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 NCP Certificates

die Erfüllung aller Anforderungen der Norm (EN)

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

Die Anlage zum Zertifikat ist Bestandteil des Zertifikats und besteht aus 5 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem Prüfbericht.

ETSI EN 319 411-1 2019 TÜVIT® Trusted Site

Certificate ID: 67111.19

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-CA67111, e-Szignó NCP Certificates“, 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

Die anwendbare ETSI Zertifizierungspolitiken sind:

- LCP: Einfache Zertifizierungspolitik
- NCP: Standardisierte Zertifizierungspolitik
- NCP+: Standardisierte Zertifizierungspolitik, die ein sicheres kryptograrisches Modul fordert

Prüfgegenstand

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

e-Szignó NCP Certificates:

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 = Advanced Class 3 e-Szigno CA 2009	19
CN = Advanced Code Signing Class3 e-Szigno CA 2016	00 8c 55 d8 66 52 70 2e f1 1b 33 ae 0a
CN = Advanced Pseudonymous e-Szigno CA 2009	1a
CN = Class3 KET e-Szigno CA 2018	00 bd ac 3d 35 98 4f 42 e5 56 0e 22 0a
CN = Advanced Class 2 e-Szigno CA 2009	18
CN = Advanced eIDAS Class2 e-Szigno CA 2016	00 8b 28 8a dd 98 af 79 1b 02 20 7f 0a
CN = Advanced Code Signing Class2 e-Szigno CA 2016	00 8d 8d d2 21 ee d2 53 5b 84 3e 1e 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 CA 2017	00 a2 a6 92 bf 8e 59 6b 56 02 ea 8b 0a
CN = e-Szigno Class3 CodeSigning CA 2017	00 ab 5b 68 15 64 a5 20 93 18 f6 ab 0a
CN = e-Szigno Pseudonymous CA 2017	00 a8 a6 20 7e 07 5c e7 8d 92 3a f7 0a
CN = e-Szigno Class2 CA 2017	00 a1 5a 22 e9 dc 03 5b ef e8 fd 99 0a
CN = e-Szigno Class2 CodeSigning CA 2017	00 aa 7d b8 ee 27 7d aa c2 e3 e5 cb 0a

Aussteller des CA-Zertifikats (Root CA oder Intermediate CA): CN = KGYHSZ (Public Administration Root CA - Hungary) Zertifikatsseriennummer: 43 7c 92 a4	
Name der CA (wie im Zertifikat)	**Seriennummer des Zertifikates**
CN = Signature Class 3 KET e-Szigno CA 2009	43 7c 94 a7

Zusammen mit der Dokumentation des Betreibers:

- „e-Szignó Certification Authority eIDAS conform Non-Qualified Certificate for Electronic Seal Certificate Policies“, Version 2.8, gültig ab 14.12.2018, Microsec Ltd.

- „e-Szignó Certification Authority Non eIDAS covered Certificate Certificate Policies“, Version 2.8, gültig ab 14.12.2018, Microsec Ltd.
- „e-Szignó Certification Authority eIDAS conform Non-Qualified Certificate for Electronic Signature Certificate Policies“, Version 2.8, gültig ab 14.12.2018, Microsec Ltd.
- „e-Szignó Certification Authority eIDAS conform Non-Qualified Certificate for Electronic Signature Certification Practice Statement“, Version 2.8, gültig ab 14.12.2018, Microsec Ltd.
- „e-Szignó Certification Authority eIDAS conform Non-Qualified Certificate for Electronic Seal Certification Practice Statement“, Version 2.8, gültig ab 14.12.2018, Microsec Ltd.
- „e-Szignó Certification Authority Non eIDAS covered Certificates Certification Practice Statement“, Version 2.8, gültig ab 14.12.2018, Microsec Ltd.
- „e-Szignó Certification Authority eIDAS conform Non-Qualified Certificate for Electronic Signature Disclosure Statement“, Version 2.8, gültig ab 14.12.2018, Microsec Ltd.
- „e-Szignó Certification Authority eIDAS conform Non-Qualified Certificate for Electronic Seal 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 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 05.02.2020 ergänzt das Zertifikat mit der Certificate ID: 67111.19 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-CA67111A2, e-Szignó NCP Certificates“, 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

