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
Phone: +49 (0) 201 / 8999-9

With best regards,

Dr. Silke Keller
Reviewer

Matthias Wiedenhorst
Lead Auditor
Identification of the conformity assessment body (CAB):

| 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)”.

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 | 91E2F5788D5810EBA7BA58737DE1548A8ECACD014598BC0B143E041B17052552

| Certificate Serial number | 01

| Applied policy | ETSI EN 319 411-1 V1.2.2, LCP

¹ In the following termed shortly „TÜViT“

This template (version 2.2 as of 2019-05-28) was approved for use by ACAB-c.
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 1536082, T-Systems: Insufficient serial number entropy: 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.
<table>
<thead>
<tr>
<th>Identification of the Sub-CA</th>
<th>Distinguished Name</th>
<th>SHA-256 fingerprint</th>
<th>Certificate Serial number</th>
<th>Applied policy</th>
<th>Service</th>
<th>EKU</th>
<th>Validity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deutsche Telekom AG Issuing CA 01</td>
<td>C=DE, O=Deutsche Telekom AG, OU=Trust Center, CN=Deutsche Telekom AG Issuing CA 01</td>
<td>C6193077C6189D1DFBBF813B87DC7CBF0498ACF727887BC7EC54320906DE9BC8</td>
<td>EEDB8860E523B2E43</td>
<td>LCP</td>
<td>Signature, encryption</td>
<td>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)</td>
<td>2016-07-13 until 2026-07-13</td>
</tr>
<tr>
<td>Deutsche Telekom AG secure email CA</td>
<td>C=DE, O=Deutsche Telekom AG, OU=Trust Center, CN=Deutsche Telekom AG secure email CA</td>
<td>D0805A3E6A628E9405613023DE87827A76118DC116B64903D3E75B9DDF4BDB97</td>
<td>1531B1A1347C85A97A37F60EBB50FD86</td>
<td>LCP</td>
<td>Signature, encryption</td>
<td>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)</td>
<td>2019-04-09 until 2029-04-09</td>
</tr>
<tr>
<td>Deutsche Telekom AG secure email CA</td>
<td>C=DE, O=Deutsche Telekom AG, OU=Trust Center, CN=Deutsche Telekom AG secure email CA</td>
<td>1ACF28AA8C5303EFE5C30118623936B6F501F94D3BB7AD35B810B764345F4F01</td>
<td>7581AA9F9830A3ABB5BB69F84D856</td>
<td>LCP</td>
<td>Signature, encryption</td>
<td>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)</td>
<td>2018-01-18 until 2028-01-18</td>
</tr>
</tbody>
</table>

Table 1: Sub-CA’s issued by the Root-CA

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Issuing Date</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0</td>
<td>2020-01-23</td>
<td>Initial attestation</td>
</tr>
<tr>
<td>Version 1.1</td>
<td>2020-01-24</td>
<td>Editorial corrections</td>
</tr>
</tbody>
</table>

End of the audit attestation letter.