

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

Reference: HUNG-AA-003-2021

Budapest, 18 October, 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-003-2021” and consist of 6 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

Tibor Némethvári
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-6-0048/2018¹ 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 registered under 01-10-047218

Identification of the audited Root-CA: e-Szigno Root CA 2017

Distinguished Name	/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/ CN=e-Szigno Root CA 2017
SHA-256 fingerprint	BEB00B30839B9BC32C32E4447905950641F26421B15ED089198B518AE 2EA1B99
Certificate Serial number	015448EF21FD97590DF5040A
Applied policy	LCP, NCP, NCP+, OVCP, DVCP, IVCP and EVCP of ETSI EN 319 411-1 QCP-l, QCP-l-qscd, QCP-n, QCP-n-qscd and QCP-w of ETSI EN 319 411-2 BTSP of ETSI EN 319 421
Validity	Aug 22, 2017 until Aug 22, 2042

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 2021-09-07 until 2021-09-10 and covered the period from 2020-09-14 until 2021-09-10. Lead Auditor was Tibor Némethvári (CISA).

The trust service provider has two facility. One main facility (Facility 1 in Budapest: Ángel Sanz Briz út 13, 1033 Budapest, Hungary. Note that this data centre of the organisation, although located in the same place, has a different postal address: Záhony utca 7, 1031 Budapest, Hungary), where the whole service is provided (registration office, IT infrastructure, HSM) and one back up facility in a datacentre (Facility 2 in Budapest: T-Systems Cloud & Data Center – Asztalos Sándor út 13, 1087 Budapest, Hungary) where all the back up infrastructure is being operated. This year audit, only Facility 1 was inspected physically, Facility 2 was inspected by interview. In the case of Facility 2, there were no changes in security solutions.

The audit was performed according to the European Standards “ETSI EN 319 411-2, V2.3.1 (2021-05)”, “ETSI EN 319 411-1, V1.3.1 (2021-05)”, and “ETSI EN 319 401, V2.3.1 (2021-05)” considering the

¹ https://nah.gov.hu/uploads/attachment/file/8509/RO_2_-200116-6-0048-2018-F1-MP-10398221-alairt2.pdf

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: 2.22 as of 2021-05-31, Date of effect: 2021-06-30
2. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Signature Certification Practice Statement, version: 2.22 as of 2021-05-31, Date of effect: 2021-06-30
3. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Signature Disclosure Statement, version: 2.22 as of 2021-05-31, Date of effect: 2021-06-30
4. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Signature, Certificate Policies, version: 2.23 as of 2021-07-01, Date of effect: 2021-07-31
5. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Signature Certification Practice Statement, version: 2.23 as of 2021-07-01, Date of effect: 2021-07-31
6. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Signature Disclosure Statement, version: 2.23 as of 2021-07-01, Date of effect: 2021-07-31
7. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Seal Certificate Policies, version: 2.22 as of 2021-05-31, Date of effect: 2021-06-30
8. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Seal Certification Practice Statement, version: 2.22 as of 2021-05-31, Date of effect: 2021-06-30
9. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Seal Disclosure Statement, version: 2.22 as of 2021-05-31, Date of effect: 2021-06-30
10. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Seal Certificate Policies, version: 2.23 as of 2021-07-01, Date of effect: 2021-07-31
11. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Seal Certification Practice Statement, version: 2.23 as of 2021-07-01, Date of effect: 2021-07-31
12. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Seal Disclosure Statement, version: 2.23 as of 2021-07-01, Date of effect: 2021-07-31
13. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Certificate Policies, version: 2.22 as of 2021-05-31, Date of effect: 2021-06-30
14. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Certification Practice Statement, version: 2.22 as of 2021-05-31, Date of effect: 2021-06-30
15. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Disclosure Statement, version: 2.22 as of 2021-05-31, Date of effect: 2021-06-30
16. e-Szignó Certification Authority, eIDAS conform Qualified Certificates for Website Authentication Certificate Policy, version: 2.22 as of 2021-05-31, Date of effect: 2021-06-30
17. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Website Authentication Certification Practice Statement, version: 2.22 as of 2021-05-31, Date of effect: 2021-06-30
18. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Website Authentication Disclosure Statement, version: 2.22 as of 2021-05-31, Date of effect: 2021-06-30
19. e-Szignó Certification Authority, Non eIDAS covered Certificate, Certificate Policies, version: 2.22 as of 2021-05-31, Date of effect: 2021-06-30
20. e-Szignó Certification Authority, Non eIDAS covered Certificates Certification Practice Statement, version: 2.22 as of 2021-05-31, Date of effect: 2021-06-30

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

Findings with regard to ETSI EN 319 401

319 401- REQ-7.7-02

It was discovered that the hardening settings for the virtual switch were not applied correctly, with several functions operating on factory settings.

319 401 - REQ-7.7-09

It was discovered that the servers responsible for virtualisation were not up to date. It was also found that the firmware version of the firewall used was not the latest version.

