

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH
bescheinigt hiermit dem Unternehmen

Deutsche Telekom Security GmbH
Untere Industriestraße 20
57250 Netphen

für den Vertrauensdienst

TeleSec Public Key Service

die Erfüllung aller relevanten Anforderungen der Norm (EN)

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

Die Anlage zum Zertifikat ist Bestandteil des Zertifikats und besteht
aus 3 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem Prüfbericht.



Certificate ID: 67132.20

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

Zertifikatsgültigkeit:
01.07.2020 - 01.07.2022

Essen, 01.07.2020

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH

TÜV NORD GROUP
Langemarckstraße 20
45141 Essen
www.tuvit.de



Zertifikat

Zertifizierungssystem

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH ist bei der „DAkKS Deutsche Akkreditierungsstelle GmbH“ für die Zertifizierung von Produkten in den Bereichen IT-Sicherheit und Sicherheitstechnik nach DIN EN ISO/IEC 17065 akkreditiert. Die Zertifizierungsstelle führt ihre Zertifizierungen auf Basis des folgenden akkreditierten Zertifizierungssystems durch:

- „Zertifizierungssystem (akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH“, Version 2.1 vom 01.03.2020, TÜV Informationstechnik GmbH

Prüfbericht

- „Audit Report – Re-Certification – ETSI EN 319 411-1 TUVIT-CA67132, TeleSec Public Key Service“, Version 2.0 vom 29.06.2020, TÜV Informationstechnik GmbH

Prüfanforderungen

Die Prüfanforderungen sind in der Norm ETSI EN 319 411-1 definiert:

- 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

Die anwendbare ETSI Zertifizierungspolitik ist:

- NCP+: Erweiterte standardisierte Zertifizierungspolitik, die eine sichere Nutzereinheit fordert

Prüfgegenstand

Der Prüfgegenstand ist charakterisiert durch die Zertifikatsinformation zum untersuchten Vertrauensdienst:

TeleSec Public Key Service:

Aussteller des CA-Zertifikats (Root CA oder Intermediate CA): CN = T-TeleSec GlobalRoot Class 2 Zertifikatsseriennummer: 01	
Name der CA (wie im Zertifikat)	Seriennummer des Zertifikates
CN = TeleSec PKS CA 8	341B47752B0FE27 CE864557691F29 A44

zusammen mit der Dokumentation des Betreibers:

- „Deutsche Telekom PKS – Certificate Practice Statement (CPS)“, Version 07.00 vom 01.07.2020, Deutsche Telekom Security GmbH
- „T-Systems PKS,PKI Disclosure Statement (PDS)“, Version 1.0 vom 30.06.2017, T-Systems International GmbH
- „Allgemeine Geschäftsbedingungen TeleSec Public Key Service“ vom 14.10.2019, Deutsche Telekom AG

Prüfergebnis

- Der Prüfgegenstand erfüllt alle anwendbaren Anforderungen aus den Prüfkriterien.
- Die im Zertifizierungssystem definierten Zertifizierungsvoraussetzungen sind erfüllt.

Zusammenfassung der Prüfanforderungen

ETSI EN 319 411-1 enthält Anforderungen für Vertrauensdiensteanbieter (VDA) bzgl. der Tätigkeit des VDAs unter folgenden Überschriften:

- 1 Verantwortlichkeiten bzgl. Veröffentlichung und öffentlichem Verzeichnis**
- 2 Identifizierung und Authentifizierung**
- 3 Betriebsanforderungen an den Zertifikatslebenszyklus**
- 4 Anforderungen an Einrichtung, Verwaltung und Betrieb**
- 5 Technische Sicherheitsanforderungen**
- 6 Zertifikats-, Sperrlisten- (CRL-) und OCSP-Profile**
- 7 Compliance-Audit und andere Bewertungen**
- 8 Sonstige geschäftliche und rechtliche Angelegenheiten**
- 9 Sonstige Maßnahmen**