

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

Reference: HUNG-AA-010-2024

“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-010-2024 covers multiple Root-CAs and consists of 49 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

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-6-0048/2023¹ 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

<p>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.</p> <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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. 	
<p>Identification and qualification of the reviewer performing audit quality management</p>	
<ul style="list-style-type: none"> 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. 	
<p>Identification of the CA / Trust Service Provider (TSP):</p>	<p>MICROSEC Micro Software Engineering & Consulting Private Limited Company by Shares, Ángel Sanz Briz út 13, 1033 Budapest, Hungary, registered under 01-10-047218</p>
<p>Type of audit:</p>	<p><input type="checkbox"/> Point in time audit <input type="checkbox"/> Period of time, after x month of CA operation <input checked="" type="checkbox"/> Period of time, full audit</p>
<p>Audit period covered for all policies:</p>	<p>2023-09-10 to 2024-09-09</p>
<p>Point in time date:</p>	<p>none, as audit was a period of time audit</p>
<p>Audit dates:</p>	<p>2024-09-09 to 2024-09-11 (on site)</p>
<p>Audit location:</p>	<p>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</p>

	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:	<div>European Standards:<ul style="list-style-type: none">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)ETSI TS 119 411-6 V1.1.1 (2023-08)</div> <div>CA Browser Forum Requirements:<ul style="list-style-type: none">EV Guidelines for TLS Server Certificates, version 2.0.1Baseline Requirements for TLS Server Certificates, version 2.0.8Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.6Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, version 3.9.0</div> <div>For the Trust Service Provider Conformity Assessment:<ul style="list-style-type: none">ETSI EN 319 403-1 V2.3.1 (2020-06)</div>
-----------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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

- e-Szignó Certification Authority, Unified Certificate Policies, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
- e-Szignó Certification Authority, Unified Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
- e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Signature Certificate Policies, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
- e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Signature Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
- e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Signature Disclosure Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
- e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Signature, Certificate Policies, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
- e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Signature Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
- e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Signature Disclosure Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
- e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Seal Certificate Policies, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
- e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Seal Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01

11. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Seal Disclosure Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
12. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Seal Certificate Policies, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
13. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Seal Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
14. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Seal Disclosure Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
15. 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
16. 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
17. 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
18. e-Szignó Certification Authority, eIDAS conform Qualified Certificates for Website Authentication Certificate Policy, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
19. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Website Authentication Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
20. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Website Authentication Disclosure Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
21. e-Szignó Certification Authority, Non eIDAS covered Certificate, Certificate Policies, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
22. e-Szignó Certification Authority, Non eIDAS covered Certificates Certification Practice 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.

There were no non-conformity during the audit.

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

Incident 1:

- MICROSEC: Incident report - Disallowed subject attribute field in DV certificate
 - o 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
 - o 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]

Incident 3:

- Microsec: Misissuance an EV TLS certificate without CPSuri
 - https://bugzilla.mozilla.org/show_bug.cgi?id=1886257

Summary

It was reported by email to info@... , that Microsec misissued an EV certificate.

The problem is 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 contact persons CCADB.

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.

The current bug focuses on the certificate misissuance (Bug 1).

Other issues will be presented in separate bugs.

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

- Microsec released a new version of its Certificate Profiles. One of the most important changes was the update of the TLS certificate profiles according to the CABF Baseline Requirements ver 2.2.2. In this CABF BR version, the whole section 7 was overwritten and there were many specific and detailed requirements. In section 7.1.2.10.5 CA Certificate Policies Table 68 says that the presence of the policyQualifiers extension is NOT RECOMMENDED. Based on this requirement, Microsec decided to remove the policyQualifiers information from the TLS certificates.
- This was an error on Microsec's part, as the CABF EVG requires this information to be present in EV TLS subscriber certificates.
- Microsec uses two linters before the issuance (certlint and zlint), but none of them could find this problem.
- From this date until 2024-03-18, all issued EV TLS certificates were missing this CPSuri information.

Incident 4:

- Microsec: Delayed revocation of the misissued certificates
 - https://bugzilla.mozilla.org/show_bug.cgi?id=1887110

Summary

It was reported by email to info@... , that Microsec misissued an EV certificate.

The problem is 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 contact persons CCADB.

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.

