Certificate

The certification body of TÜV Informationstechnik GmbH
hereby awards this certificate to the company

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

to confirm that its trust service

e-Szignó NCP Certificates

fulfils all requirements defined in the standard (EN)

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

The appendix to the certificate is part of the certificate and consists of 5 pages.

The certificate is valid only in conjunction with the evaluation report.

ETSI EN 319 411-1 2019 TÜViT Trusted Site

Certificate ID: 67111.19

Certificate valid until 2021-02-07

Essen, 2019-05-16

Dr. Christoph Sutter
Head of Certification Body

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Langemarckstr. 20
45141 Essen, Germany
www.tuvit.de

DAkkS Deutsche Akkreditierungsstelle D-ZE-12022-01-01

Certification System

The certification body of TÜV Informationstechnik GmbH is accredited by "DAkkS Deutsche Akkreditierungsstelle GmbH" according to EN ISO/IEC 17065 for the scopes IT security and security technology product certification. The certification body performs its certification on the basis of the following accredited certification system:

- "Certification System (accredited scope) of the certification body of TÜV Informationstechnik GmbH", version 2.0 as of 2016-06-06, TÜV Informationstechnik GmbH

Evaluation Report

- "Evaluation Report – Change Audit – ETSI EN 319 411-1, TUVIT-CA67111, e-Szignó NCP Certificates", Version 1.1 as of 2019-05-06, TÜV Informationstechnik GmbH

Evaluation Requirements

The evaluation requirements are defined in the standard ETSI EN 319 411-1:

- 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

The applicable ETSI Certificate Policies are:

- LCP: Lightweight Certificate Policy
- NCP: Normalized Certificate Policy
- NCP+: Normalized Certificate Policy requiring a secure cryptographic device

Evaluation Target

The target of evaluation is characterized by the certificate information of the inspected trust service:

e-Szignó NCP Certificates:

Issuer of CA certificate (Root CA or intermediate CA): CN = Microsec e-Szigno Root CA 2009 Certificate Serial Number: 00 c2 7e 43 04 4e 47 3f 19	
Name of CA (as in certificate)	**serial number of certificate**
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

Issuer of CA certificate (Root CA or intermediate CA): CN = e-Szigno Root CA 2017 **Certificate Serial Number: 01 54 48 ef 21 fd 97 59 0d f5 04 0a**	
Name of CA (as in certificate)	**serial number of certificate**
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

Issuer of CA certificate (Root CA or intermediate CA): CN = KGYHSZ (Public Administration Root CA - Hungary) **Certificate Serial Number: 43 7c 92 a4**	
Name of CA (as in certificate)	**serial number of certificate**
CN = Signature Class 3 KET e-Szigno CA 2009	43 7c 94 a7

together with the documentation of the operator:

- "e-Szignó Certification Authority eIDAS conform Non-Qualified Certificate for Electronic Seal Certificate Policies", version 2.8, date of effect: 2018-12-14, Microsec Ltd.

- "e-Szignó Certification Authority Non eIDAS covered Certificate Certificate Policies", version 2.8, date of effect: 2018-12-14, Microsec Ltd.
- "e-Szignó Certification Authority eIDAS conform Non-Qualified Certificate for Electronic Signature Certificate Policies", version 2.8, date of effect: 2018-12-14, Microsec Ltd.
- "e-Szignó Certification Authority eIDAS conform Non-Qualified Certificate for Electronic Signature Certification Practice Statement", version 2.8, date of effect: 2018-12-14, Microsec Ltd.
- "e-Szignó Certification Authority eIDAS conform Non-Qualified Certificate for Electronic Seal Certification Practice Statement", version 2.8, date of effect: 2018-12-14, Microsec Ltd.
- "e-Szignó Certification Authority Non eIDAS covered Certificates Certification Practice Statement", version 2.8, date of effect: 2018-12-14, Microsec Ltd.
- "e-Szignó Certification Authority eIDAS conform Non-Qualified Certificate for Electronic Signature Disclosure Statement", version 2.8, date of effect: 2018-12-14, Microsec Ltd.
- "e-Szignó Certification Authority eIDAS conform Non-Qualified Certificate for Electronic Seal Disclosure Statement", version 2.8, date of effect: 2018-12-14, Microsec Ltd.
- "e-Szignó Certification Authority General Terms and Conditions", version 1.6, effective date: 2018-12-14, Microsec Ltd.

Evaluation Result

- The target of evaluation fulfills all applicable evaluation requirements.
- The certification requirements defined in the certification system are fulfilled.

