HUNGUARD Kft. • 1123 Budapest, Kékgolyó u. 6.
TEL: +36 1 792 0880 • FAX: +36 1 445 0414 WWW.HUNGUARD.HU

**Audit attestation for Microsec Micro Software Engineering & Consulting Private Limited Company by Shares as a Qualified Trusted Service Provider**

Reference: HUNG-AA-002-2020

Budapest, 04 January, 2021

To whom it may concern,

This is to confirm that „HUNGUARD Kft." has successfully audited the CAs of Microsec Micro Software Engineering & Consulting Private Limited Company by Shares without critical findings. This present Audit Attestation Letter is registered under the unique identifier number "HUNG-AA-002-2020" and consist of 9 pages. Kindly find here-below the details accordingly.

In case of any question, please contact:

HUNGUARD Kft., 6 Kékgolyó Street, 1123 Budapest, Hungary

Tel: +36 1 792 0880; Fax: +36 1 445 0414

e-mail: iroda@hunguard.hu

With best regards:

Zsolt Attila Endrődi
reviewer

Digitálisan aláírta: HUNGUARD

Tibor Németvári
lead auditor

| | |
|---|---|
| Identification of the conformity assessment body (CAB): | HUNGUARD Informatics and IT R&D and General Service Provider Ltd. (6 Kékgolyó str. Budapest 1123 Hungary) as a certification authority. Accredited by the accreditation document No. NAH-6-0048/2018[1] of National Accreditation Authority according to "MSZ EN ISO/IEC 17065:2013" and "ETSI EN 319 403 V2.2.2 (2015-08) |
| Identification of the trust service provider (TSP): | MICROSEC Micro Software Engineering & Consulting Private Limited Company by Shares, Ángel Sanz Briz út 13, 1033 Budapest, Hungary<br>registered under 01-10-047218 |
| Identification of the audited Root-CA: | Microsec e-Szigno Root CA 2009 |
| Distinguished Name | /C=HU/L=Budapest/O=Microsec Ltd./CN=Microsec e-Szigno Root CA 2009 |
| SHA-256 fingerprint | 3C5F81FEA5FAB82C64BFA2EAECAFCDE8E077FC8620A7CAE537163DF36EDBF378 |
| Certificate Serial number | C27E43044E473F19 |
| Applied policy | LCP, NCP, NCP+, OVCP, DVCP, IVCP and EVCP of ETSI EN 319 411-1<br>QCP-l, QCP-l-qscd, QCP-n, QCP-n-qscd and QCP-w of ETSI EN 319 411-2<br>BTSP of ETSI EN 319 421 |
| Validity | Jun 16, 2009 until Dec 30, 2029 |
| Identification of the audited Root-CA: | Microsec e-Szigno Root CA 2009[2] |
| Distinguished Name | /C=HU/L=Budapest/O=Microsec Ltd./CN=Microsec e-Szigno Root CA 2009 |
| SHA-256 fingerprint | 72F9AF2158181BAF16D60C9B4E6F4BD7CA8D2341AD48AFDB67CB4C8332D546F6 |
| Certificate Serial number | E8849639AB66105A |
| Applied policy | LCP, NCP, NCP+, OVCP, DVCP, IVCP and EVCP of ETSI EN 319 411-1<br>QCP-l, QCP-l-qscd, QCP-n, QCP-n-qscd and QCP-w of ETSI EN 319 411-2<br>BTSP of ETSI EN 319 421 |
| Validity | Mar 6, 2009 until Jan 18, 2038 |
| Identification of the audited Root-CA: | Microsec e-Szigno Root CA 2009[3] |
| Distinguished Name | /C=HU/L=Budapest/O=Microsec Ltd./CN=Microsec e-Szigno Root CA 2009 |

[1] https://nah.gov.hu/uploads/attachment/file/8509/RO_2_-200116-6-0048-2018-F1-MP-10398221-alairt2.pdf
[2] Not used
[3] Not used

| | |
|---|---|
| SHA-256 fingerprint | 8E8C6EBF77DC73DB3E38E93F4803E62B6B5933BEB51EE4152F68D7AA14426B31 |
| Certificate Serial number | C27E43044E473F18 |
| Applied policy | LCP, NCP, NCP+, OVCP, DVCP, IVCP<br>and EVCP of ETSI EN 319 411-1<br>QCP-l, QCP-l-qscd, QCP-n, QCP-n-qscd<br>and QCP-w of ETSI EN 319 411-2<br>BTSP of ETSI EN 319 421 |
| Validity | Jun 16, 2009 until Dec 30, 2029 |

The Sub-CAs that have been issued by Root-CA and that have been covered by this audit are listed in table 1 below.

