TLS BR Audit Attestation for

Microsec Micro Software Engineering & Consulting

Private Limited Company by Shares

as a Qualified Trusted Service Provider

Reference: HUNG-AA-007-TLS-BR-2023

"Budapest, 19 February, 2024"

To whom it may concern,

This is to confirm that "HUNGUARD Kft." has audited the CAs of the 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-007-TLS-BR-2023 covers multiple Root-CAs and consists of 20 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   *Tibor Németvári*
reviewer   Lead Auditor

This attestation is based on the template version 3.1 as of 2023-08-24, that was approved for use by ACAB-c.

General audit information

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor

- CAB HUNGUARD Informatics and IT R&D and General Service Provider Ltd., 6 Kékgolyó str. Budapest 1123 Hungary, registered under 01 09 069295
- Accredited by National Accreditation Authority (Hungary) under registration NAH-6-0048/2018[1] for the certification of trust services according to "EN ISO/IEC 17065:2013" and ETSI EN 319 403-1 V2.3.1 (2020-06)".
- Insurance Carrier (BRG section 8.2):
  Generali Biztosító Zrt.
- Third-party affiliate audit firms involved in the audit:
  None.

Identification and qualification of the audit team

- Number of team members: 2
- Academic qualifications of team members:
  All team members have formal academic qualifications or professional training or extensive experience indicating general capability to carry out audits based on the knowledge given below and at least four years full time practical workplace experience in information technology, of which at least two years have been in a role or function relating to relevant trust services, public key infrastructure, information security including risk assessment/management, network security and physical security.
- Additional competences of team members:
- All team members have knowledge of
  1) audit principles, practices and techniques in the field of CA/TSP audits gained in a training course of at least five days;
  2) the issues related to various areas of trust services, public key infrastructure, information security including risk assessment/management, network security and physical security;
  3) the applicable standards, publicly available specifications and regulatory requirements for CA/TSPs and other relevant publicly available specifications including standards for IT product evaluation; and
  4) the Conformity Assessment Body's processes.
  Furthermore, all team members have language skills appropriate for all organizational levels within the CA/TSP organization; note-taking, report-writing, presentation, and interviewing skills; and relevant personal attributes: objective, mature, discerning, analytical, persistent and realistic.
- Professional training of team members:
  See "Additional competences of team members" above. Apart from that are all team members trained to demonstrate adequate competence in:
  a) knowledge of the CA/TSP standards and other relevant publicly available specifications;
  b) understanding functioning of trust services and information security including network security issues;
  c) understanding of risk assessment and risk management from the business perspective;

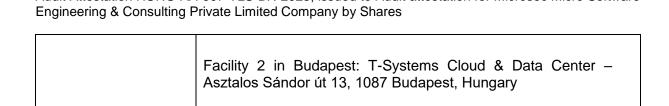[1] https://nah.gov.hu/admin/staticmedia/Reszletezo_okiratok/RO3-NAH-220217-6-0048-2018-V2-BNN-10398221-a.pdf

d) technical knowledge of the activity to be audited;
e) general knowledge of regulatory requirements relevant to TSPs; and
f) knowledge of security policies and controls.

- Types of professional experience and practical audit experience:
  The CAB ensures, that its personnel performing audits maintains competence on the basis of appropriate education, training or experience; that all relevant experience is current and prior to assuming responsibility for performing as an auditor, the candidate has gained experience in the entire process of CA/TSP auditing. This experience shall have been gained by participating under supervision of lead auditors in a minimum of four TSP audits for a total of at least 20 days, including documentation review, on-site audit and audit reporting.
- Additional qualification and experience Lead Auditor:
  On top of what is required for team members (see above), the Lead Auditor
  a) has acted as auditor in at least three complete TSP audits;
  b) has adequate knowledge and attributes to manage the audit process; and
  c) has the competence to communicate effectively, both orally and in writing.
- Special skills or qualifications employed throughout audit:
  National security clearance up to top secret level
- Special Credentials, Designations, or Certifications:
  All members are qualified and registered assessors within the accredited CAB.
  All members have CISA certificate
- Auditors code of conduct incl. independence statement:
  Code of Conduct as of Annex A, ETSI EN 319 403 or ETSI EN 319 403-1 respectively.

