

The certification body of TÜV Informationstechnik GmbH
hereby awards this certificate to the company

Deutsche Telekom Security GmbH
Untere Industriestraße 20
57250 Netphen, Germany

to confirm that its trust service

TeleSec cPKI

fulfils all requirements defined in the standard (EN)

ETSI EN 319 411-1 V1.2.2 (2018-04),
policy LCP.

The appendix to the certificate is part of the certificate and
consists of 3 pages.

The certificate is valid only in conjunction with the evaluation
report.



Certificate ID: 67126.20

© TÜVIT - TÜV NORD GROUP - www.tuvit.de

Certificate validity:
2020-07-01 – 2022-07-01

Essen, 2020-07-01

Dr. Christoph Sutter
Head of Certification Body

TÜV Informationstechnik GmbH

TÜV NORD GROUP
Langemarckstr. 20
45141 Essen, Germany
www.tuvit.de



Certificate

Certification Scheme

The certification body of TÜV Informationstechnik GmbH is accredited by “DAkKS Deutsche Akkreditierungsstelle GmbH” according to EN ISO/IEC 17065 for the scopes IT security and security technology product certification. The certification body performs its certification on the basis of the following accredited certification system:

- “Certification System (accredited scope) of the certification body of TÜV Informationstechnik GmbH”, version 2.1 as of 2020-03-01, TÜV Informationstechnik GmbH

Evaluation Report

- „Audit Report – Re-Certification – ETSI EN 319 411-1, TUVIT-CA67126, TeleSec cPKI“, version 2.0 as of 2020-06-29, TÜV Informationstechnik GmbH

Evaluation Requirements

The evaluation requirements are defined in the standard ETSI EN 319 411-1

- ETSI EN 319 411-1 V1.2.2 (2018-04): „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements“, Version 1.2.2, 2018-04, European Telecommunications Standards Institute

The applicable ETSI Certificate Policy is:

- LCP: Lightweight Certificate Policy

Evaluation Target

The target of evaluation is characterized by the certificate information of the inspected trust service:

TeleSec cPKI:

Issuer of CA certificate (Root CA or Intermediate CA): CN = T-TeleSec GlobalRoot Class 2 Certificate Serial Number: 01	
Name of CA (as in certificate)	serial number of certificate
CN = Deutsche Telekom AG Issuing CA 01	EEDB860E523B2E43
CN = Deutsche Telekom AG secure email CA	1531B1A1347C85A97A37F60EBB50FD86
CN = Deutsche Telekom AG secure email CA	7581AA9F9830A3ABBF5BB69F84D856
CN = Deutsche Telekom AG secure email CA E02	34D22925006C85582FE89B82D7976D59

together with the documentation of the operator:

- “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, Deutsche Telekom Security GmbH
- “Deutsche Telekom Corporate PKI (DTAG cPKI) – PKI-Offenlegungspflichten (PKI Disclosure Statement (PDS))“, version 3.0 as of 2019-10-18, T-Systems International GmbH
- “Nutzungsbedingungen (Terms of Use) der Corporate PKI (cPKI) der Deutschen Telekom AG“, version 2.0 as of 2019-10-17, T-Systems International GmbH

Evaluation Result

- The target of evaluation fulfills all applicable evaluation requirements.
- The certification requirements defined in the certification system are fulfilled.

Summary of the Evaluation Requirements

ETSI EN 319 411-1 contains requirements for Trust Service Providers practice under the following headlines:

- 1 Publication and repository responsibilities**
- 2 Identification and authentication**
- 3 Certificate Life-Cycle operational requirements**
- 4 Facility, management, and operational controls**
- 5 Technical security controls**
- 6 Certificate, CRL, and OCSP profiles**
- 7 Compliance audit and other assessment**
- 8 Other business and legal matters**
- 9 Other provisions**