

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 Website Authentication

fulfils all requirements defined in the standard (EN)

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

The appendix to the certificate is part of the certificate and consists of 4 pages.

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



Certificate ID: 67112.19
© TÜVIT - TÜV NORD GROUP - www.tuvit.de

Certificate valid until
2021-02-07

21

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



Certificate

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-CA67112, e-Szignó Website Authentication”, 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 V1.2.2 (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

Additionally the following criteria were considered in the audit:

- “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates”, version 1.6.3 as of 2019-02-01, CA/Browser Forum

The applicable ETSI Certificate Policies are:

- DVCP: Domain Validation Certificate Policy
- OVCP: Organizational Validation Certificate Policy
- IVCP: Individual Validation Certificate Policy

Evaluation Target

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

e-Szignó Website Authentication:

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 = 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

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 Online SSL CA 2017	00 a7 99 e9 a1 b9 f1 90 5b 9b 8c e6 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 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

together with the documentation of the operator:

- “e-Szignó Certification Authority eIDAS conform Certificate for Website Authentication Certificate Policies”, version 2.8, date of effect: 2018-12-14, Microsec Ltd.
- “e-Szignó Certification Authority eIDAS conform Certificate for Website Authentication Certification Practice Statement”, version 2.8, date of effect: 2018-12-14, Microsec Ltd.
- “e-Szignó Certification Authority eIDAS conform Certificate for Website Authentication 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**