Identification and qualification of the reviewer performing audit quality management

- Number of Reviewers/Audit Quality Managers involved independent from the audit team: 1
- The reviewer fulfils the requirements as described for the Audit Team Members above and has acted as an auditor in at least three complete CA/TSP audits.

Identification of the CA / 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

Type of audit:	☐ Point in time audit ☐ Period of time, after x month of CA operation ☒ Period of time, full audit
Audit period covered for all policies:	2022-09-10 to 2023-09-09
Point in time date:	none, as audit was a period of time audit
Audit dates:	2023-08-22 (on site) 2023-09-11 to 2023-09-13 (on site)
Audit location:	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

	Facility 2 in Budapest: T-Systems Cloud & Data Center – Asztalos Sándor út 13, 1087 Budapest, Hungary

Root 1: e-Szigno Root CA 2017

Standards considered:	European Standards: • ETSI EN 319 411-2 V2.4.1 (2021-11) • ETSI EN 319 411-1 V1.3.1 (2021-05) • ETSI EN 319 401 V2.3.1 (2021-05) CA Browser Forum Requirements: • Baseline Requirements for TLS Server Certificates, version 2.0.1 For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403-1 V2.3.1 (2020-06)

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

1. e-Szignó Certification Authority, Unified Certificate Policies, version: 3.9 as of 2023-09-13, Date of effect: 2023-09-15
2. e-Szignó Certification Authority, Unified Certification Practice Statement, version: 3.9 as of 2023-09-13, Date of effect: 2023-09-15
3. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Certificate Policies, version: 3.7 as of 2023-08-24, Date of effect: 2023-08-30
4. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Certification Practice Statement, version: 3.7 as of 2023-08-24, Date of effect: 2023-08-30
5. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Disclosure Statement, version: 3.7 as of 2023-08-24, Date of effect: 2023-08-30

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

Findings with regard to ETSI EN 319 401:

7.9 Incident management

It was found that one vulnerability was not categorized correctly by the organization in JIRA and therefore the organization's fix times was not accountable. The organization has presented planned changes to the JIRA ticketing system to implement categorization so that vulnerability management can be implemented as per the controls. [REQ-7.9-10]

Findings with regard to ETSI EN 319 411-1:
None.

Findings with regard to ETSI EN 319 411-2:
None.

All non-conformities have been closed before the issuance of this attestation.

This Audit Attestation also covers the following incident as described in the following.
- MICROSEC: Incident report - No OCSP status response for 2 Precertificates

- https://bugzilla.mozilla.org/show_bug.cgi?id=1844514.

Microsec OCSP responder failed to send correct answer for two precertificates (2022-12-16 and 2023-04-14). The problem was caused by a configuration problem in the CA program: the precertificate was not added to the OCSP responders database, when at least one log server could respond with an SCT, but failed to collect sufficient SCT due to an unknown log server error message.

- The CA made the following immediate actions
- added the two missing precertificates to its OCSP responders database
- revoked the two problematic precertificates immediately
- A quick initial investigation was made to find out the reason of the problem.
- identified the causes of the problem as you see it above.
- made a quick fix on the CA program, which reduces the chance to have this type of problem again
- Microsec opened an incident bug in Mozilla's Bugzilla

Our on-site inspection reviewed the measures, which we accepted and made no further comments [REQ-7.9-6]

The remediation measures taken by Microsec as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident.