The current bug focuses on the delayed revocation (Bug #2).

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

- There is a special type of certificate, called PSD2 QWAC, that can also meet EVG requirements. These certificates are not used for website authentication, so in practice they never cause problems in the operation of web browsers, but theoretically they can be used for this purpose, when issued under a Root CA that is trusted by any of the Root Programs.
- PSD2 certificates are used to secure connections between servers in financial services, as a client or server authentication certificate. A server can be connected to hundreds or even thousands of partners, such as banks or other financial service providers. In current solutions, the PSD2 QWAC certificate is propagated and trusted by each parties. In many cases this propagation cannot be done automatically, but it is a manual process that takes time. Changing a PSD2 QWAC certificate typically takes weeks on large networks, it definitely cannot be done in a few days. Early revocation of a misissued PSD2 QWAC certificate would result in a financial service interruption, resulting in potential losses and customer claims.
- It is a general problem of this PSD2 system solution, which PSD2 service providers should solve in the future by developing automation or using another trust model. In the event of a potential critical security issue with a PSD2 QWAC certificate, it shall be revoked within 24 hours, which would block these financial services. This problem cannot be solved now in this project.
- In our case the problem is the lack of CPSuri information in the certificate, which has no impact on the security in the use of the certificate. Extending the revocation deadline is much smaller problem than revoking the certificate in time and blocking these financial services.

The remediation measures taken by Microsec as described on Bugzilla (see link above) have been checked by the auditors and properlyproperlyproperlyproperly 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 V1.4.1, LCP, NCP, NCP+, OVCP, DVCP, IVCP, EVCP ETSI EN 319 411-2 V2.5.1, QCP-I, QCP-I-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 V1.4.1, LCP
/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno Class2 CodeSigning CA 2020	BA52633D91DFD48EE5B135B2543E8DD3557F2DB33C0534E41A2268097C3008CA	ETSI EN 319 411-1 V1.4.1, 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 V1.4.1, 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 V1.4.1, NCP, NCP+
/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno Class3 CodeSigning CA 2020	711CBB0479DDC596745815E797423305F95EDD792C5BC5854CED5A7FAFB4AA8D	ETSI EN 319 411-1 V1.4.1, 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 V1.4.1, 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 V1.4.1, 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 V1.4.1, 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 V2.5.1, 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 V2.5.1, QCP-I-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 V2.5.1, 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 V2.5.1, QCP-I-qscd, QCP-n-qscd, QPC-I, 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 V2.5.1, QEVCP-w
/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno TSA CA 2017	9E94BB8ADAD7A6CE4DCB1208F1239DC1E43483F1B7E81F74A90A20FB5E5C49B7	ETSI EN 319 421 V1.1.1, BTSP
/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno TSA CA 2020	B4C177E357565C99E90ED886D799F8C6BEFF806DA5A048551878489B9C27E488	ETSI EN 319 421 V1.1.1, BTSP
/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno Qualified SMIME CA 2023	A40938BABD88FF42144B611298E90B3426194099152C49EAA4A8A6EAF42D2DD2	ETSI EN 319 411-1 V1.4.1, LCP
C=HU,L=Budapest,O=Microsec Ltd.,2.5.4.97=VATHU-23584497,CN= e-Szigno SMIME CA 2023	EDFB8A183C13D1B2530F8DE9BC5F0AAEBC7145DECA4FB5094A40B2F6A3987A7C	ETSI EN 319 411-1 V1.4.1, LCP

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
2023-09-14	eqsmimeca2023	Sub CA	ECC / NIST P-256 (256 bits)	e-Szigno Qualified SMIME CA 2023	pub: 04:42:51:a3:df:35:cd:54:e3:07:a0:54:63:87:59: 5a:25:d2:2a:3b:cb:f3:f0:04:43:74:7c:bf:de:fc: 35:b4:6d:59:9b:56:0e:91:00:e6:9b:50:72:71:f0: 29:d8:79:fc:27:0d:21:25:8c:1e:1d:91:68:35:98: c0:be:4d:99:74 ASN1 OID: prime256v1 NIST CURVE: P-256

