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

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
www.tuvit.de

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

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

Management Board
Dirk Kretzschmar
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:  
TeleSec GlobalRoot Class 3 G2

| Distinguished Name | CN = TeleSec GlobalRoot Class 3 G2  
|                    | OU = T-Systems Trust Center  
|                    | O = T-Systems International GmbH  
|                    | 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  
|                | QCP-w of ETSI EN 319 411-2

¹ In the following termed shortly „TÜViT“  

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.
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.
<table>
<thead>
<tr>
<th>Identification of the Sub-CA</th>
<th>Distinguished Name</th>
<th>SHA-256 fingerprint</th>
<th>Certificate Serial number OID</th>
<th>Applied policy</th>
<th>Service</th>
<th>EKU</th>
<th>Validy</th>
</tr>
</thead>
<tbody>
<tr>
<td>TeleSec ServerPass CA 3 G2</td>
<td>CN = TeleSec ServerPass CA 3 G2 OU = T-Systems Trust Center O = T-Systems International GmbH C = D</td>
<td>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</td>
<td>00 EC 8C 2C 2F 6D 18 E3 73</td>
<td>policy EVCP of ETSI-EN 319 411-1 policy QCP-w of ETSI-EN 319 411-2</td>
<td>Server authentication</td>
<td>Not defined</td>
<td>28 June 2016 to 28 June 2026</td>
</tr>
</tbody>
</table>

Table 1: Sub-CA's issued by the Root-CA
## 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>2019-07-26</td>
<td>Initial attestation</td>
</tr>
</tbody>
</table>

End of the audit attestation letter.