Distinguished Name	SHA-256 fingerprint	Applied policy
e-Szigno Root CA 2017 C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/ CN=e-Szigno Root CA 2017	BEB00B30839B9BC32C32E4447905950641F26421B15ED089198B518AE2EA1B99	ETSI EN 319 411-1 V1.3.1, LCP, NCP, NCP+, OVCP, DVCP, IVCP, EVCP ETSI EN 319 411-2 V2.4.1, QCP-l, QCP-l-qscd, QCP-n, QCP-n-qscd and QEVCP-w of ETSI EN 319 421 V1.1.1, BTSP

Table 1: Root-CA 1 in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy
/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno Class2 CA 2017	42DC827F46FB5E85DFFAE47D3C690F501ECE25D575D597A50D8F878FA42AFCEA	ETSI EN 319 411-1 V1.3.1, LCP
/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno Class2 SSL CA 2017	2A0E3F2A77A80DCBE5CD52D50D65076EBD37FAD531DB10D6A1385A557F7B725D	ETSI EN 319 411-1 V1.3.1, OVCP, DVCP, IVCP
/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno Class3 CA 2017	4F83842F1F04AB1E04D4D8E751666FCA82E5191CAFC24062BFD1FE77C02CA4B4	ETSI EN 319 411-1 V1.3.1, NCP, NCP+
/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno Class3 SSL CA 2017	BCBC18C463B61F3A033B10C74974ED8A2C328AFCD67A338D9871506A3515419F	ETSI EN 319 411-1 V1.3.1, OVCP, DVCP, IVCP
/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno Online SSL CA 2017	974B82076154CEFF56ED4DB562186F7394A02FF387AA205D6367A8B08FF7FAA0	ETSI EN 319 411-1 V1.3.1, OVCP, DVCP, IVCP
/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno Pseudonymous CA 2017	6A6F2FA13B2D9DBBB409802002D3370672760A2178D9B8D5694D660474231FA4	ETSI EN 319 411-1 V1.3.1, LCP, NCP, NCP+
/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno Qualified CA 2017	5ABE5818F6D02F05106C6C355540E1BE217C2354B535CF2507BF8515E1A6044A	ETSI EN 319 411-2 V2.4.1, QCP-n-qscd

/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno Qualified Organization CA 2017	`12EA26F6EEEFEC76AB8592545403AB88515B00E275D9888713407A86FC5C7FD7`	ETSI EN 319 411-2 V2.4.1, QCP-l-qscd
/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno Qualified Pseudonymous CA 2017	`1648CE4AB1BB65C485CB2236C768FABB865147D426915B92AFBCA81E9B2EE3BC`	ETSI EN 319 411-2 V2.4.1, QCP-n
/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno Qualified QCP CA 2017	`6081BEE5B0DF191AC4E265AC0F6F7899F078B8C89F06055AE166AF91DF70D6E0`	ETSI EN 319 411-2 V2.4.1, QCP-l-NCP+, QCP-n-NCP+, QPC-l, QCP-n
/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno Qualified TLS CA 2018	`7DF800075F5203C017364E81195A9AC9FF00C507D64A70F737D8D3E8CB3F0845`	ETSI EN 319 411-2 V2.4.1, QEVCP-w

Table 2: Sub-CA's issued by the Root-CA 1 or its Sub-CA's in scope of the audit

Key generation date	Key identifier (short name)	Key usage	Key type and parameters	CA name	Public key

Table 3: Key generation related to e-Szigno Root CA 2017

There was no CA key generation in the period under review.

There was no CA key destruction in the period under review.

Root 2: Microsec e-Szigno Root CA 2009

Standards considered:	European Standards: • ETSI EN 319 411-2 V2.4.1 (2021-11) • ETSI EN 319 411-1 V1.3.1 (2021-05) • ETSI EN 319 401 V2.3.1 (2021-05) CA Browser Forum Requirements: • Baseline Requirements for TLS Server Certificates, version 2.0.1 For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403-1 V2.3.1 (2020-06)