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

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

Root 2: Microsec e-Szigno Root CA 2009

Standards considered:	<p>European Standards:</p> <ul style="list-style-type: none">• 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)• ETSI TS 119 411-6 V1.1.1 (2023-08) <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none">• EV Guidelines for TLS Server Certificates, version 2.0.1• Baseline Requirements for TLS Server Certificates, version 2.0.8• Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.6• Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, version 3.9.0 <p>For the Trust Service Provider Conformity Assessment: ETSI EN 319 403-1 V2.3.1 (2020-06)</p>
-----------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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 Non-Qualified Certificate for Electronic Signature Certificate Policies, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
4. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Signature Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
5. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Signature Disclosure Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
6. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Signature, Certificate Policies, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
7. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Signature Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
8. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Signature Disclosure Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
9. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Seal Certificate Policies, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
10. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Seal Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01

11. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Seal Disclosure Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
12. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Seal Certificate Policies, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
13. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Seal Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
14. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Seal Disclosure Statement, version 3.14 as of 2024-08-27, Date of effect: 2024-09-01
15. 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
16. 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
17. 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
18. e-Szignó Certification Authority, eIDAS conform Qualified Certificates for Website Authentication Certificate Policy, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
19. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Website Authentication Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
20. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Website Authentication Disclosure Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
21. e-Szignó Certification Authority, Non eIDAS covered Certificate, Certificate Policies, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
22. e-Szignó Certification Authority, Non eIDAS covered Certificates Certification Practice 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.

There were no non-conformity during the audit.

This Audit Attestation also covers the following incidents 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	3C5F81FEA5FAB82C64BFA2EAEC AFCDE8E077FC8620A7CAE537163DF36EDBF378	ETSI EN 319 411-1 V1.4.1, LCP, NCP, NCP+, OVCP, DVCP, IVCP, EVCP ETSI EN 319 411-2 V2.5.1, QCP-I, QCP-I-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 V1.4.1, LCP, NCP, NCP+, OVCP, DVCP, IVCP, EVCP ETSI EN 319 411-2 V2.5.1, QCP-I, QCP-I-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 V1.4.1, LCP, NCP, NCP+, OVCP, DVCP, IVCP, EVCP ETSI EN 319 411-2 V2.5.1, QCP-I, QCP-I-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 V1.4.1, LCP
/C=HU/L=Budapest/O=Microsec Ltd./CN=Advanced Class 3 e-Szigno CA 2009	B0A6EF0350E7C4C6056BEEA7AF9D2D860B9ED102137B9729D3C23216D195546A	ETSI EN 319 411-1 V1.4.1, 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 V1.4.1, 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 V1.4.1, 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 V1.4.1, LCP
/C=HU/L=Budapest/O=Microsec Ltd./CN=Advanced Pseudonymous e-Szigno CA 2009	D0E39AA7D2FA53581008A15D825C57D25BD49247834431F8A227A29C280A1C0C	ETSI EN 319 411-1 V1.4.1, 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 V1.4.1, OVCP, DVCP, IVCP
/C=HU/L=Budapest/O=Microsec Ltd./CN=e-Szigno SSL CA 2014	EAC241C0440A36830111383336BC20CAC7409C20F6E88D4F84F4827BE919E338	ETSI EN 319 411-1 V1.4.1, 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 V1.4.1, OVCP, DVCP, IVCP
/C=HU/L=Budapest/O=Microsec Ltd./CN=Qualified e-Szigno CA 2009	B884ED6527433687627D35157E904690D2DFF6A5DCD3CE267BBAF159C06F5054	ETSI EN 319 411-2 V2.5.1, 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 V2.5.1, QCP-l-qscd
/C=HU/L=Budapest/O=Microsec Ltd./CN=Qualified e-Szigno QCP CA 2012	CFCB60C1F0180C68E3EA5D24B4A05E9D9900D87C3D83D503CE1690B3C1656458	ETSI EN 319 411-2 V2.5.1, QCP-l-qscd, QCP-n-qscd, 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 V1.4.1, EVCP, ETSI EN 319 411-2 V2.5.1, QEVCP-w
/C=HU/L=Budapest/O=Microsec Ltd./CN=Qualified Pseudonymous e-Szigno CA 2009	F8684D2812BA98A52FE94528C4CB152378A2D73A828810A8C7B8529875C64674	ETSI EN 319 411-2 V2.5.1, QCP-n
/C=HU/L=Budapest/O=Microsec Ltd./2.5.4.97=VATHU-23584497/CN=e-Szigno TSA CA 2020	7731FE893FD5461AD2BFAFBADC530CF69B6DA5095E3AEE0FF82EF54ADD4B8B57	ETSI EN 319 421 V1.1.1 BTSP

