Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH
bescheinigt hiermit dem Unternehmen

DFN-Verein e. V.
Alexanderplatz 1
10178 Berlin

für den Vertrauensdienst

DFN-PKI Sicherheitsniveau Global

die Erfüllung aller relevanten Anforderungen der Norm (EN)

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

Die Anlage zum Zertifikat ist Bestandteil des Zertifikats und besteht aus 4 Seiten.
Dieses Zertifikat gilt nur in Verbindung mit dem Prüfbericht.

ETSI EN 319 411-1 TÜVIT® 2020 Trusted Site

Certificate ID: 67133.20

Zertifikatsgültigkeit:
01.12.2020 – 19.12.2022

Essen, 01.12.2020

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 2.1 vom 01.03.2020, TÜV Informationstechnik GmbH

Prüfbericht

- „Audit Report – Re-Certification – ETSI EN 319 411-1 TUVIT-CA67133, DFN-PKI Sicherheitsniveau Global“, Version 2.0 vom 16.11.2020, 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:

- OVCP: Organisationsvalidierende Zertifizierungspolitik

Prüfgegenstand

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

DFN-PKI Sicherheitsniveau Global:

Aussteller des CA-Zertifikats (Root CA oder Intermediate CA): CN = DFN-Verein Certification Authority 2 Zertifikatsseriennummer: E30BD5F8AF25D981	
Name der CA (wie im Zertifikat)	**Seriennummer des Zertifikates**
CN = Deutscher Bundestag CA - G02	1C3AD46FEC82C025CADB5A8D
CN = DFN-Verein Global Issuing CA	1B63BAD01E2C3D
CN = Fraunhofer Service CA - G02	1B63BAB8CF33FA
CN = Fraunhofer User CA - G02	1B63BAC68B5242
CN = KIT-CA	1C3AD48C24ED922EB0F490AE
CN = MPG CA - G02	1C3AD450847EEEF358F88E77
CN = RUB-Chipcard CA G2	1B9DCDA0A1BB20DCD658CFFF
CN = TU Dortmund Chipcard CA 2	1B809DBAC8F194EBDD5D27A8
CN = TU Dresden CA	1C6E34243F3AD82C1BCC9135
CN = TU Ilmenau CA G2	1B9DCD8A84F6517B4758CCF4

zusammen mit der Dokumentation des Betreibers:

- Zertifizierungsrichtlinie der DFN-PKI – Sicherheitsniveau "Global" –, Version 8 vom 30.09.2020, DFN-Verein
- Erklärung zum Zertifizierungsbetrieb der DFN-PKI – Sicherheitsniveau "Global" -, Version 8 vom 30.09.2020, DFN-Verein
- Pflichten der Teilnehmer der DFN-PKI im Sicherheitsniveau Global, Version 2 vom 30.09.2020, DFN-Verein
- Aufgaben des Teilnehmerservice (TS) in der DFN-PKI im Sicherheitsniveau Global, Version 2 vom 30.04.2020, DFN-Verein
- Informationen für Zertifikatinhaber in der DFN-PKI im Sicherheitsniveau Global, Version 1.2 vom 15.02.2018, DFN-Verein

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