The audit was performed as full period of time audit at the TSP's locations in Budapest, Hungary. It took place from 2020-09-08 until 2020-09-14 and covered the period from 2019-09-15 until 2020-09-14.

The audit was performed according to the European Standards "ETSI EN 319 411-2, V2.2.2 (2018-04)", "ETSI EN 319 411-1, V1.2.2 (2018-04)", and "ETSI EN 319 401, V2.2.1 (2018-04)" considering the requirements of the "ETSI EN 319 403, V2.2.2 (2015-08)" for the Trust Service Provider Conformity Assessment.

The audit was based on the following policy and practice statement documents of the TSP:

1. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Signature Certificate Policies, version: 2.17 as of 2020-10-21, Date of effect: 2020-10-28
2. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Signature Certification Practice Statement, version: 2.17 as of 2020-10-21, Date of effect: 2020-10-28
3. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Signature Disclosure Statement, version: 2.17 as of 2020-10-21, Date of effect: 2020-10-28
4. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Signature, Certificate Policies, version: 2.17 as of 2020-10-21, Date of effect: 2020-10-28
5. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Signature Certification Practice Statement, version: 2.17 as of 2020-10-21, Date of effect: 2020-10-28
6. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Signature Disclosure Statement, version: 2.17 as of 2020-10-21, Date of effect: 2020-10-28
7. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Seal Certificate Policies, version: 2.17 as of 2020-10-21, Date of effect: 2020-10-28
8. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Seal Certification Practice Statement, version: 2.17 as of 2020-10-21, Date of effect: 2020-10-28
9. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Seal Disclosure Statement, version: 2.17 as of 2020-10-21, Date of effect: 2020-10-28
10. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Seal Certificate Policies, version: 2.17 as of 2020-10-21, Date of effect: 2020-10-28
11. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Seal Certification Practice Statement, version: 2.17 as of 2020-10-21, Date of effect: 2020-10-28

12. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Seal Disclosure Statement, version: 2.17 as of 2020-10-21, Date of effect: 2020-10-28
13. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Certificate Policies, version: 2.17 as of 2020-10-21, Date of effect: 2020-10-28
14. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Certification Practice Statement, version: 2.17 as of 2020-10-21, Date of effect: 2020-10-28
15. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Disclosure Statement, version: 2.17 as of 2020-10-21, Date of effect: 2020-10-28
16. e-Szignó Certification Authority, eIDAS conform Qualified Certificates for Website Authentication Certificate Policy, version: 2.17 as of 2020-10-21, Date of effect: 2020-10-28
17. e-Szignó Certification Authority ,eIDAS conform Qualified Certificate for Website Authentication Certification Practice Statement, version: 2.17 as of 2020-10-21, Date of effect: 2020-10-28
18. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Website Authentication Disclosure Statement, version: 2.17 as of 2020-10-21, Date of effect: 2020-10-28
19. e-Szignó Certification Authority, Non eIDAS covered Certificate, Certificate Policies, version: 2.17 as of 2020-10-21, Date of effect: 2020-10-28
20. e-Szignó Certification Authority, Non eIDAS covered Certificates Certification Practice Statement, version: 2.17 as of 2020-10-21, Date of effect: 2020-10-28

In the following areas, non-conformities have been identified throughout the audit:

**Findings with regard to ETSI EN 319 401**

**319 401- REQ-6.2-02**

The TSP shall give every information to the customer (subject) about the services and its security. It was found, when a subject demand a PUK code, it will be uploaded to a website, called Ügyféltér. Based on the terms and conditions and public policies, it is not obviously clear, which are the values to be protected.

**319 401 - REQ-7.4-09**

The TSP shall audit all user activities, especially privileged use. It was found, when two privileged users log in to the database server with SSH command, the TSP system do not have audit trails to identify who logged in the systems.

**319 401 - REQ-7.7-01**

The TSP shall ensure the use of only trustworthy systems, which are not obsolete, have up to date patches. On the audit, some obsolete system were found.

The TSP shall use system, which is fully under control. Some client device was out of the TSP central management.

**319 401 - REQ-7.7-03**

The TSP shall have a well documented change control procedure. It was found, different systems had different change process.

**319 401 - REQ-7.8-1**

The TSP shall control remote access to its trusted systems. The TSP allowed any, without central security managed workstations (e.g. laptop) to connect trusted systems via VPN connection.