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

1. e-Szignó Certification Authority, Unified Certificate Policies, version: 3.9 as of 2023-09-13, Date of effect: 2023-09-15
2. e-Szignó Certification Authority, Unified Certification Practice Statement, version: 3.9 as of 2023-09-13, Date of effect: 2023-09-15
3. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Certificate Policies, version: 3.7 as of 2023-08-24, Date of effect: 2023-08-30
4. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Certification Practice Statement, version: 3.7 as of 2023-08-24, Date of effect: 2023-08-30
5. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Disclosure Statement, version: 3.7 as of 2023-08-24, Date of effect: 2023-08-30

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

Findings with regard to ETSI EN 319 401:

7.9 Incident management

It was found that one vulnerability was not categorized correctly by the organization in JIRA and therefore the organization's fix times was not accountable. The organization has presented planned changes to the JIRA ticketing system to implement categorization so that vulnerability management can be implemented as per the controls. [REQ-7.9-10]

Findings with regard to ETSI EN 319 411-1:
None.

Findings with regard to ETSI EN 319 411-2:
None.

All non-conformities have been closed before the issuance of this attestation.

This Audit Attestation also covers the following incident as described in the following.

- MICROSEC: Incident report - No OCSP status response for 2 Precertificates
  - https://bugzilla.mozilla.org/show_bug.cgi?id=1844514.

    Microsec OCSP responder failed to send correct answer for two precertificates (2022-12-16 and 2023-04-14). The problem was caused by a configuration problem in the CA program: the precertificate was not added to the OCSP responders database, when at least one log server could respond with an SCT, but failed to collect sufficient SCT due to an unknown log server error message.

    - The CA made the following immediate actions
    - added the two missing precertificates to its OCSP responders database
    - revoked the two problematic precertificates immediately
    - A quick initial investigation was made to find out the reason of the problem.
    - identified the causes of the problem as you see it above.
    - made a quick fix on the CA program, which reduces the chance to have this type of problem again
    - Microsec opened an incident bug in Mozilla's Bugzilla

    Our on-site inspection reviewed the measures, which we accepted and made no further comments [REQ-7.9-6]

The remediation measures taken by Microsec as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident.

Distinguished Name	SHA-256 fingerprint	Applied policy
/C=HU/L=Budapest/O=Microsec Ltd./CN=Microsec e-Szigno Root CA 2009	3C5F81FEA5FAB82C64BFA2EAECAFCDE8E077FC8620A7CAE537163DF36EDBF378	ETSI EN 319 411-1 V1.3.1, LCP, NCP, NCP+, OVCP, DVCP, IVCP, EVCP ETSI EN 319 411-2 V2.4.1, QCP-l, QCP-l-qscd, QCP-n, QCP-n-qscd, QEVCP-w of ETSI EN 319 421 V1.1.1, BTSP
/C=HU/L=Budapest/O=Microsec Ltd./CN=Microsec e-Szigno Root CA 2009	72F9AF2158181BAF16D60C9B4E6F4BD7CA8D2341AD48AFDB67CB4C8332D546F6	ETSI EN 319 411-1 V1.3.1, LCP, NCP, NCP+, OVCP, DVCP, IVCP, EVCP ETSI EN 319 411-2 V2.4.1, QCP-l, QCP-l-qscd, QCP-n, QCP-n-qscd, QEVCP-w of ETSI EN 319 421 V1.1.1, BTSP
/C=HU/L=Budapest/O=Microsec Ltd./CN=Microsec e-Szigno Root CA 2009	8E8C6EBF77DC73DB3E38E93F4803E62B6B5933BEB51EE4152F68D7AA14426B31	ETSI EN 319 411-1 V1.3.1, LCP, NCP, NCP+, OVCP, DVCP, IVCP, EVCP ETSI EN 319 411-2 V2.4.1, QCP-l, QCP-l-qscd, QCP-n, QCP-n-qscd, QEVCP-w of ETSI EN 319 421 V1.1.1, BTSP

