Audit Attestation for

T-Systems International GmbH

Reference: AA2019082101

Essen, 21.08.2019

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 "**AA2019082101**" 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. Silke Keller	Matthias Wiedenhorst
Reviewer	Leadauditor

Identification of the conformity assessment body (CAB):	TÜV Informationstechnik GmbH[1], Langemarckstraße 20, 45141 Essen, Germany registered under HRB 11687, Amtsgericht Essen, Germany 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, registered under "HRB 55933" at Amtsgericht Frankfurt am Main, Germany.

Identification of the audited Root-CA:	Baltimore CyberTrust Root	
	Distinguished Name	CN=Baltimore CyberTrust Root OU=CyberTrust O=Baltimore C=IE
	SHA-256 fingerprint	16AF57A9F676B0AB126095AA5EBADE F22AB31119D644AC95CD4B93DBF3F2 6AEB
	Certificate Serial number	020000B9
	Applied policy	OVCP OF ETSI EN 319 411-1

---

[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 319 411-1, 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 1.6.4" 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-CA that has been issued by the aforementioned Root-CA and that has been covered by this audit is listed in table 1 below. The Root CA "Baltimore CyberTrust Root" is not operated by T-Systems and has **not** been in the scope of this audit. Only the mentioned Issuing CA "TeleSec ServerPass CA 2" is covered by this audit attestation.

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]

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

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 2	CN=TeleSec ServerPass CA 2 OU=Trust Center Services O=T-Systems International GmbH C=DE	49BBF728C00CF CF5B443D66DE9 D3811F64F829B1 1D8DB5B186ACA 27B8AC2F294	0727B216	policy OVCP of ETSI EN 319 411-1	server authentication	1.3.6.1.5.5.7.3. 1 (id-kp-serverAuth) 1.3.6.1.5.5.7.3. 2 (id-kp-clientAuth)	2014-07-09 to 2021-07-09

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

Modifications record

Version	Issuing Date	Changes
Version 1.0	2019-08-21	Initial attestation

End of the audit attestation letter.