

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

DTAG CorporatePKI

fulfils all requirements defined in the standard

ETSI EN 319 411-1, V1.3.1 (2021-05)
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.



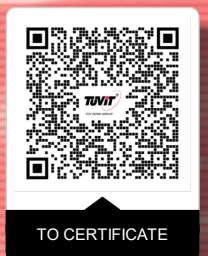
Certificate validity:
2022-07-01 – 2024-07-01

Certificate ID: 67143.22
© TÜVIT – TÜV NORD GROUP – www.tuvit.de

Essen, 2022-07-01

Dr. Christoph Sutter
Head of Certification Body

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Am TÜV 1
45307 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 3.0 as of 2022-04-06, TÜV Informationstechnik GmbH

Evaluation Report

- „Audit Report – Re-Certification – ETSI EN 319 411-1, TUVIT-CA67143, DTAG CorporatePKI“, version 2.1 as of 2022-07-01, TÜV Informationstechnik GmbH

Evaluation Requirements

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

- ETSI EN 319 411-1 V1.3.1 (2021-05): „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (V1.3.1 2021-05)“, version V1.3.1, 2021-05-01, 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:

DTAG CorporatePKI:

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 secure email CA E03	39EC6CFC261ACF BE898FA145705C 9B0A

together with the documentation of the operator:

- Deutsche Telekom Corporate PKI (DTAG cPKI), Certificate Policy & Certificate Practice Statement, Zertifizierungsrichtlinie und Erklärung zum Zertifizierungsbetrieb, version 11.0 as of 2022-02-17, Deutsche Telekom Security GmbH
- Deutsche Telekom Corporate PKI (DTAG cPKI), PKI Disclosure Statement (PDS), version 6.0 as of 2022-02-17, Deutsche Telekom Security GmbH
- Nutzungsbedingungen (Terms of Use) der Corporate PKI (cPKI) der Deutschen Telekom AG, version 4.0 as of 2021-11-10, Deutsche Telekom Security 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**