Die anwendbare ETSI Zertifizierungspolitiken sind:

- LCP: Einfache Zertifizierungspolitik
- NCP: Standardisierte Zertifizierungspolitik
- NCP+: Erweiterte standardisierte Zertifizierungspolitik, die eine sichere Nutzereinheit fordert

Prüfgegenstand

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

e-Szignó NCP Certificates:

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 = Advanced Class 3 e-Szigno CA 2009	19
CN = Advanced Code Signing Class3 e-Szigno CA 2016	008C55D86652702EF11B33AE0A
CN = Advanced Pseudonymous e-Szigno CA 2009	1A
CN = Class3 KET e-Szigno CA 2018	00BDAC3D35984F42E5560E220A
CN = Advanced Class 2 e-Szigno CA 2009	18
CN = Advanced eIDAS Class2 e-Szigno CA 2016	008B288ADD98AF791B02207F0A
CN = Advanced Code Signing Class2 e-Szigno CA 2016	008D8DD221EED2535B843E1E0A

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 Class3 CA 2017	00A2A692BF8E596B5602EA8B0A
CN = e-Szigno Class3 CodeSigning CA 2017	00AB5B681564A5209318F6AB0A
CN = e-Szigno Pseudonymous CA 2017	00A8A6207E075CE78D923AF70A
CN = e-Szigno Class2 CA 2017	00A15A22E9DC035BEFE8FD990A
CN = e-Szigno Class2 CodeSigning CA 2017	00AA7DB8EE277DAAC2E3E5CB0A

Aussteller des CA-Zertifikats (Root CA oder Intermediate CA): CN = KGYHSZ (Public Administration Root CA - Hungary) Zertifikatsseriennummer: 437C92A4	
Name der CA (wie im Zertifikat)	**Seriennummer des Zertifikates**
CN = Signature Class 3 KET e-Szigno CA 2009	437C94A7

zusammen mit der Dokumentation des Betreibers:

- „e-Szignó Certification Authority eIDAS conform Non-Qualified Certificate for Electronic Signature Certificate Policies“, Version 2.11 vom 23.09.2019, gültig ab 25.09.2019, Microsec Ltd.
- „e-Szignó Certification Authority eIDAS conform Non-Qualified Certificate for Electronic Seal Certificate Policies“,

Version 2.11 vom 23.09.2019, gültig ab 25.09.2019, Microsec Ltd.

- „e-Szignó Certification Authority Non eIDAS covered Certificate Certificate Policies“, Version 2.11 vom 23.09.2019, gültig ab 25.09.2019, Microsec Ltd.
- „e-Szignó Certification Authority eIDAS conform Non-Qualified Certificate for Electronic Signature Certification Practice Statement“, Version 2.11 vom 23.09.2019, gültig ab 25.09.2019, Microsec Ltd.
- “e-Szignó Certification Authority eIDAS conform Non-Qualified Certificate for Electronic Seal Certification Practice Statement”, version 2.11 vom 23.09.2019, gültig ab 25.09.2019, Microsec Ltd.
- „e-Szignó Certification Authority Non eIDAS covered Certificates Certification Practice Statement“, Version 2.11 vom 23.09.2019, gültig ab 25.09.2019, Microsec Ltd.
- “e-Szignó Certification Authority eIDAS conform Non-Qualified Certificate for Electronic Signature Disclosure Statement”, Version 2.11 vom 23.09.2019, gültig ab 25.09.2019, Microsec Ltd.
- „e-Szignó Certification Authority eIDAS conform Non-Qualified Certificate for Electronic Seal 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