Audit Attestation for

T-Systems International GmbH

Reference: AA2019072606

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 “**AA2019072606**” and consist of 8 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

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:	Deutsche Telekom Root CA 2	

	Distinguished Name	CN = Deutsche Telekom Root CA 2
		OU = T-TeleSec Trust Center
		O = Deutsche Telekom AG
		C = DE

	SHA-256 fingerprint	B6 19 1A 50 D0 C3 97 7F 7D A9 9B CD AA C8 6A 22 7D AE B9 67 9E C7 0B A3 B0 C9 D9 22 71 C1 70 D3
	Certificate Serial number	26
	Applied policy	NCP+, NCP & 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

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.

The TSP demonstrated that the CA "Shared Business CA 3" is deactivated, only used to issue revocation status information and that it had not issued any certificates during the audit period.

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:

6.2 Identification and authentication

Documentation and implementation of the processes regarding the revocation of a certificate and the change of the status information of that certificate and issuance of CRLs shall be improved. [ETSI EN 319 411-1, REV-6.2.4-04, CSS-6.3.9-05]

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
- 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.

Identification of the Sub-CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number OID	Applied policy	Service	EKU	Validy
T-TeleSec GlobalRoot Class 2	CN = T-TeleSec GlobalRoot Class 2 OU = T-Systems Trust Center O = T-Systems Enterprise Services GmbH C = DE	09 BC 51 51 7A 97 F6 63 39 E2 4D 77 E9 CA BE 4E 46 69 5C 2E C1 B4 2A 23 9E 1E FB A7 B7 2F 32 8F	11 9C 14 8C C1 AC 0E 95	policy NCP & OVCP of ETSI EN 319 411-1	Cross certificate	Not defined	25 Apr 2016 to 9 July 2019
TeleSec PKS CA 7:PN	CN = TeleSec PKS CA 7:PN OU = Trust Center Deutsche Telekom O = T-Systems International GmbH C = DE	10 C6 91 8C 58 ED 94 DD 6A 6B 51 58 8C 40 1F A2 C8 EB 4C C6 D4 0F 12 5F FA D4 14 96 12 8D 7B 58	00 B6 98 01 67	policy NCP+ of ETSI EN 319 411-1	Authentication, signature encryption	Not defined	9 June 2016 to 9 July 2019

Shared Business CA 4	CN = Shared Business CA 4 STREET = Untere Industriestr. 20 L = Netphen PostalCode = 57250 S = Nordrhein Westfalen OU = T-Systems Trust Center O = T-Systems International GmbH C = DE	5C 7D 59 57 F5 56 46 15 42 B6 5B 2D B6 D5 9F EA 1A E0 32 7D D8 18 14 3A 2E 2C 21 6D 07 15 44 22	30 15 8B 58 CD 56 31 F5	policy NCP & OVCP of ETSI EN 319 411-1	signature, encryption, server authentication	Not defined	11 Feb 2014 to 9 July 2019
Shared Business CA 3	CN = Shared Business CA 3 OU = T-Systems Trust Center O = T-Systems International GmbH C = DE	D8 02 2A 38 FD 51 AA A4 F7 9E 2E 95 22 5B 5B 8A CC 71 A8 28 9E D7 91 79 97 AE 70 15 40 88 8D 96	03 81 0F 39 E0 0C B4	policy NCP & OVCP of ETSI EN 319 411-1	Not active any more	Not defined	4 Sept 2012 to 9 July 2019 not issuing certificates any more

TeleSec ServerPass DE-2	CN = Telesec ServerPass DE-2 STREET = Untere Industriestr. 20 L = Netphen PostalCode = 57250 S = Nordrhein Westfalen OU = T-Systems Trust Center O = T-Systems International GmbH C = DE	0E 11 76 3E 42 9E 42 28 67 F9 2D 79 BB 14 0B 86 C1 E4 6D 50 E0 B2 E8 B9 D5 23 0E 56 A1 F7 FD B5	00 c7 5e 01 58 2a c3 be e7	policy OVCP of ETSI EN 319 411-1	server authentication	Not defined	11 Feb 2014 to 9 July 2019

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.