



Audit Attestation for

T-Systems International GmbH

Reference: AA2019072602

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 "**AA2019072602**" and consist of 7 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
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
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 Kretschmar

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:	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	91 E2 F5 78 8D 58 10 EB A7 BA 58 73 7D E1 54 8A 8E CA CD 01 45 98 BC 0B 14 3E 04 1B 17 05 25 52
	Certificate Serial number	01
	Applied policy	OVCP & NCP 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>

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. Public Key Service, Certificate Practice Statement, Version 3.5 as of 2018-08-01, T-Systems International GmbH
2. Trust Center Solutions, TeleSec Shared-Business-CA, Certificate Policy (CP) and Certification Practice Statement (CPS), Version 6.00 as of 2018-10-11, T-Systems International GmbH
3. 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]

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 1530718, T-Systems: Invalid SAN Entries
https://bugzilla.mozilla.org/show_bug.cgi?id=1530718

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.

Identification of the Sub-CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number OID	Applied policy	Service	EKU	Validly
TeleSec GlobalRoot Class 2 G2	CN = TeleSec GlobalRoot Class 2 G2 OU = T-Systems Trust Center O = T-Systems International GmbH C = DE	05 50 3F 08 D2 DC 8E DD 24 67 CD 21 1E 6D C3 56 BB 1B 78 69 FE A2 B6 2F 69 7D C1 36 B7 96 06 75	27 12 C0 61 05 E5 5F 37 F6 C2 93 15 C4 05 24 3F	policy OVCP of ETSI EN 319 411-1	Cross certificate	Not defined	12 Feb 2019 to 12 Feb 2029
TeleSec Business CA 1	CN = TeleSec Business CA 1 OU = T-Systems Trust Center O = T-Systems International GmbH C = DE	44 EB F0 12 3E 27 FF 1D B0 49 7B D2 DA E1 81 55 B2 A4 14 E6 BC D9 C6 C8 FB 8F 48 39 84 49 B9 E9	48 8D 02 5D D6 F4	policy OVCP & NCP of ETSI EN 319 411-1	signature, encryption, server authentication	Not defined	29 Nov 2012 to 29 Nov 2024

TeleSec ServerPass Class 2 CA	CN = TeleSec ServerPass Class 2 CA STREET = Untere Industriestr. 20 L = Netphen PostalCode = 57250 S = Nordrhein Westfalen OU = T-Systems Trust Center O = T-Systems International GmbH C = DE	AC 1E C5 56 31 8E 3E A7 0F 8F 04 E0 3A 0F 26 33 BF E7 39 92 35 9A 81 01 45 FF DF 1A 42 73 96 EE	7E 39 C7 AD 1D D9 F0 43	policy OVCP of ETSI EN 319 411-1	Server authentication	Not defined	11 Feb 2014 to 11 Feb 2024
TeleSec PKS CA 8	CN = TeleSec PKS CA 8 OU = T-Systems Trust Center O = T-Systems International GmbH C = DE	D4 86 BF A3 F0 0D 16 5E E2 CF 62 70 FD A7 D0 08 17 E5 8C DA 2D F4 FA 25 6E 0F 2E B1 22 CF 8F 02	34 1B 47 75 2B 0F E2 7C E8 64 55 76 91 F2 9A 44	policy NCP+ of ETSI EN 319 411-1	Authentication, signature encryption	1.3.6.1.5.5.7.3.2 (id-kp-clientAuth) 1.3.6.1.5.5.7.3.4 (id-kp-emailProtection) 1.3.6.1.5.5.7.3.9 (id-kp-OCSPSigning) 1.3.6.1.4.1.311.20.2.2 (Smartcard logon)	20 Mar 2019 to 2 Oct 2033

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

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

Modifications record

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

End of the audit attestation letter.