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

TLS BR Audit Attestation for

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

Reference: HUNG-AA-010-TLS-BR-2024

"Budapest, 26 November, 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-010-TLS-BR-2024 covers multiple Root-CAs and consists of 23 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,

Digitálisan aláírta: HUNGUARD

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-6-0048/2023[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/RO1-231019-6-0048-2018-UA_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:	2023-09-10 to 2024-09-09
Point in time date:	none, as audit was a period of time audit
Audit dates:	2024-09-09 to 2024-09-11 (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 V2.5.1 (2023-10) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.1 (2024-06) CA Browser Forum Requirements: • Baseline Requirements for TLS Server Certificates, version 2.0.8 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: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
2. e-Szignó Certification Authority, Unified Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
3. e-Szignó Certification Authority, eIDAS conform Certificates for Website Authentication Certificate Policy, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
4. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
5. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Disclosure Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01

No major or minor non-conformities have been identified during the audit.

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

Incident 1:

- MICROSEC: Incident report - Disallowed subject attribute field in DV certificate
  - https://bugzilla.mozilla.org/show_bug.cgi?id=1889699.

Summary

It was reported on an MELASZ's internal mailing list that the Digicert linter (https://github.com/digicert/pkilint) already supports the current CABFBR requirements. Three misissued DV certificates was reported to Microsec. The problem is that the reported DV certificates contain the SerialNumber extension (2.5.4.5), which is not allowed in DV certificates. The next day, Microsec received another email from Sectigo reporting a misissued DV certificate with the same problem.

Impact

The misissued DV certificates contain the SerialNumber (2.5.4.5) extension, which is not allowed in DV certificates. The presence of this extra field has no impact on the usability or security of the certificate, but it unnecessarily increases the size of the certificate.

Root cause

- Microsec assigns a unique OID to each Client and places this OID into this field for each certificate type to easily identify the Client. The only exception was EV certificates, where this field is used to store other information.
- Microsec made a mistake when it failed to recognize that this field is not allowed in DV certificates
- Due to the small number of DV certificates issued, this problem has remained unexplored until now
- Microsec uses two linters prior the issuance (certlint and zlint), but none of them could indicate this problem.

Incident 2:

- MICROSEC: Incident report – Late response to a CPR
    - https://bugzilla.mozilla.org/show_bug.cgi?id=1886998.

Summary

It was reported by email to info@... , that Microsec misissued an EV certificate. The problem was that the certificate does not contain the CPSuri link. Microsec did not react in time, so a second email was sent to info@... and also to the Microsec's CCADB contact persons. Due to the delay, 3 separate incident reports will be created as follows:

- Bug #1 must focus on the certificate misissuance reported in the problem report.
- Bug #2 must focus on the delayed revocation of the misissued certificates described in the problem report.
- Bug #3 must focus on the failure to respond to a certificate problem report in a complete and/or timely manner.

- Bug #1 already opened, see https://bugzilla.mozilla.org/show_bug.cgi?id=1886257
- Bug #2 issue will be presented in separate bug.
- The current bug focuses on the late response (Bug #3).

Impact

The missing CPSuri information has no impact on the usability or security of the certificate, but it makes it more difficult for users to find the policy information. The misissued certificate is: https://crt.sh/?id=12302329269

Root Cause

The late response was caused by different thing happening simultaneously

- the emails were sent to info@ email address
    - Microsec offers special email addresses for revocation requests and for High Priority Problem Reports.
        - emails received on these special addresses are processed within 24 hours

- This email address is given in CCADB as a general contact email. The purpose of this email address according to CCADB note:
  - "CA Email Alias 1 and 2 are used to reach more than one person in your organization to receive notifications in case the primary contact is out of the office or leaves the organization."

- The input email did not match to any existing classification so it was forwarded to "Standard waiting list"
- Peek load on the "Standard waiting list"
  - Microsec launched a big campaign to replace old signature cards on 2024-03-06, and this resulted a huge pick load in the incoming email traffic.
  - Usually each ticket in this list is processed in less than 3 workdays, but due to the mentioned project the processing delay temporarily increased to 8-10 days
  - First email was to be processed when the second email arrived

- The second email was sent to the contact persons directly and was processed in two hours by one of the contact persons

- The first email was sent from a standard @gmail.com address
  - there are special domain names which are managed with higher priority, but free email addresses are not among them
  - the second email was sent from @google com domain
    - it was forwarded to another waiting list and was processed very quickly

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 V2.5.1 (2023-10) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.1 (2024-06) CA Browser Forum Requirements: • Baseline Requirements for TLS Server Certificates, version 2.0.8 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: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
2. e-Szignó Certification Authority, Unified Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
3. e-Szignó Certification Authority, eIDAS conform Certificates for Website Authentication Certificate Policy, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
4. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
5. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Disclosure Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01

No major or minor non-conformities have been identified during the audit.

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

Due to over-certification, the same incidents occurred under this root certificate, which we presented in detail in the chapter Root 1: e-Szigno Root CA 2017

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,
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

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

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

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 V2.5.1 (2023-10) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.1 (2024-06) CA Browser Forum Requirements: • Baseline Requirements for TLS Server Certificates, version 2.0.8 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: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
2. e-Szignó Certification Authority, Unified Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
3. e-Szignó Certification Authority, eIDAS conform Certificates for Website Authentication Certificate Policy, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
4. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
5. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Disclosure Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01

No major or minor non-conformities have been identified during the audit.