/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 V1.4.1, 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 V2.5.1, QCP-I-qscd, QCP-I, QCP-n-qscd, QCP-n
C=HU ,L=Budapest ,O=Microsec Ltd. ,2.5.4.97=VATHU-23584497 ,CN= e-Szigno Qualified SMIME CA 2023	206ED85E0F129A6DE85FEB064BADCB1B57F8DA94FA7D51BEF81F9C74317D2B184	ETSI EN 319 411-1 V1.4.1, LCP
C=HU,L=Budapest,O=Microsec Ltd.,2.5.4.97=VATHU-23584497,CN=e-Szigno Class2 SSL CA 2017	FD8E0C8CCCDDBAE4C1F07C248D11FEBBB0FB3DA0CD0D894A8A80D804A8D39A7D	ETSI EN 319 411-1 V1.4.1, 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 V1.4.1, 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 V1.4.1, 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 V1.4.1, 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 V1.4.1, OVCP,
C=HU,L=Budapest,O=Microsec Ltd.,2.5.4.97=VATHU-23584497,CN= e-Szigno SMIME CA 2023	45A0C311E31DAD443AF1F714A32CF353DA1225CA0780C172567210FFB9FB14A7	ETSI EN 319 411-1 V1.4.1, LCP
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 V1.4.1, 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 V1.4.1, 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
2023-09-14	eqsmimeca2023	Sub CA	ECC / NIST P-256 (256 bits)	e-Szigno Qualified SMIME CA 2023	pub: 04:42:51:a3:df:35:cd:54:e3:07:a0:54:63:87:59: 5a:25:d2:2a:3b:cb:f3:f0:04:43:74:7c:bf:de:fc: 35:b4:6d:59:9b:56:0e:91:00:e6:9b:50:72:71:f0: 29:d8:79:fc:27:0d:21:25:8c:1e:1d:91:68:35:98: c0:be:4d:99:74 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:	<div>European Standards:<ul style="list-style-type: none">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)</div> <div>CA Browser Forum Requirements:<ul style="list-style-type: none">EV Guidelines for TLS Server Certificates, version 2.0.1Baseline Requirements for TLS Server Certificates, version 2.0.8</div> <div>For the Trust Service Provider Conformity Assessment:<ul style="list-style-type: none">ETSI EN 319 403-1 V2.3.1 (2020-06)</div>
-----------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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

- e-Szignó Certification Authority, Unified Certificate Policies, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
- e-Szignó Certification Authority, Unified Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
- 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
- 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
- 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
- e-Szignó Certification Authority, eIDAS conform Qualified Certificates for Website Authentication Certificate Policy, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
- e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Website Authentication Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
- e-Szignó Certification Authority, eIDAS conform Qualified 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.

There were no non-conformity 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 V1.4.1, LCP, NCP, OVCP, DVCP, IVCP, EVCP ETSI EN 319 411-2 V2.5.1, QEVCP-w, QCP-w-psd2

Table 7: Root-CA 3 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 V1.4.1, 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	076B30115E430F7C58EBBC1B79ECCE567704D9AA3DA15F5060855A880E237155	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	6F265CCE1F350817ED888C9A07CE8D117E6647090894971C405C0D72EC959D5C	ETSI EN 319 411-1 V1.4.1, LCP, OVCP, IVCP

Table 8: Sub-CA's issued by the Root-CA 3 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:	<div>European Standards:<ul style="list-style-type: none">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)</div> <div>CA Browser Forum Requirements:<ul style="list-style-type: none">EV Guidelines for TLS Server Certificates, version 2.0.1Baseline Requirements for TLS Server Certificates, version 2.0.8</div> <div>For the Trust Service Provider Conformity Assessment:<ul style="list-style-type: none">ETSI EN 319 403-1 V2.3.1 (2020-06)</div>
-----------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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

- e-Szignó Certification Authority, Unified Certificate Policies, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
- e-Szignó Certification Authority, Unified Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
- 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
- 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
- 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
- e-Szignó Certification Authority, eIDAS conform Qualified Certificates for Website Authentication Certificate Policy, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
- e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Website Authentication Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
- e-Szignó Certification Authority, eIDAS conform Qualified 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.

