Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

T-Systems International GmbH
Untere Industriestraße 20
57250 Netphen

für den Vertrauensdienst

TeleSec cPKI

die Erfüllung aller Anforderungen der Norm (EN)

ETSI EN 319 411-1 V1.1.1 (2016-02), policy LCP.

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

Dieses Zertifikat gilt nur in Verbindung mit dem Prüfbericht.

ETSI EN 319 411-1 2019 TÜViT® Trusted Site

Certificate ID: 67103.19

Zertifikat gültig bis 23.01.2021

Essen, 23.01.2019

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

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

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

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 2.0 vom 06.06.2016, TÜV Informationstechnik GmbH

Prüfbericht

- „Evaluation Report – Initial Certification – ETSI EN 319 411-1, TUVIT-CA67103, TeleSec cPKI“, Version 1.1 vom 17.01.2019, TÜV Informationstechnik GmbH

Prüfanforderungen

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

- ETSI EN 319 411-1 V1.1.1 (2016-02): „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements“, Version 1.1.1, 2016-02, European Telecommunications Standards Institute

Die anwendbare ETSI Zertifizierungspolitik ist:

- LCP: Einfache Zertifizierungspolitik

Prüfgegenstand

Der Prüfgegenstand ist charakterisiert durch die Zertifikatsinformation zum untersuchten Vertrauensdienst:

TeleSec cPKI:

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 = Deutsche Telekom AG Issuing CA 01	00 ee db 86 0e 52 3b 2e 43
CN = Deutsche Telekom AG secure email CA	75 81 aa 9f 98 30 a3 ab bf 5b b6 9f 84 d8 56

zusammen mit der Certificate Policy (CP) und dem Certification Practice Statement (CPS) des Betreibers:

- „Deutsche Telekom Corporate PKI (DTAG cPKI) – Certificate Policy (CP) & Certificate Practice Statement (CPS) – Zertifizierungsrichtlinie und Erklärung zum Zertifikatsbetrieb“, Version 3.20 vom 20.08.2018, T-Systems International GmbH

und mit dem PKI Disclosure Statement (PDS) des Betreibers:

- „Deutsche Telekom Corporate PKI (DTAG cPKI) – PKI-Offenlegungspflichten (PKI Disclosure Statement (PDS))“, Version 1.0 vom 20.08.2018, T-Systems International GmbH

und mit den Terms of Use (ToU) des Betreibers:

- „Nutzungsbedingungen (Terms of Use)“, Version 1.0 vom 20.08.2018, 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 Vertrauensdienstanbieter (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

Gegenstand des Nachtrags

Dieser Nachtrag vom 23.01.2020 ergänzt das Zertifikat mit der Certificate ID: 67103.19 vom 23.01.2019 aufgrund des durchgeführten Überwachungsaudits.

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 2.0 vom 06.06.2016, TÜV Informationstechnik GmbH

Prüfbericht

- „Audit Report – Surveillance Onsite Inspection – ETSI EN 319 411-1, TUVIT-CA67103, TeleSec cPKI“, Version 2.1 vom 23.01.2020, TÜV Informationstechnik GmbH

Prüfanforderungen

Die Prüfanforderungen sind in der Norm ETSI EN 319 411-1 V1.2.2 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:

- LCP: Einfache Zertifizierungspolitik

Prüfgegenstand

Der Prüfgegenstand ist charakterisiert durch die Zertifikats-information zum untersuchten Vertrauensdienst:

TeleSec cPKI:

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 = Deutsche Telekom AG Issuing CA 01	EEDB860E523B2E43
CN=Deutsche Telekom AG secure email CA	1531B1A1347C85A97A37F60EBB50FD86
CN=Deutsche Telekom AG secure email CA	7581AA9F9830A3ABBF5BB69F84D856

zusammen mit der Dokumentation des Betreibers:

- „Deutsche Telekom Corporate PKI (DTAG cPKI) – Certificate Policy (CP) & Certificate Practice Statement (CPS) – Zertifizierungsrichtlinie und Erklärung zum Zertifikatsbetrieb“, Version 05.00 vom 08.11.2019, T-Systems International GmbH, Telekom Security
- „Deutsche Telekom Corporate PKI (DTAG cPKI) – PKI-Offenlegungspflichten (PKI Disclosure Statement (PDS))“, Version 3.0 vom 18.10.2019, T-Systems International GmbH, Telekom Security

- „Nutzungsbedingungen (Terms of Use) der Corporate PKI (cPKI) der Deutschen Telekom AG“, Version 2.0 vom 17.10.2019, T-Systems International GmbH, Telekom Security

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 Vertrauensdienstanbieter (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