To the best of our knowledge, no incidents have occurred within this Root-CA's hierarchy during the audited period.

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

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

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

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

Root 4: e-Szigno TLS Root CA 2024

Standards considered:	European Standards: • ETSI EN 319 411-2 V2.5.1 (2023-10) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.1 (2024-06) CA Browser Forum Requirements: • Baseline Requirements for TLS Server Certificates, version 2.0.8 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: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
2. e-Szignó Certification Authority, Unified Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
3. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Certificate Policies, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
4. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
5. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Disclosure Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01

No major or minor non-conformities have been identified during the audit.

To the best of our knowledge, no incidents have occurred within this Root-CA's hierarchy during the audited period.

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 2024	328CDF63622AFB8A3FBC1347FD3389F918DA4A33F80AF34522D34B5BDA9CCB82	ETSI EN 319 411-1 V1.4.1, LCP, NCP, OVCP, DVCP, IVCP, EVCP ETSI EN 319 411-2 V2.5.1, QEVCP-w, QCP-w-psd2

Table 10: Root-CA 4 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	88D307173ACDECF48B81F6469EAE798BAE6E5703CB6223EE82534AC769ACC422	ETSI EN 319 411-1 V1.4.1, NCP, OVCP, EVCP ETSI EN 319 411-2 V2.5.1, QEVCP-w, QCP-w-psd2
C=HU,L=Budapest,O=Microsec Ltd.,2.5.4.97=VATHU-23584497,CN= e-Szigno DV TLS CA 2023	57A019C680987C8CB86B01F84F7DEF2C98B39B29A7C4F14AF1765ECF457A0706	ETSI EN 319 411-1 V1.4.1, LCP, DVCP
C=HU,L=Budapest,O=Microsec Ltd.,2.5.4.97=VATHU-23584497,CN= e-Szigno OV TLS CA 2023	728E604C51CFBD6ED1A673529598DDA17523DC61DD90E2551B0D57DD3A19F7AA	ETSI EN 319 411-1 V1.4.1, LCP, OVCP, IVCP

Table 11: Sub-CA’s issued by the Root-CA 4 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
2024-07-03	etlsrootca2024	root CA	ECC / NIST P-384	e-Szigno TLS Root CA 2024	pub: 04:73:84:65:1d:04:da:db:fa:63:1b:6c:3f:58:d2:80: ce:71:c6:4e:d3:05:ad:86:0f:97:5e:91:b1:9a:a5:55: a5:e0:2f:ae:96:e6:b1:f5:36:97:38:35:a0:92:98:0c: 49:2d:f6:25:75:7f:5e:15:0c:d9:40:a4:f3:b3:f6:5f: 97:0a:e9:2a:3b:1b:e9:35:fd:1b:7c:33:f8:29:2a:9f: 5a:66:a3:b0:6c:19:c3:ab:14:8a:19:df:56:96:9b:79:f3 ASN1 OID: secp384r1 NIST CURVE: P-384

Table 12: Key generation related to e-Szigno TLS Root CA 2024

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

Other aspects of key management

The HSMs used by Microsec store the keys in encrypted files on the servers in highly protected environments.

Microsec creates key backup CD-s that contain all Root CA and Subordinate CA keys after any change in CA key list.

The key backup CD-s are created in 2 copies and stored in two physically separate locations at a safe distance (>10km).

After the new key backup CDs are created, the new CD-s are delivered to the backup locations, and the previous key backup CDs are collected and destroyed.

The table below summarizes the most important key backup events in the period under review.

Change in keys	Backup key CD move to backup site	Backup key CD bring back to Microsec	Backup key CD destruction	Backup key CD title	Backup location
2023-11-24		2024-03-18	2024-03-21	Microsec szolgáltatói kulcs archív CD Graphisoft	Graphisoft Fokozottan Védett Helyiség
2023-11-24		2024-03-21	2024-03-21	Microsec szolgáltatói kulcs archív CD Dataplex	Dataplex Fokozottan Védett Helyiség
2024-03-04	2024-03-18	2024-07-26	2024-08-21	Microsec szolgáltatói kulcs archív CD Graphisoft	Graphisoft Fokozottan Védett Helyiség
2024-03-04	2024-03-21	2024-07-26	2024-08-21	Microsec szolgáltatói kulcs archív CD Dataplex	Dataplex Fokozottan Védett Helyiség
2024-07-03	---	---	2024-08-21	Microsec szolgáltatói kulcs archív CD Graphisoft	Graphisoft Fokozottan Védett Helyiség
2024-07-03	---	---	2024-08-21	Microsec szolgáltatói kulcs archív CD Dataplex	Dataplex Fokozottan Védett Helyiség
2024-07-17	2024-07-26	2024-10-03	2024-10-15	Microsec szolgáltatói kulcs archív CD Graphisoft	Graphisoft Fokozottan Védett Helyiség
2024-07-17	2024-07-26	2024-10-03	2024-10-15	Microsec szolgáltatói kulcs archív CD Dataplex	Dataplex Fokozottan Védett Helyiség

2024-09-26	2024-10-03			Microsec szolgáltatói kulcs archív CD Graphisoft	Graphisoft Fokozottan Védett Helyiség
2024-09-26	2024-10-03			Microsec szolgáltatói kulcs archív CD Dataplex	Dataplex Fokozottan Védett Helyiség

Modifications record

Version	Issuing Date	Changes
Version 1.0	2024-11-26	Initial attestation

End of the audit attestation letter.