use by ACAB-c. It may only be used to without modification.

The audit was performed as full period of time audit at the TSP's locations in Netphen, Germany. It took place from 2019-04-08 until 2019-04-12 and 2019-05-08 and 2019-05-09 and covered the period from May 18th, 2018 until May 9th 2019. The audit was performed according to the European Standards "ETSI EN 319 411-2, V2.2.2 (2018-04)", "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 "EV SSL Certificate Guidelines, version 1.6.8" and "Baseline Requirements, version 1.6.4" 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. CP/CPS TeleSec ServerPass, Zertifizierungsrichtlinie und Erklärung zum Zertifizierungsbetrieb (CP/CPS), Version 10.00 as of 2018-10-16, T-Systems International GmbH

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.

This template (version 2 as of 2018-03-05) was approved for use by ACAB-c. It may only be used to without modification.

Pending major non-conformities have been closed, if any.

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:

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]

Findings with regard to ETSI EN 319 411-2:

6.3 Certificate Life-Cycle operational requirements

Documentation and implementation of the X.509 "ExpiredCertsonCRL" extension shall be improved. [ETSI EN 319 411-2, CSS-6.3.10-05]

All minor non-conformities are scheduled for remediation within three months after the onsite audit and will be covered by a corresponding audit.

This Audit Attestation also covers the following incidents as documented under

- Bug 1391074, T-Systems: Non-BR-Compliant Certificate Issuance
  https://bugzilla.mozilla.org/show_bug.cgi?id=1391074
- Bug 1498463, T-Systems: Improperly encoded QCStatements extension
  https://bugzilla.mozilla.org/show_bug.cgi?id=1498463

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 as of 2018-03-05) was approved for use by ACAB-c. It may only be used to without modification.

| Identification of the Sub-CA | Distinguished Name | SHA-256 fingerprint | Certificate Serial number OID | Applied policy | Service | EKU | Validy |
|---|---|---|---|---|---|---|---|
| TeleSec ServerPass CA 3 G2 | CN = TeleSec ServerPass CA 3 G2 OU = T-Systems Trust Center O = T-Systems International GmbH C = D | 5F F1 EA D6 DD FA DD 77 D9 6B BE 8E 22 D5 78 C6 EF DC AD CF 05 94 2E A2 04 D3 84 0A C7 D4 AF 1E | 00 EC 8C 2C 2F 6D 18 E3 73 | policy EVCP of ETSI-EN 319 411-1 policy QCP-w of ETSI-EN 319 411-2 | Server authentication | Not defined | 28 June 2016 to 28 June 2026 |

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

**Modifications record**

| Version | Issuing Date | Changes |
|---|---|---|
| Version 1.0 | 2019-07-26 | Initial attestation |

**End of the audit attestation letter.**