Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

Microsec Ltd.
Ángel Sanz Briz út 13.
1033 Budapest, Ungarn

für den Vertrauensdienst

e-Szignó Qualified Website Authentication

die Erfüllung aller Anforderungen der Norm (EN)

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

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®
2019 Trusted Site

Certificate ID: 67113.19

21

Zertifikat gültig bis 07.02.2021

Essen, 16.05.2019

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 – Change Audit – ETSI EN 319 411-1, TUVIT-CA67113, e-Szignó Qualified Website Authentication“, Version 1.1 vom 06.05.2019, 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

Zusätzlich wurden folgende Kriterien bei dem Audit berücksichtigt:

„Guidelines for the issuance and management of Extended Validation Certificates“, Version 1.6.8 vom 09.03.2018

Die anwendbare ETSI Zertifizierungspolitik ist:

- EVCP: Zertifizierungspolitik mit erweiterter Validierung

Prüfgegenstand

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

e-Szignó Qualified Website Authentication:

Aussteller des CA-Zertifikats (Root CA oder Intermediate CA): CN = Microsec e-Szigno Root CA 2009 Zertifikatsseriennummer: 00 c2 7e 43 04 4e 47 3f 19	
Name der CA (wie im Zertifikat)	**Seriennummer des Zertifikates**
CN = Qualified e-Szigno TLS CA 2018	00 b8 6e df 27 d8 f6 96 7c 64 70 63 0a

Aussteller des CA-Zertifikats (Root CA oder Intermediate CA): CN = e-Szigno Root CA 2017 Zertifikatsseriennummer: 01 54 48 ef 21 fd 97 59 0d f5 04 0a	
Name der CA (wie im Zertifikat)	**Seriennummer des Zertifikates**
CN = e-Szigno Qualified TLS CA 2018	00 b7 f3 3e b7 78 eb 63 1c be 7c 80 0a

zusammen mit der Dokumentation des Betreibers:

- „e-Szignó Certification Authority eIDAS conform Qualified Certificates for Website Authentication Certificate Policy", Version 2.8, gültig ab 14.12.2018, Microsec Ltd.

- „e-Szignó Certification Authority eIDAS conform Qualified Certificate for Website Authentication Certification Practice Statement", Version 2.8, gültig ab 14.12.2018, Microsec Ltd.
- "e-Szignó Certification Authority eIDAS conform Qualified Certificate for Website Authentication Disclosure Statement", version 2.8, gültig ab 14.12.2018, Microsec Ltd.
- "General Terms and Conditions of the e-Szignó Certification Service Provider", version 1.6, gültig ab 14.12.2018, Microsec Ltd.

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