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

Two incidents were reviewed by the audit team which was reported to Mozilla:

1. 2020-11-10 Microsec e-Szigno: Certificate validity period greater than 398 days:
Bug number: 1676352
Bug address: https://bugzilla.mozilla.org/show_bug.cgi?id=1676352
2. 2021-08-31 Microsec: Misissuance of one OV certificate with Key Usage KeyEncipherment
Bug number: 1728384
Bug address: https://bugzilla.mozilla.org/show_bug.cgi?id=1728384

Identification of the Sub-CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number	Applied policy	Validity
e-Szigno Class2 CA 2017	/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno Class2 CA 2017	42DC827F46FB5E85DFFAE47D3C690F501 ECE25D575D597A50D8F878FA42AFCEA	A15A22E9DC03 5BEFE8FD990A	LCP	Sep 17, 2017 until Aug 22, 2042
e-Szigno Class2 CodeSigning CA 2020	/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno Class2 CodeSigning CA 2020	BA52633D91DFD48EE5B135B2543E8DD35 57F2DB33C0534E41A2268097C3008CA	D370F0C588F7 E4FE859A850A	LCP	Aug 25, 2020 until Aug 22, 2042
e-Szigno Class2 SSL CA 2017	/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno Class2 SSL CA 2017	2A0E3F2A77A80DCBE5CD52D50D65076EB D37FAD531DB10D6A1385A557F7B725D	A6E94D04B3BC A2DC1AD69D0A	OVCP, DVCP, IVCP	Sep 17, 2017 until Aug 22, 2042
e-Szigno Class3 CA 2017	/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno Class3 CA 2017	4F83842F1F04AB1E04D4D8E751666FCA8 2E5191CAFCD24062BFD1FE77C02CA4B4	A2A692BF8E59 6B5602EA8B0A	NCP, NCP+	Sep 17, 2017 until Aug 22, 2042
e-Szigno Class3 CodeSigning CA 2020	/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno Class3 CodeSigning CA 2020	711CBB0479DDC596745815E797423305F 95EDD792C5BC5854CED5A7FAFB4AA8D	D44A4BC0FBA0 A1BF0258AB0A	NCP	Aug 25, 2020 until Aug 22, 2042
e-Szigno Class3 SSL CA 2017	/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno Class3 SSL CA 2017	BCBC18C463B61F3A033B10C74974ED8A2 C328AFCD67A338D9871506A3515419F	A3F1C99D5256 9D8D992E4C0A	OVCP, DVCP, IVCP	Sep 17, 2017 until Aug 22, 2042
e-Szigno Online SSL CA 2017	/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno Online SSL CA 2017	974B82076154CEFF56ED4DB562186F739 4A02FF387AA205D6367A8B08FF7FAA0	A799E9A1B9F1 905B9B8CE60A	OVCP, DVCP, IVCP	Sep 17, 2017 until Aug 22, 2042
e-Szigno Pseudonymous CA 2017	/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno Pseudonymous CA 2017	6A6F2FA13B2D9DBBB409802002D337067 2760A2178D9B8D5694D660474231FA4	A8A6207E075C E78D923AF70A	LCP, NCP, NCP+	Sep 17, 2017 until Aug 22, 2042
e-Szigno Qualified CA 2017	/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno Qualified CA 2017	5ABE5818F6D02F05106C6C355540E1BE2 17C2354B535CF2507BF8515E1A6044A	9C68095849E0 8BEAB447EF0A	QCP-n-qscd	Sep 17, 2017 until Aug 22, 2042
e-Szigno Qualified Organization CA 2017	/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno Qualified Organization CA 2017	12EA26F6EEEFEC76AB8592545403AB885 15B00E275D9888713407A86FC5C7FD7	9D6D3EFF75E6 0FFF2CA1060A	QCP-l-qscd	Sep 17, 2017 until Aug 22, 2042

e-Szigno Qualified Pseudonymous CA 2017	/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno Qualified Pseudonymous CA 2017	1648CE4AB1BB65C485CB2236C768FABB865147D426915B92AFBCA81E9B2EE3BC	9F1D566220B1E414FB913D0A	QCP-n	Sep 17, 2017 until Aug 22, 2042
e-Szigno Qualified QCP CA 2017	/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno Qualified QCP CA 2017	6081BEE5B0DF191AC4E265AC0F6F7899F078B8C89F06055AE166AF91DF70D6E0	9E2C5EB959FD774CDD866A0A	QCP-I-NCP+, QCP-n-NCP+, QPC-I, QCP-n	Sep 17, 2017 until Aug 22, 2042
e-Szigno Qualified TLS CA 2018	/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno Qualified TLS CA 2018	7DF800075F5203C017364E81195A9AC9FF00C507D64A70F737D8D3E8CB3F0845	B7F33EB778EB631CBE7C800A	QCP-w	Jul 31, 2018 until Aug 22, 2042
e-Szigno TSA CA 2017	/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno TSA CA 2017	9E94BB8ADAD7A6CE4DCB1208F1239DC1E43483F1B7E81F74A90A20FB5E5C49B7	A98958CFD801AF006F1E690A	BTSP	Sep 17, 2017 until Aug 22, 2042
e-Szigno TSA CA 2020	/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno TSA CA 2020	B4C177E357565C99E90ED886D799F8C6BEFF806DA5A048551878489B9C27E488	D11C60534E95C90EA5B9600A	BTSP	Aug 25, 2020 until Aug 22, 2042

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

End of the audit attestation letter.