Root 5: e-Szigno SMIME 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) ETSI TS 119 411-6 V1.1.1 (2023-08) CA Browser Forum Requirements: Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.6 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 Non-Qualified Certificate for Electronic Signature Certificate Policies, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
4. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Signature Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
5. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Signature Disclosure Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
6. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Signature, Certificate Policies, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
7. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Signature Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
8. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Signature Disclosure Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
9. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Seal Certificate Policies, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
10. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Seal Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
11. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Seal Disclosure Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
12. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Seal Certificate Policies, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01

13. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Seal Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
14. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Seal Disclosure Statement, version 3.14 as of 2024-08-27, Date of effect: 2024-09-01
15. e-Szignó Certification Authority, Non eIDAS covered Certificate, Certificate Policies, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
16. e-Szignó Certification Authority, Non eIDAS covered Certificates Certification Practice 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.

There were no non-conformity 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., CN= e-Szigno SMIME Root CA 2024	7A422EC237B4DA7D326C232278F6DBE329B0C9ED5A56AAFCC110A8BC83ED0A96	ETSI EN 319 411-1 V1.4.1, LCP, NCP, NCP+ ETSI EN 319 411-2 V2.4.1, QCP-I, QCP-I-qscd, QCP-n, QCP-n-qscd

Table 13: Root-CA 5 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 SMIME CA 2023	BD042314382B35B39FEF05E417E0801001596536D35651F1013A5158AAD41560	ETSI EN 319 411-1 V1.4.1, LCP, NCP, NCP+ ETSI EN 319 411-2 V2.4.1, QCP-I, QCP-I-qscd, QCP-n, QCP-n-qscd
C=HU, L=Budapest, O=Microsec Ltd., 2.5.4.97=VATHU-23584497, CN= e-Szigno SMIME CA 2023	1215546B2B1D0A60EA0FE6F6389566E0AD69CE38D9EF41EC15395828D2F8FD6C	ETSI EN 319 411-1 V1.4.1, LCP

Table 14: Sub-CA's issued by the Root-CA 5 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	esmimerootca2024	root CA	ECC / NIST P-384	e-Szigno SMIME Root CA 2024	pub: 04:ff:69:88:8a:7a:95:43:81:86:75:dc:88:a6:d6:06: af:9a:46:c7:49:02:20:99:86:0d:0b:12:ca:19:88:bc: 51:11:3d:7e:e8:24:90:f5:aa:46:d1:4e:c0:7f:0a:59: 93:0b:da:8b:4b:3e:87:85:39:d6:66:ab:8c:73:de:02: 50:ad:33:c9:8a:e1:f5:db:49:e6:5b:85:a1:6a:87:2c: 83:a8:fe:c9:96:a3:f8:af:29:8a:f8:48:e5:76:26:d1:e3 ASN1 OID: secp384r1 NIST CURVE: P-384

Table 15: Key generation related to e-Szigno SMIME Root CA 2024

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

Root 6: e-Szigno CodeSigning 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 the Issuance and Management of Publicly-Trusted Code Signing Certificates, version 3.9.0 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, Non eIDAS covered Certificate, Certificate Policies, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
- 4. e-Szignó Certification Authority, Non eIDAS covered Certificates Certification Practice 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.

There were no non-conformity 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., CN= e-Szigno CodeSigning Root CA 2024	5AF98353650C2AC49961F51883600AE5C61101035CDD7782822322127FACEC6D	ETSI EN 319 411-1 V1.4.1, LCP

Table 16: Root-CA 6 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= e-Szigno CodeSigning CA 2024	EAB8DA8EC9C4B3454CEE24E59243750B62E433D12A8807674C25E270F0B74268	ETSI EN 319 411-1 V1.4.1, LCP

