



Audit Attestation for

Deutsche Telekom Security GmbH

Reference: AA2020112305

Essen, 2020-11-23

To whom it may concern,

This is to confirm that "TÜV Informationstechnik GmbH" has audited the key destruction of four CAs of "Deutsche Telekom Security GmbH" without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number "AA2020112305" and consists of 4 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: certuivit@tuvit.de
Phone: +49 (0) 201 / 8999-9

With best regards,

Dr. Silke Keller
Reviewer

Matthias Wiedenhorst
Lead auditor

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 Kretzschmar

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 affected 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	91E2F5788D5810EBA7BA58737DE1548A8ECACD014598BC0B143E041B17052552

The audit was performed as a point in time key destruction audit at the TSP’s location in Netphen, Germany. It took place on 2020-11-12. The audit was performed considering the requirements of the “ETSI EN 319 403, V2.2.2 (2015-08)” for the Trust Service Provider Conformity Assessment.

During the key destruction ceremony on 2020-11-12, the TSP deleted the key pairs of the Sub-CAs “Deutsche Telekom AG secure email CA E02”, “Deutsche Telekom AG secure email CA” (s/n 7581aa9f9830a3abbf5bb69f84d856), “Deutsche Telekom AG secure email CA” (s/n 1531b1a1347c85a97a37f60ebb50fd86) and “Deutsche Telekom AG Issuing CA 01” from all its operational HSMs. The two Sub-CAs with the CN “Deutsche Telekom AG secure email CA” share the same key pair. Backup copies were present on two dedicated backup HSMs. After a safeguarding phase but still during the audit, the TSP deleted these two backup copies also under attendance of the auditor.

The TSP assured that no further backup copies exist. The audit did not reveal any indication for doubts with regard to this assurance.

¹ In the following termed shortly „TÜViT“

² <http://www.dakks.de/en/content/accredited-bodies-dakks?Regnr=D-ZE-12022-01-01>

Distinguished Name	SHA-256 fingerprint	Applied policy	EKU
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)
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, 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 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)

Table 1: Sub-CAs for which key destruction has been audited

Modifications record

Version	Issuing Date	Changes
Version 1.0	2020-11-23	Initial attestation

End of the audit attestation letter.