Certificate

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

Microsec Ltd.
Záhony utca 7.
H-1031 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 V1.1.1 (2016-02), policy OVCP.

The appendix to the certificate is part of the certificate and consists of 3 pages.

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

ETSI EN 319 411-1 2017 TÜViT® Trusted Site

Certificate ID: 6794.17

Certificate valid until 2018-02-28

Essen, 2017-02-03

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-12022-01-00

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 – Initial Certification – ETSI EN 319 411-1, TUVIT-CA6794, e-Szignó Website Authentication", Version 2.0 as of 2017-01-31, 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 Policy is:

- OVCP: Organizational 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 = 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
CN = Online e-Szigno SSL CA 2016	00 8f 81 6e d5 51 c9 92 4e d7 8f b1 0a

together with the Certificate Policy (CP) of the operator:

- "e-Szignó Certification Authority eIDAS conform Non-Qualified Certificate for Website Authentication Certificate Policies", version 2.2 as of 2016-10-30, Microsec Ltd.

and with the Certification Practice Statement (CPS) of the operator:

- "e-Szignó Certification Authority eIDAS conform Certificate for Website Authentication Certification Practice Statement", version 2.2 as of 2016-10-30, 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**