

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 Qualified Website  
Authentication**

fulfils all requirements defined in the standard (EN)

**ETSI EN 319 411-1 V1.1.1 (2016-02),  
policy EVCP.**

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.



Certificate ID: 67113.19  
© TÜVIT - TÜV NORD GROUP - www.tuvt.de

21  
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.tuvt.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-CA67113, e-Szignó Qualified 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 V1.1.1 (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

Additionally the following criteria were considered in the audit:

- “Guidelines for the issuance and management of Extended Validation Certificates”, version 1.6.8 as of 2018-03-09, CA/Browser Forum

The applicable ETSI Certificate Policy is:

- EVCP: Extended Validation Certificate Policy

### Evaluation Target

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

#### e-Szignó Qualified 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 = Qualified e-Szigno TLS CA 2018	00 b8 6e df 27 d8 f6 96 7c 64 70 63 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 Qualified TLS CA 2018	00 b7 f3 3e b7 78 eb 63 1c be 7c 80 0a

together with the documentation of the operator:

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

- “e-Szignó Certification Authority eIDAS conform Qualified 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**