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 Website Authentication

die Erfüllung aller Anforderungen der Norm (EN)

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

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 2019 TÜVIT Trusted Site

Certificate ID: 67112.19

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-CA67112, e-Szignó 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 V1.2.2 (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

Zusätzlich wurden folgende Kriterien bei dem Audit berücksichtigt:

- „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates“, Version 1.6.3 vom 01.02.2019, CA/Browser Forum

Die anwendbaren ETSI Zertifizierungspolitiken sind:

- DVCP: Zertifizierungspolitik mit Domänenvaldierung
- OVCP: Zertifizierungspolitik mit Organisationsvalidierung
- IVCP: Zertifizierungspolitik mit Personenvalidierung

Prüfgegenstand

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

e-Szignó 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 = Online e-Szigno SSL CA 2016	00 8f 81 6e d5 51 c9 92 4e d7 8f b1 0a
CN = e-Szigno SSL CA 2014	53 5c d2 a3 ac 13 d9 dc 4a 4b 83 0a
CN = Class2 e-Szigno SSL CA 2016	00 8e 5f 46 ef 1e c4 e1 0f ca 08 16 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 Online SSL CA 2017	00 a7 99 e9 a1 b9 f1 90 5b 9b 8c e6 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 Class3 SSL CA 2017	00 a3 f1 c9 9d 52 56 9d 8d 99 2e 4c 0a
CN = e-Szigno Class2 SSL CA 2017	00 a6 e9 4d 04 b3 bc a2 dc 1a d6 9d 0a

zusammen mit der Dokumentation des Betreibers:

- „e-Szignó Certification Authority eIDAS conform Certificate for Website Authentication Certificate Policies“, Version 2.8, gültig ab 14.12.2018, Microsec Ltd.
- „e-Szignó Certification Authority eIDAS conform Certificate for Website Authentication Certification Practice Statement“, Version 2.8, gültig ab 14.12.2018, Microsec Ltd.
- „e-Szignó Certification Authority eIDAS conform Certificate for Website Authentication Disclosure Statement“, Version 2.8, gültig ab 14.12.2018, Microsec Ltd.
- „e-Szignó Certification Authority General Terms and Conditions“, 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 Vertrauensdienste-anbieter (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 05.02.2020 ergänzt das Zertifikat mit der Certificate ID: 67112.19 vom 16.05.2019 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

- „Evaluation Report – Surveillance Audit – ETSI EN 319 411-1, TUVIT-CA67112A2, e-Szignó Website Authentication“, Version 2.0 vom 03.02.2020, 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

Zusätzlich wurden folgende Kriterien bei dem Audit berücksichtigt:

- „Baseline Requirements for the issuance and management of Publicly-Trusted Certificates“, Version 1.6.6 vom 09.09.2019, CA/Browser Forum

Die anwendbaren ETSI Zertifizierungspolitiken sind:

- DVCP: Domänenvalidierende Zertifizierungspolitik
- OVCP: Organisationsvalidierende Zertifizierungspolitik
- IVCP: Personenvalidierende Zertifizierungspolitik

Prüfgegenstand

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

e-Szignó Website Authentication:

Aussteller des CA-Zertifikats (Root CA oder Intermediate CA): CN = Microsec e-Szigno Root CA 2009 Zertifikatsseriennummer: 00C27E43044E473F19	
Name der CA (wie im Zertifikat)	**Seriennummer des Zertifikates**
CN = Online e-Szigno SSL CA 2016	008F816ED551C9924ED78FB10A
CN = e-Szigno SSL CA 2014	535CD2A3AC13D9DC4A4B830A
CN = Class2 e-Szigno SSL CA 2016	008E5F46EF1EC4E10FCA08160A

Aussteller des CA-Zertifikats (Root CA oder Intermediate CA): CN = e-Szigno Root CA 2017 Zertifikatsseriennummer: 015448EF21FD97590DF5040A	
Name der CA (wie im Zertifikat)	**Seriennummer des Zertifikates**
CN = e-Szigno Online SSL CA 2017	00A799E9A1B9F1905B9B8CE60A
CN = e-Szigno Class3 SSL CA 2017	00A3F1C99D52569D8D992E4C0A
CN = e-Szigno Class2 SSL CA 2017	00A6E94D04B3BCA2DC1AD69D0A

zusammen mit der Dokumentation des Betreibers:

- „e-Szignó Certification Authority eIDAS conform Certificate for Website Authentication Certificate Policies“, Version 2.11 vom 23.09.2019, gültig ab 25.09.2019, Microsec Ltd.
- „e-Szignó Certification Authority eIDAS conform Certificate for Website Authentication Certification Practice Statement“, Version 2.11 vom 23.09.2019, gültig ab 25.09.2019, Microsec Ltd.
- „e-Szignó Certification Authority eIDAS conform Certificate for Website Authentication Disclosure Statement“, Version 2.11 vom 23.09.2019, gültig ab 25.09.2019, Microsec Ltd.
- „e-Szignó Certification Authority General Terms and Conditions“, Version 1.7 vom 23.09.2019, gültig ab 25.09.2019, 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