Table 4: Root-CA 2 in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy
/C=HU/L=Budapest/O=Microsec Ltd./CN=Advanced Class 2 e-Szigno CA 2009	C63543729A370C26952B47E1D1D1AEA84CB1B07F1B0F964C2FEDDC523FD7C795	ETSI EN 319 411-1 V1.3.1, LCP
/C=HU/L=Budapest/O=Microsec Ltd./CN=Advanced Class 3 e-Szigno CA 2009	B0A6EF0350E7C4C6056BEEA7AF9D2D860B9ED102137B9729D3C23216D195546A	ETSI EN 319 411-1 V1.3.1, NCP, NCP+
/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	ETSI EN 319 411-1 V1.3.1, LCP
/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	ETSI EN 319 411-1 V1.3.1, NCP, NCP+

/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497-2-41/CN=Advanced eIDAS Class2 e-Szigno CA 2016	A29C104B100C3A7933473E62E4BE6371D653A1604D04EDAAD02C95806065CEE3	ETSI EN 319 411-1 V1.3.1, LCP
/C=HU/L=Budapest/O=Microsec Ltd./CN=Advanced Pseudonymous e-Szigno CA 2009	D0E39AA7D2FA53581008A15D825C57D25BD49247834431F8A227A29C280A1C0C	ETSI EN 319 411-1 V1.3.1, LCP, NCP, NCP+
/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497-2-41/CN=Class2 e-Szigno SSL CA 2016	3912C585E727F2B077888F678F043FD8DDCEE9E91E6628A6245B1B8EBBCC3912	ETSI EN 319 411-1 V1.3.1, OVCP, DVCP, IVCP
/C=HU/L=Budapest/O=Microsec Ltd./CN=e-Szigno SSL CA 2014	EAC241C0440A36830111383336BC20CAC7409C20F6E88D4F84F4827BE919E338	ETSI EN 319 411-1 V1.3.1, OVCP, DVCP, IVCP
/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497-2-41/CN=Online e-Szigno SSL CA 2016	31DAA25D142D08B90E640D4BC50B249F0FE39785C98D5E53E233259C0FAE9398	ETSI EN 319 411-1 V1.3.1, OVCP, DVCP, IVCP
/C=HU/L=Budapest/O=Microsec Ltd./CN=Qualified e-Szigno CA 2009	B884ED6527433687627D35157E904690D2DFF6A5DCD3CE267BBAF159C06F5054	ETSI EN 319 411-2 V2.4.1, QCP-n-qscd
/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497-2-41/CN=Qualified e-Szigno Organization CA 2016	60AF9E5F39D873B236BE142BC706DA571849AED7FAE635FC5A1461A0CF7459C5	ETSI EN 319 411-2 V2.4.1, QCP-l-qscd
/C=HU/L=Budapest/O=Microsec Ltd./CN=Qualified e-Szigno QCP CA 2012	CFCB60C1F0180C68E3EA5D24B4A05E9D9900D87C3D83D503CE1690B3C1656458	ETSI EN 319 411-2 V2.4.1, QCP-l-NCP+, QCP-n-NCP+, QCP-l, QCP-n
/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=Qualified e-Szigno TLS CA 2018	F7C7E28FB5E79F314AAAC6BBBA932F15E1A72069F435D4C9E707F93CA1482EE3	ETSI EN 319 411-1 V1.3.1, EVCP, ETSI EN 319 411-2 V2.4.1, QEVCP-w
/C=HU/L=Budapest/O=Microsec Ltd./CN=Qualified Pseudonymous e-Szigno CA 2009	F8684D2812BA98A52FE94528C4CB152378A2D73A828810A8C7B8529875C64674	ETSI EN 319 411-2 V2.4.1, QCP-n
/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=Class3 KET e-Szigno CA 2018	7BCF1C8A12EE0B2854A1B41070652B0325E7D0C20B9C44D4ACE9C643387F1431	ETSI EN 319 411-1 V1.3.1, NCP, NCP+