Summary of the Evaluation Requirements

ETSI EN 319 411-1 contains requirements for Trust Service Providers practice under the following headlines:

1 Publication and repository responsibilities

2 Identification and authentication

3 Certificate Life-Cycle operational requirements

4 Facility, management, and operational controls

5 Technical security controls

6 Certificate, CRL, and OCSP profiles

7 Compliance audit and other assessment

8 Other business and legal matters

9 Other provisions

Scope of the Amendment

This amendment as of 2020-02-05 supplements the certificate with certificate ID: 67111.19 as of 2019-05-16 because of the conducted surveillance audit.

Certification System

The certification body of TÜV Informationstechnik GmbH is accredited by "DAkkS Deutsche Akkreditierungsstelle GmbH" according to EN ISO/IEC 17065 for the scopes IT security and security technology product certification. The certification body performs its certification on the basis of the following accredited certification system:

- "Certification System (accredited scope) of the certification body of TÜV Informationstechnik GmbH", version 2.0 as of 2016-06-06, TÜV Informationstechnik GmbH

Evaluation Report

- "Evaluation Report – Surveillance Audit – ETSI EN 319 411-1, TUVIT-CA67111A2, e-Szignó NCP Certificates", Version 2.0 as of 2020-02-03, TÜV Informationstechnik GmbH

Evaluation Requirements

The evaluation requirements are defined in the standard ETSI EN 319 411-1 V1.2.2:

- 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

The applicable ETSI Certificate Policies are:

- LCP: Lightweight Certificate Policy
- NCP: Normalized Certificate Policy
- NCP+: Extended Normalized Certificate Policy requiring a secure cryptographic device

Evaluation Target

The target of evaluation is characterized by the certificate information of the inspected trust service:

e-Szignó NCP Certificates:

Issuer of CA certificate (Root CA or Intermediate CA): CN = Microsec e-Szigno Root CA 2009 Certificate Serial Number: 00C27E43044E473F19	
Name of CA (as in certificate)	**Serial number of certificate**
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

Issuer of CA certificate (Root CA or Intermediate CA): CN = e-Szigno Root CA 2017 Certificate Serial Number: 015448EF21FD97590DF5040A	
Name of CA (as in certificate)	**Serial number of certificate**
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

Issuer of CA certificate (Root CA or Intermediate CA): CN = KGYHSZ (Public Administration Root CA - Hungary) Certificate Serial Number: 437C92A4	
Name of CA (as in certificate)	**Serial number of certificate**
CN = Signature Class 3 KET e-Szigno CA 2009	437C94A7

together with the documentation of the operator:

- "e-Szignó Certification Authority eIDAS conform Non-Qualified Certificate for Electronic Signature Certificate Policies", version 2.11 as of 2019-09-23, valid from 2019-09-25, Microsec Ltd.
- "e-Szignó Certification Authority eIDAS conform Non-Qualified Certificate for Electronic Seal Certificate Policies", version 2.11 as of 2019-09-23, valid from 2019-09-25, Microsec Ltd.

- "e-Szignó Certification Authority Non eIDAS covered Certificate Certificate Policies", version 2.11 as of 2019-09-23, valid from 2019-09-25, Microsec Ltd.
- "e-Szignó Certification Authority eIDAS conform Non-Qualified Certificate for Electronic Signature Certification Practice Statement", version 2.11 as of 2019-09-23, valid from 2019-05-25, Microsec Ltd.
- "e-Szignó Certification Authority eIDAS conform Non-Qualified Certificate for Electronic Seal Certification Practice Statement", version 2.11 as of 2019-09-23, valid from 2019-9-25, Microsec Ltd.
- "e-Szignó Certification Authority Non eIDAS covered Certificates Certification Practice Statement", version 2.11 as of 2019-09-23, valid from 2019-09-25, Microsec Ltd.
- "e-Szignó Certification Authority eIDAS conform Non-Qualified Certificate for Electronic Signature Disclosure Statement", version 2.11 as of 2019-09-23, valid from 2019-09-25, Microsec Ltd.
- "e-Szignó Certification Authority eIDAS conform Non-Qualified Certificate for Electronic Seal Disclosure Statement", version 2.11 as of 2019-09-23, valid from 2019-09-25, Microsec Ltd.
- "e-Szignó Certification Authority General Terms and Conditions", version 1.7 as of 2019-09-23, valid from 2019-09-25, Microsec Ltd.

Evaluation Result

- The target of evaluation fulfills all applicable evaluation requirements.
- The certification requirements defined in the certification system are fulfilled.

Summary of the Evaluation Requirements

ETSI EN 319 411-1 contains requirements for Trust Service Providers practice under the following headlines:

1 Publication and repository responsibilities

2 Identification and authentication

3 Certificate Life-Cycle operational requirements

4 Facility, management, and operational controls

5 Technical security controls

6 Certificate, CRL, and OCSP profiles

7 Compliance audit and other assessment

8 Other business and legal matters

9 Other provisions