TÜVIT

Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH
bescheinigt hiermit dem Unternehmen

Deutsche Telekom Security GmbH
Untere Industriestraße 20
57250 Netphen

Zertifikatsgültigkeit:
29.10.2021 – 29.10.2023

für den Vertrauensdienst

Telekom Security Public Certificate Service Platform

die Erfüllung aller relevanten Anforderungen der Norm

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

Die Anlage zum Zertifikat ist Bestandteil des Zertifikats mit der ID 67140.21 und besteht aus 2 Seiten.
Dieses Zertifikat gilt nur in Verbindung mit dem Prüfbericht.

Essen, 26.10.2022

Dr. Christoph Sutter, Leiter Zertifizierungsstelle

Zum Zertifikat

TÜV Informationstechnik GmbH
Am TÜV 1 ▪ 45307 Essen
tuvit.de

DAkkS Deutsche Akkreditierungsstelle D-ZE-12022-01-01

TÜV®

TÜVNORDGROUP

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 Zertifizierungsprogramms durch:

- „Zertifizierungssystem (akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH“, Version 3.0 vom 06.04.2022, TÜV Informationstechnik GmbH

Prüfbericht

- „Audit Report – Surveillance Audit – ETSI EN 319 411-1, TUVIT-CA67140 A1, Telekom Security Public Certificate Service Platform“, Version 2.1 vom 24.10.2022, TÜV Informationstechnik GmbH

Prüfanforderungen

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

- 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, 01.05.2021, European Telecommunications Standards Institute

Die anwendbare ETSI Zertifizierungspolitik ist:

- DVCP: Domainvalidierende Zertifizierungspolitik.

Prüfgegenstand

Der Prüfgegenstand ist charakterisiert durch die Zertifikatsinformation zum untersuchten Vertrauensdienstes:

Telekom Security Public Certificate Service Platform

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 = Telekom Security DV RSA CA 21	2CF3C72F3F7D0FB31FC362D6B869558E

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 = Telekom Security DV RSA CA 22	2103BE2C2AA30A5B5B1F0E1A4456239A

zusammen mit der Dokumentation des Betreibers:

- Trust Center Certificate Policy, Version 02.00 vom 01.03.2022, gültig ab 02.03.2022, Deutsche Telekom Security GmbH
- Certificate Practice Statement Public, Version 03.00 vom 13.08.2022, gültig ab 22.08.2022, Deutsche Telekom Security GmbH
- Allgemeine Geschäftsbedingungen IT-Leistungen, Version vom 28.07.2022, Deutsche Telekom Security GmbH
- LEISTUNGSBESCHREIBUNG Public Certificate Service Platform (PCSP), Version 4.0 vom 15.09.2022, gültig ab 15.09.2022, Deutsche Telekom Security GmbH
- NUTZUNGSBEDINGUNGEN Public Certificate Service Platform (PCSP), Version 4.0 vom 15.09.2022, gültig ab 15.09.2022, Deutsche Telekom Security GmbH

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**