Table 17: Sub-CA's issued by the Root-CA 6 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	csrootca2024	root CA	RSA 4096	e-Szigno CodeSigning Root CA 2024	Public-Key: (4096 bit) Modulus: 00:c3:b1:0f:45:f9:f8:b5:88:66:32:a3:15:0d:4e:dd: 94:2c:8b:d7:51:19:a0:9e:f1:ec:ed:ce:28:a9:37:54: b8:73:84:ba:f9:f9:cf:42:ce:36:e5:55:ec:0a:90:1b: 6c:3c:ef:79:06:f5:63:d5:a3:e4:1e:1a:22:61:42:41: b4:32:7e:20:c1:84:f0:7b:3e:67:7b:19:96:13:fb:eb: c5:d8:3f:58:b8:e1:72:ff:69:7d:33:3d:e2:50:37:48: 52:f4:73:77:a7:ce:b6:52:32:ab:d6:83:f9:e7:6c:9d: bb:7f:bd:87:37:ba:8c:01:37:1b:58:7b:14:36:a9:01: 61:72:4c:18:e2:d7:cc:77:4f:7d:a9:da:5f:07:98:34: df:f0:a0:f6:4c:66:73:76:13:e7:f6:83:ba:f9:aa:65: 86:86:a4:4f:3e:87:e0:ee:e5:33:d0:a6:7e:9d:b8:d1: fc:77:a1:d0:6f:8f:bd:53:12:9f:4d:21:2e:65:25:bb: 67:5a:78:72:ac:5f:e0:10:b9:dd:b5:ba:fc:c0:5f:c6: 7f:7e:33:10:f3:fe:68:bc:0e:63:4f:a3:36:e8:fd:23: 99:3d:c6:3a:65:95:b7:e8:6c:ce:fd:7a:df:e6:48:99: 7d:55:52:99:5a:a5:d4:57:0f:17:00:cd:55:78:84:df: fa:20:5a:1c:57:d2:29:88:5a:c1:a6:37:36:64:72:28: a2:5e:62:7e:00:e2:d4:2e:da:87:77:b0:cd:c5:e5:b7: 6b:eb:40:05:ab:96:6a:6e:07:aa:0c:eb:a1:17:dc:29: a9:b7:0c:30:f8:27:ee:25:ec:51:d8:d2:b2:1d:bd:ee: c5:d6:df:3c:c0:53:c9:7c:4b:36:3d:1a:16:36:86:d8: 6c:ec:50:70:83:f5:12:ae:b1:1d:35:88:45:0c:36:fd: d3:a2:be:9e:17:e6:c6:88:31:c2:98:82:4d:88:7b:93: a3:56:15:4f:eb:51:69:cf:2c:2b:89:42:48:f2:70:78: 4f:4a:d8:a5:28:21:9d:32:63:17:82:08:90:16:8e:2e: 0c:05:f4:3a:00:5f:14:1a:cc:fd:f1:80:7c:cf:2b:74: 45:3e:38:c5:63:ad:3b:29:6f:a1:71:71:c8:e7:39:db: 31:c0:f9:72:08:54:8e:94:cf:0f:85:53:c1:77:73:45: 4a:6b:83:93:b2:83:4e:ce:8b:ad:75:42:7f:0c:b6:ac: 33:5d:53:9b:ed:8d:0e:95:c0:af:12:55:65:4f:3a:9c: fc:67:3d:c2:9e:44:34:95:03:44:3f:4d:fe:ea:10:18: 15:15:23:92:a7:71:b3:64:64:12:d2:0c:4f:bd:42:56:c3 Exponent: 65537 (0x10001)

