

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:

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

<b>Issuer of CA certificate (Root CA or intermediate CA):</b> <b>CN = e-Szigno Root CA 2017</b> <b>Certificate Serial Number: 01 54 48 ef 21 fd 97 59 0d f5 04 0a</b>	
<b>Name of CA (as in certificate)</b>	<b>serial number of certificate</b>
CN = e-Szigno Online SSL CA 2017	00 a7 99 e9 a1 b9 f1 90 5b 9b 8c e6 0a

<b>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</b>	
<b>Name of CA (as in certificate)</b>	<b>serial number of certificate</b>
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**

## Scope of the Amendment

This amendment as of 2020-02-05 supplements the certificate with certificate ID: 67112.19 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-CA67112A2, e-Szignó Website Authentication”, 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

Additionally the following criteria were considered in the audit:

- “Baseline Requirements for the issuance and management of Publicly-Trusted Certificates”, Version 1.6.6 as of 2019-09-09, 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:

<b>Issuer of CA-certificates (Root CA or intermediate CA):                      CN = Microsec e-Szigno Root CA 2009                      Certificate serial number: 00C27E43044E473F19</b>	
<b>Name of CA (as in certificate)</b>	<b>serial number of certificate</b>
CN = Online e-Szigno SSL CA 2016	008F816ED551C992 4ED78FB10A
CN = e-Szigno SSL CA 2014	535CD2A3AC13D9 DC4A4B830A
CN = Class2 e-Szigno SSL CA 2016	008E5F46EF1EC4E1 0FCA08160A

<b>Issuer of CA certificates (Root CA or intermediate CA):</b> <b>CN = e-Szigno Root CA 2017</b> <b>Certificate serial number:</b> <b>015448EF21FD97590DF5040A</b>	
<b>Name of CA (as in certificate)</b>	<b>serial number of certificate</b>
CN = e-Szigno Online SSL CA 2017	00A799E9A1B9F190 5B9B8CE60A
CN = e-Szigno Class3 SSL CA 2017	00A3F1C99D52569 D8D992E4C0A
CN = e-Szigno Class2 SSL CA 2017	00A6E94D04B3BCA 2DC1AD69D0A

together with the documentation of the operator:

- “e-Szignó Certification Authority eIDAS conform Certificate for Website Authentication Certificate Policies”, version 2.11 as of 2019-09-23, valid from 2019-09-25, Microsec Ltd.
- “e-Szignó Certification Authority eIDAS conform Certificate for Website Authentication Certification Practice Statement”, version 2.11 as of 2019-09-23, valid from 2019-09-25, Microsec Ltd.
- “e-Szignó Certification Authority eIDAS conform Certificate for Website Authentication 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**