**319 401 - REQ-7.9-01**

The TSP should monitor incidents and categorize them appropriately. It was found that there were two incident where proper categorization has not taken place, and therefore the notification to the authority was not substantiated.

**Findings with regard to ETSI EN 319 411-1,-2**

**319 411-1 - OVR-5.2-03**

The TSP's CPS shall include the complete CA hierarchy, including root and subordinate CA's. It was found, in the public policies, only two were mentioned, but in practice, there were three RootCA.

**319 411-1 - REG-6.2.2-01**

The TSP shall verify the identity of the subscriber and subject, and shall check that certificate requests are accurate. In the case of 2nd class authentication certificates, it was not clear, what kind of evidence shall the subject represent to the TSP.

**319 411-1 REV-6.2.4-01 – non-eidas**

The TSP shall document as part of its CPS the procedures for revocation of end user and CA certificates. The TSP has a policy when a code signing certificate is revoked second time due to key compromise, the TSP refuse to issue a certificate for the third time. But this policy was not part of a public policy, so the subject were not aware of that.

**319 411-1 - OVR-6.3.4-01**

The TSP shall clearly define the acceptance of the certificate. In certificate acceptance there was a difference between the practice and the policy. In the policy, the customer (the subject) had to sign physically an acceptance paper, but in the practice there was no need to do it.

**319 411-1 - REG-6.3.4-11**

The TSP shall include in the contract and the annex (concerning the subject) the reference to the authentication policy in the issued certificate.

**319 411-1 - SDP-6.3.12-07 – non-eidas**

The TSP shall regulate the key escrow process. It was found that the public policy does not include the key escrow process.

For all non-conformities, the remediation has been successfully checked by provided evidences, which can be read in the audit report.

This Audit Attestation has not recorded any incident.

| Identification of the Sub-CA | Distinguished Name | SHA-256 fingerprint | Certificate Serial number | Applied policy | Validity |
|---|---|---|---|---|---|
| Advanced Class 2 e-Szigno CA 2009 | /C=HU/L=Budapest/O=Microsec Ltd./CN=Advanced Class 2 e-Szigno CA 2009 | C63543729A370C26952B47E1D1D1AEA84CB1B07F1B0F964C2FEDDC523FD7C795 | 18 | LCP | Dec 02, 2009 until Dec 29, 2029 |
| Advanced Class 3 e-Szigno CA 2009 | /C=HU/L=Budapest/O=Microsec Ltd./CN=Advanced Class 3 e-Szigno CA 2009 | B0A6EF0350E7C4C6056BEEA7AF9D2D860B9ED102137B9729D3C23216D195546A | 19 | NCP, NCP+, | Dec 02, 2009 until Dec 29, 2029 |
| Advanced Code Signing Class2 e-Szigno CA 2016 | /C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497-2-41/CN=Advanced Code Signing Class2 e-Szigno CA 2016 | A98C8CED93F9A43631ABE4573864E06C5192900723E97D1EED2C0D7C68B2D079 | 8D8DD221EED2535B843E1E0A | LCP | Aug 29, 2016 until Dec 29, 2029 |
| Advanced Code Signing Class3 e-Szigno CA 2016 | /C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497-2-41/CN=Advanced Code Signing Class3 e-Szigno CA 2016 | 283CA6939530C1B5503915051936378AE36871967B03E4C2E7C243F14967DEB1 | 8C55D86652702EF11B33AE0A | NCP, NCP+ | Jun 22, 2016 until Dec 29, 2029 |
| Advanced eIDAS Class2 e-Szigno CA 2016 | /C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497-2-41/CN=Advanced eIDAS Class2 e-Szigno CA 2016 | A29C104B100C3A7933473E62E4BE6371D653A1604D04EDAAD02C95806065CEE3 | 8B288ADD98AF791B02207F0A | LCP | Jun 22, 2016 until Dec 29, 2029 |
| Advanced Pseudonymous e-Szigno CA 2009 | /C=HU/L=Budapest/O=Microsec Ltd./CN=Advanced Pseudonymous e-Szigno CA 2009 | D0E39AA7D2FA53581008A15D825C57D25BD49247834431F8A227A29C280A1C0C | 1A | LCP, NCP, NCP+ | Dec 02, 2009 until Dec 29, 2029 |
| Class2 e-Szigno SSL CA 2016 | /C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497-2-41/CN=Class2 e-Szigno SSL CA 2016 | 3912C585E727F2B077888F678F043FD8DDCEE9E91E6628A6245B1B8EBBCC3912 | 8E5F46EF1EC4E10FCA08160A | OVCP, DVCP, IVCP | Aug 29, 2016 until Dec 29, 2029 |
| e-Szigno SSL CA 2014 | /C=HU/L=Budapest/O=Microsec Ltd./CN=e-Szigno SSL CA 2014 | EAC241C0440A36830111383336BC20CAC7409C20F6E88D4F84F4827BE919E338 | 535CD2A3AC13D9DC4A4B830A | OVCP, DVCP, IVCP | Jul 08, 2014 until Dec 29, 2029 |
| Online e-Szigno SSL CA 2016 | /C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497-2-41/CN=Online e-Szigno SSL CA 2016 | 31DAA25D142D08B90E640D4BC50B249F0FE39785C98D5E53E233259C0FAE9398 | 8F816ED551C9924ED78FB10A | OVCP, DVCP, IVCP | Aug 29, 2016 until Dec 29, 2029 |