/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=Qualified KET e-Szigno CA 2018	`D9E445B22C6FCB37B296FCD1331486569651A8DB98071753FEFC73D2C97BF732`	ETSI EN 319 411-2 V2.4.1, QCP-l-qscd, QCP-l, QCP-n-qscd, QCP-n
C=HU,L=Budapest,O=Microsec Ltd.,2.5.4.97=VATHU-23584497,CN=e-Szigno Class2 SSL CA 2017	`FD8E0C8CCCDBBAE4C1F07C248D11FEBBB0FB3DA0CD0D894A8A80D804A8D39A7D`	ETSI EN 319 411-1 V1.3.1, OVCP, DVCP, IVCP
C=HU,L=Budapest,O=Microsec Ltd.,2.5.4.97=VATHU-23584497,CN=e-Szigno Class3 SSL CA 2017	`1744D73134F95CE916ADEBEE6F75742C47936868B64D2A0C162EF132900F0EE4`	ETSI EN 319 411-1 V1.3.1, OVCP, DVCP, IVCP
C=HU,L=Budapest,O=Microsec Ltd.,2.5.4.97=VATHU-23584497,CN= e-Szigno DV TLS CA 2023	`C04C30E40DD7E96982F8606EBEF35548E5C6F4F792A52A5178CF24A0E9FD7396`	ETSI EN 319 411-1 V1.3.1, DVCP
C=HU,L=Budapest,O=Microsec Ltd.,2.5.4.97=VATHU-23584497,CN= e-Szigno Online SSL CA 2017	`B274FEBE6EBC71866C339F018AD933E7CD6805B43BFDE6D218DC21147169D76B`	ETSI EN 319 411-1 V1.3.1, OVCP, DVCP, IVCP
C=HU,L=Budapest,O=Microsec Ltd.,2.5.4.97=VATHU-23584497,CN= e-Szigno OV TLS CA 2023	`12D4537A7547FF63C36923622A281AFFE9481120DB781776AAF981A1F9B668D8`	ETSI EN 319 411-1 V1.3.1, OVCP, DVCP, IVCP
Subject: C=HU,L=Budapest,O=Microsec Ltd.,2.5.4.97=VATHU-23584497,CN= e-Szigno Qualified TLS CA 2023	`A115EC0D73C2E8ABB1883134FA2DF0D985E741881604A4082907D705E2407C72`	ETSI EN 319 411-1 V1.3.1, OVCP, DVCP, IVCP
Subject: C=HU,L=Budapest,O=Microsec Ltd.,2.5.4.97=VATHU-23584497,CN=e-Szigno Qualified TLS CA 2018	`6A48E734AC6F067140C928ADBBCC4492469D416DE2D3C9A7A197D62370EAC0E2`	ETSI EN 319 411-1 V1.3.1, OVCP, DVCP, IVCP

Table 5: Sub-CA's issued by the Root-CA 2 or its Sub-CA's in scope of the audit

Key generation date	Key identifier (short name)	Key usage	Key type and parameters	CA name	Public key
2023-07-05	eovtlsca2023	Sub CA	ECC / NIST P-256 (256 bits)	e-Szigno OV TLS CA 2023	pub: 04:33:9b:b3:8f:23:ea:aa:fe:70:15:ff:9a:38:05: f5:26:3d:b6:8b:95:51:16:1d:4c:61:ed:8b:79:37:

					60:52:b6:aa:8a:86:0f:c2:b0:9d:6a:39:7b:ce:99: 38:f4:3e:87:dd:10:ee:0c:3e:a6:41:b7:0e:89:4f: c7:b9:01:9e:80 ASN1 OID: prime256v1 NIST CURVE: P-256
2023-07-05	edvtlsca2023	Sub CA	ECC / NIST P-256 (256 bits)	e-Szigno DV TLS CA 2023	pub: 04:a2:e6:25:9a:e1:f4:1a:ba:8a:f5:c3:13:66:12: 58:8f:7d:57:c1:f5:da:26:10:81:2c:da:34:66:b2: dc:ab:e6:ab:75:b7:93:64:df:c9:4e:97:cb:e8:3a: ce:a3:98:3a:c9:85:73:77:5b:ac:47:b8:48:44:03: c6:db:ec:be:77 ASN1 OID: prime256v1 NIST CURVE: P-256

Table 6: Key generation related to Microsec e-Szigno Root CA 2009

There was no CA key destruction in the period under review.

