Audit Attestation for

Deutsche Telekom Security GmbH

Reference: AA2020071702

Essen, 2020-07-29

To whom it may concern,

This is to confirm that “TÜV Informationstechnik GmbH” has audited the CAs of “Deutsche Telekom Security GmbH” without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number “**AA2020071702**” 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. Silke Keller
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):	Deutsche Telekom Security GmbH, Bonner Talweg 100, 53113 Bonn, Germany, registered under “HRB 15241” at Amtsgericht Bonn, Germany Postal address: Deutsche Telekom Security GmbH, Trust Center & ID Solutions, Untere Industriestr. 20, 57250 Netphen, Germany

Identification of the audited Root-CA:	T-TeleSec GlobalRoot Class 2	
	Distinguished Name	C=DE, O=T-Systems Enterprise Services GmbH, OU=T-Systems Trust Center, CN=T-TeleSec GlobalRoot Class 2
	SHA-256 fingerprint	91E2F5788D5810EBA7BA58737DE1548A8EC ACD014598BC0B143E041B17052552
	Applied policy	ETSI EN 319 411-1 V1.2.2, LCP, NCP, NCP+, OVCP

[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 partly as a remote audit using video conference with screen sharing functionality and partly at the TSP's location in Netphen, Germany and Frankfurt am Main, Germany. It took place on 2020-02-27, from 2020-03-23 until 2020-03-26, from 2020-03-30 until 2020-04-01 and on 2020-07-08 and covered the period from 2019-05-10 until 2020-05-09. 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 "Baseline Requirements, version 1.6.8" 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), Deutsche Telekom Security GmbH, version 13.00 as of 2020-06-04
2. Trust Center Solutions, TeleSec Shared-Business-CA, Zertifizierungsrichtlinie (Certificate Policy, CP) und Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS), Deutsche Telekom Security GmbH, version 10.00 as of 2020-05-29
3. Deutsche Telekom PKS – Certificate Practice Statement (CPS), Deutsche Telekom Security GmbH, version 07.00 as of 2020-07-01
4. Deutsche Telekom Corporate PKI (DTAG cPKI) – Certificate Policy (CP) & Certificate Practice Statement (CPS) – Zertifizierungsrichtlinie und Erklärung zum Zertifikatsbetrieb, Deutsche Telekom Security GmbH, Version 07.00 as of 2020-07-01

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in table 1 and that been covered in this audit.

In the following areas, non-conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:

7.8 Network security

Documentation and implementation of configuration review shall be improved. [REQ-7.8-06]
https://bugzilla.mozilla.org/show_bug.cgi?id=1651611

Findings with regard to ETSI EN 319 411-1:

6.5.5 Computer security controls

Same issue as for ETSI EN 319 401 above. Documentation and implementation of configuration review shall be improved. [GEN-6.5.5-03]
https://bugzilla.mozilla.org/show_bug.cgi?id=1651611

Findings with regard to ETSI EN 319 411-2:
None.

All non-conformities have been closed before the issuance of this attestation.

This Audit Attestation also covers the following incidents as documented under

- Bug 1551371, T-Systems: "Some-State" in stateOrProvinceName: https://bugzilla.mozilla.org/show_bug.cgi?id=1551371
- Bug 1567456, T-Systems: "Some-State" comparable issues: https://bugzilla.mozilla.org/show_bug.cgi?id=1567456
- Bug 1578417, T-Systems: Issue with Organization field: https://bugzilla.mozilla.org/show_bug.cgi?id=1578417
- Bug 1649941, T-Systems: Incorrect OCSP Delegated Responder Certificate: https://bugzilla.mozilla.org/show_bug.cgi?id= 1649941

The remediation measures taken by Deutsche Telekom Security GmbH as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident. The long-term effectiveness of the measures will be rechecked at the next regular audit.

Distinguished Name	SHA-256 fingerprint	Applied policy	EKU
C=DE, O=Deutsche Telekom AG, OU=Trust Center, CN=Deutsche Telekom AG Issuing CA 01	C6193077C6189D1DFBBF813B87DC7CBF0498ACF727887BC7EC54320906DE9BC8	ETSI EN 319 411-1 V1.2.2, LCP	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)
C=DE, O=Deutsche Telekom AG, OU=Trust Center, CN=Deutsche Telekom AG secure email CA	D0805A3E6A628E9405613023DE87827A76118DC116B64903D3E75B9DDF4BDB97	ETSI EN 319 411-1 V1.2.2, LCP	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)
C=DE, O=Deutsche Telekom AG, OU=Trust Center, CN=Deutsche Telekom AG secure email CA	1ACF28AA8C5303EFE5C30118623936B6F501F94D3BB7AD35B810B764345F4F01	ETSI EN 319 411-1 V1.2.2, LCP	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)
C=DE, O=Deutsche Telekom AG, CN=Deutsche Telekom AG secure email CA E02	029379118E5775226C54D7182A367A240B51770F5011BB35177CFD17D9B2445A	ETSI EN 319 411-1 V1.2.2, LCP	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)

Distinguished Name	SHA-256 fingerprint	Applied policy	EKU
C=DE, O=T-Systems International GmbH, OU=T-Systems Trust Center, CN=TeleSec Business CA 1	44EBF0123E27FF1DB0497BD2DAE18155B2A414E6BCD9C6C8FB8F48398449B9E9	ETSI EN 319 411-1 V1.2.2, NCP, OVCP	not defined
C=DE, O=T-Systems International GmbH, OU=T-Systems Trust Center, CN=TeleSec PKS CA 8	D486BFA3F00D165EE2CF6270FDA7D00817E58CDA2DF4FA256E0F2EB122CF8F02	ETSI EN 319 411-1 V1.2.2, NCP+	id-kp-clientAuth (1.3.6.1.5.5.7.3.2) id-kp-emailProtection (1.3.6.1.5.5.7.3.4) id-kp-OCSPSigning (1.3.6.1.5.5.7.3.9) Smartcard logon (1.3.6.1.4.1.311.20.2.2)
C=DE, O=T-Systems International GmbH, OU=T-Systems Trust Center, ST=Nordrhein Westfalen, PostalCode=57250, L=Netphen, STREET=Untere Industriestr. 20, CN=TeleSec ServerPass Class 2 CA	AC1EC556318E3EA70F8F04E03A0F2633BFE73992359A810145FFDF1A427396EE	ETSI EN 319 411-1 V1.2.2, OVCP	not defined

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

Modifications record

Version	Issuing Date	Changes
Version 1.0	2020-07-17	Initial attestation
Version 1.1	2020-07-29	Correction of a typing error in the audit period date

End of the audit attestation letter.