

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

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

Die Anlage zum Zertifikat ist Bestandteil des Zertifikats mit der ID 67142.22 und besteht
aus 3 Seiten.

Essen, 16.12.2022

Dr. Christoph Sutter, Leiter Zertifizierungsstelle



Zertifikatsgültigkeit:
16.12.2022 – 19.12.2024



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

Evaluierungsbericht

- „Evaluation Report – Re-Certification – ETSI EN 319 411-1, TUVIT-CA67142, DFN-PKI Sicherheitsniveau Global“, Version 2.0 vom 12.12.2022, TÜV Informationstechnik GmbH

Evaluierungsanforderungen

Die Evaluierungsanforderungen 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:

- OVCP: Organisationsvalidierende Zertifizierungspolitik.

Evaluierungsgegenstand

Der Evaluierungsgegenstand ist charakterisiert durch die Zertifikatsinformation zum untersuchten Vertrauensdienstes:

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

**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 = 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 11 vom 14.11.2022, DFN-Verein
- Erklärung zum Zertifizierungsbetrieb der DFN-PKI - Sicherheitsniveau „Global“ -, Version 11 vom 14.11.2022, DFN-Verein
- Pflichten der Teilnehmer der DFN-PKI im Sicherheitssystem Global, Version 3 vom 15.02.2022,
- 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 2, gültig ab 20.11.2020, DFN-Verein

Evaluierungsergebnis

- Der Evaluierungsgegenstand erfüllt alle anwendbaren Anforderungen aus den Evaluierungskriterien.
- Die im Zertifizierungssystem definierten Zertifizierungsvoraussetzungen sind erfüllt.

Zusammenfassung der Evaluierungsanforderungen

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**