Root 3: e-Szigno TLS Root CA 2023

Standards considered:	European Standards: • ETSI EN 319 411-2 V2.4.1 (2021-11) • ETSI EN 319 411-1 V1.3.1 (2021-05) • ETSI EN 319 401 V2.3.1 (2021-05) CA Browser Forum Requirements: • Baseline Requirements for TLS Server Certificates, version 2.0.1 For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403-1 V2.3.1 (2020-06)

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

1. e-Szignó Certification Authority, Unified Certificate Policies, version: 3.9 as of 2023-09-13, Date of effect: 2023-09-15
2. e-Szignó Certification Authority, Unified Certification Practice Statement, version: 3.9 as of 2023-09-13, Date of effect: 2023-09-15
3. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Certificate Policies, version: 3.7 as of 2023-08-24, Date of effect: 2023-08-30
4. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Certification Practice Statement, version: 3.7 as of 2023-08-24, Date of effect: 2023-08-30
5. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Disclosure Statement, version: 3.7 as of 2023-08-24, Date of effect: 2023-08-30
6.

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

Findings with regard to ETSI EN 319 401:

7.9 Incident management

It was found that one vulnerability was not categorized correctly by the organization in JIRA and therefore the organization's fix times was not accountable. The organization has presented planned changes to the JIRA ticketing system to implement categorization so that vulnerability management can be implemented as per the controls. [REQ-7.9-10]

Findings with regard to ETSI EN 319 411-1:
None.

Findings with regard to ETSI EN 319 411-2:
None.

All non-conformities have been closed before the issuance of this attestation.

This Audit Attestation also covers the following incident as described in the following.

- MICROSEC: Incident report - No OCSP status response for 2 Precertificates
  - https://bugzilla.mozilla.org/show_bug.cgi?id=1844514.

    Microsec OCSP responder failed to send correct answer for two precertificates (2022-12-16 and 2023-04-14). The problem was caused by a configuration problem in the CA program: the precertificate was not added to the OCSP responders database, when at least one log server could respond with an SCT, but failed to collect sufficient SCT due to an unknown log server error message.

    - The CA made the following immediate actions
    - added the two missing precertificates to its OCSP responders database
    - revoked the two problematic precertificates immediately
    - A quick initial investigation was made to find out the reason of the problem.
    - identified the causes of the problem as you see it above.
    - made a quick fix on the CA program, which reduces the chance to have this type of problem again
    - Microsec opened an incident bug in Mozilla's Bugzilla

    Our on-site inspection reviewed the measures, which we accepted and made no further comments [REQ-7.9-6]

The remediation measures taken by Microsec as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident.

Distinguished Name	SHA-256 fingerprint	Applied policy
C=HU, L=Budapest, O=Microsec Ltd./2.5.4.97=VATHU-23584497, CN= e-Szigno TLS Root CA 2023	B49141502D00663D740F2E7EC340C52800962666121A36D09CF7DD2B90384FB4	ETSI EN 319 411-1 V1.3.1, LCP, NCP, NCP+, OVCP, DVCP, IVCP, EVCP ETSI EN 319 411-2 V2.4.1, QCP-l, QCP-l-qscd, QCP-n, QCP-n-qscd, QEVCP-w of ETSI EN 319 421 V1.1.1, BTSP