| | | | | | |
|---|---|---|---|---|---|
| Qualified e-Szigno CA 2009 | /C=HU/L=Budapest/O=Microsec Ltd./CN=Qualified e-Szigno CA 2009 | B884ED6527433687627D35157E904690D2DFF6A5DCD3CE267BBAF159C06F5054 | 16 | QCP-n-qscd | Dec 02, 2009 until Dec 29, 2029 |
| Qualified e-Szigno Organization CA 2016 | /C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497-2-41/CN=Qualified e-Szigno Organization CA 2016 | 60AF9E5F39D873B236BE142BC706DA571849AED7FAE635FC5A1461A0CF7459C5 | 90274984CBF0D2D9AFAFF30A | QCP-l-qscd | Aug 29, 2016 until Dec 29, 2029 |
| Qualified e-Szigno QCP CA 2012 | /C=HU/L=Budapest/O=Microsec Ltd./CN=Qualified e-Szigno QCP CA 2012 | CFCB60C1F0180C68E3EA5D24B4A05E9D9900D87C3D83D503CE1690B3C1656458 | 2EEBA3B3AF911A4B31BDB10A | QCP-l-NCP+, QCP-n-NCP+, QCP-l, QCP-n | Mar 30, 2012 until Dec 29, 2029 |
| Qualified e-Szigno TLS CA 2018 | /C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=Qualified e-Szigno TLS CA 2018 | F7C7E28FB5E79F314AAAC6BBBA932F15E1A72069F435D4C9E707F93CA1482EE3 | B86EDF27D8F6967C6470630A | EVCP, QCP-w | Jul 31, 2018 until Dec 29, 2029 |
| Qualified Pseudonymous e-Szigno CA 2009 | /C=HU/L=Budapest/O=Microsec Ltd./CN=Qualified Pseudonymous e-Szigno CA 2009 | F8684D2812BA98A52FE94528C4CB152378A2D73A828810A8C7B8529875C64674 | 17 | QCP-n | Dec 02, 2009 until Dec 29, 2029 |
| e-Szigno TSA CA 2020 | /C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno TSA CA 2020 | 7731FE893FD5461AD2BFAFBADC530CF69B6DA5095E3AEE0FF82EF54ADD4B8B57 | D2F05E9A83DB987AA5755E0A | BTSP | Aug 25, 2020 until Sep 29, 2029 |
| Class3 KET e-Szigno CA 2018 | /C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=Class3 KET e-Szigno CA 2018 | 7BCF1C8A12EE0B2854A1B41070652B0325E7D0C20B9C44D4ACE9C643387F1431 | BDAC3D35984F42E5560E220A | NCP, NCP+ | Sep 06, 2018 until Dec 29, 2029 |
| Qualified KET e-Szigno CA 2018 | /C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=Qualified KET e-Szigno CA 2018 | D9E445B22C6FCB37B296FCD1331486569651A8DB98071753FEFC73D2C97BF732 | BC3D9A56D441A2BB5987620A | QCP-l-qscd, QCP-l, QCP-n-qscd, QCP-n | Sep 06, 2018 until Dec 29, 2029 |

Table 1 Sub-CAs that have been issued by Root-CA

**Modifications record**

| Version | Issuing Date | Changes |
|---|---|---|
| Version 1.0 | 30 October, 2020 | Initial attestation |
| Version 1.1 | 04 January, 2021 | Correction in order to support CCADB upload |

**End of the audit attestation letter.**