Table 7: Root-CA 2 in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy
C=HU,L=Budapest,O=Microsec Ltd.,2.5.4.97=VATHU-23584497,CN= e-Szigno Qualified TLS CA 2023	9E4115FD70E2317E15BF811552610643B32818A0304AA3C97685A76465493261	ETSI EN 319 411-1 V1.3.1, OVCP, DVCP, IVCP
C=HU,L=Budapest,O=Microsec Ltd.,2.5.4.97=VATHU-23584497,CN= e-Szigno DV TLS CA 2023	076B30115E430F7C58EBBC1B79ECCE567704D9AA3DA15F5060855A880E237155	ETSI EN 319 411-1 V1.3.1, DVCP
C=HU,L=Budapest,O=Microsec Ltd.,2.5.4.97=VATHU-23584497,CN= e-Szigno OV TLS CA 2023	6F265CCE1F350817ED888C9A07CE8D117E6647090894971C405C0D72EC959D5C	ETSI EN 319 411-1 V1.3.1, OVCP

Table 8: Sub-CA's issued by the Root-CA 2 or its Sub-CA's in scope of the audit

Key generation date	Key identifier (short name)	Key usage	Key type and parameters	CA name	Public key
2023-06-07	tlsrootca2023	root CA	ECC / NIST P-521	e-Szigno TLS Root CA 2023	pub: 04:00:68:0f:df:a2:7c:3c:aa:74:88:61:0a:8d:c2: 4c:a5:01:22:14:d4:f7:60:77:42:9c:0a:38:60:a1: 8c:67:3e:b3:63:e9:fa:91:b0:8b:4b:e6:39:df:02: c2:30:01:52:00:bf:df:8c:ed:59:ad:32:65:ab:09: 59:50:b5:19:c2:68:1c:00:e0:05:5f:da:50:26:1c: c3:ac:04:22:c5:3a:4d:ef:e9:57:58:36:a3:c1:19: 53:10:0a:d1:cd:3f:ef:4b:35:1a:43:8f:42:13:4c: b9:2c:1a:9c:be:30:b6:c4:de:dc:4b:9d:e4:a4:3c: cb:2e:d9:ad:df:df:7d:09:df:2e:92:ff:a1 ASN1 OID: secp521r1 NIST CURVE: P-521
2023-07-05	eovtlsca2023	Sub CA	ECC / NIST P-256 (256 bits)	e-Szigno OV TLS CA 2023	pub: 04:33:9b:b3:8f:23:ea:aa:fe:70:15:ff:9a:38:05: f5:26:3d:b6:8b:95:51:16:1d:4c:61:ed:8b:79:37: 60:52:b6:aa:8a:86:0f:c2:b0:9d:6a:39:7b:ce:99: 38:f4:3e:87:dd:10:ee:0c:3e:a6:41:b7:0e:89:4f: c7:b9:01:9e:80 ASN1 OID: prime256v1 NIST CURVE: P-256
2023-07-05	edvtlsca2023	Sub CA	ECC / NIST P-256 (256 bits)	e-Szigno DV TLS CA 2023	pub: 04:a2:e6:25:9a:e1:f4:1a:ba:8a:f5:c3:13:66:12: 58:8f:7d:57:c1:f5:da:26:10:81:2c:da:34:66:b2: dc:ab:e6:ab:75:b7:93:64:df:c9:4e:97:cb:e8:3a: ce:a3:98:3a:c9:85:73:77:5b:ac:47:b8:48:44:03: c6:db:ec:be:77 ASN1 OID: prime256v1 NIST CURVE: P-256

Table 9: Key generation related to e-Szigno TLS Root CA 2023

There was no CA key destruction in the period under review.

Modifications record

Version	Issuing Date	Changes
Version 1	2023-10-16	Initial attestation
Version 1.1	2023-10-25	1st amended attestation
Version 1.2	2023-12-20	2nd amended attestation
Version 1.3	2024-02-19	3rd amended attestation

End of the audit attestation letter.

Audit Attestation HUNG-AA-007-TLS-BR-2023, issued to Audit attestation for Microsec Micro Software Engineering & Consulting Private Limited Company by Shares

page 20 of 20 pages