Key generation date	Key identifier (short name)	Key usage	Key type and parameters	CA name	Public key
2024-07-17	cscs2024	Subordinate CA	RSA 4096	e-Szigno CodeSigning CA 2024	Public-Key: (4096 bit) Modulus: 00:e6:c7:2e:99:df:de:49:b0:b7:62:57:63:43:f2:4d: 4d:64:40:42:3f:a2:90:21:65:bf:6a:3b:d9:66:48:7d: 7a:62:15:50:98:d0:04:34:5f:54:73:f7:dc:f8:db:9d: a0:7d:cb:32:52:ba:5f:71:71:0e:20:c0:fb:d9:55:7c: ea:a7:69:98:95:33:24:9a:e4:a6:ee:96:3a:10:91:23: a4:72:95:9c:52:3d:eb:0e:24:9c:2b:84:d9:72:47:9b: e4:e1:a9:cc:61:c7:ef:f5:51:32:9f:84:6d:dc:e7:1c: 18:b1:17:bd:d3:f6:3d:ed:e5:10:18:98:0c:01:f6:7b: 43:5f:95:c6:85:c9:52:bb:0d:07:05:14:02:5c:4f:be: 7e:e1:ea:a7:00:41:75:3c:47:b6:c5:27:20:f1:c8:be: c7:a6:3f:7c:d0:f2:19:ca:e3:56:5e:be:db:a1:9c:ad: 05:cc:e1:f3:2e:16:e1:11:b5:c1:a0:ed:76:8b:81:fe: f8:ac:d3:ad:bc:5f:50:67:84:ad:b2:32:0f:a0:10:5e: bf:99:a0:7a:4a:51:47:79:5c:d5:eb:9f:76:15:a5:a8: 54:70:5a:c7:6a:e8:d2:ee:86:4b:35:2e:28:b4:96:37: 01:2e:29:c8:87:cb:2d:d8:e2:d1:95:9d:d1:f4:b1:e7: 41:5a:11:70:13:0e:f1:a9:bb:f9:c4:fa:0f:8f:bd:c0: 03:e9:f0:2c:f4:14:d5:d9:fc:cd:97:0c:dc:fa:3b:20: ab:52:b9:cb:50:07:16:f4:d1:d0:fb:14:4c:cc:04:9b: 52:f4:73:49:ac:9c:8c:3b:e8:00:a3:93:4d:ef:f1:7f: 63:10:ab:4d:9c:c4:e2:21:5d:f5:42:e8:6c:f8:fb:e6: 30:7f:df:37:e2:a9:c1:c7:9b:18:09:9a:f1:89:86:4d: 0f:4e:f0:a4:f3:29:c2:d5:24:73:8a:35:cc:42:06:1d: a3:2c:49:64:86:b9:f5:f2:af:4b:95:55:ff:f2:1b:ec: 9a:cb:27:ab:d5:0c:71:bb:fd:1b:58:5c:e1:ae:5a:fc: 3f:3b:10:69:c0:13:16:cb:72:6b:13:ff:76:0d:ea:f7: 5c:38:95:26:e7:cc:7f:9c:ee:0d:3b:83:7d:06:85:68: 5e:f2:a5:e5:07:34:9e:a4:f8:6b:71:7e:d3:fc:7e:dd: 28:6e:b5:8e:df:22:03:bd:cb:ab:34:9b:40:b2:3f:1e: d4:5b:dc:33:21:60:7d:3f:65:12:19:05:bd:70:75:d3: 5b:05:b7:bd:2f:5c:72:7c:59:1d:a8:99:3f:a7:d5: c7:01:2e:8a:0f:1f:6e:45:5f:bf:98:03:49:07:9f:3e:85 Exponent: 65537 (0x10001)

Table 18: Key generation related to e-Szigno CodeSigning Root CA 2024

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

Root 7: e-Szigno ECC TSA 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 the Issuance and Management of Publicly-Trusted Code Signing Certificates, version 3.9.0 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 Non-Qualified Certificate for Electronic Seal Certificate Policies, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
4. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Seal Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
5. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Seal 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.

There were no non-conformity 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., CN= e-Szigno ECC TSA Root CA 2024	814934F610FBF7B8579DCA297D3EBB3F667F4958E18CDCA75848DE0E4C9CCF7F	ETSI EN 319 411-1 V1.4.1, LCP

Table 19: Root-CA 7 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=e-Szigno ECC CodeSigning TSA CA 2024	25781E35E0B7D05C93F4AA5F20C2C6E84060D600BF66606362C5E064F169ED08	ETSI EN 319 411-1 V1.4.1, LCP

Table 20: Sub-CA's issued by the Root-CA 7 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	etsarootca2024	root CA	ECC / NIST P-384	e-Szigno ECC TSA Root CA 2024	pub: 04:5e:13:3a:3e:d2:a1:26:18:cd:11:6b:d2:9c:72:b6: f2:fd:74:c2:da:34:52:c3:fb:cd:6c:af:33:6e:f9:29: 0c:0c:50:76:91:07:98:80:0c:15:65:9c:e4:ba:09:8c: cd:42:ce:5f:4a:b1:91:2d:03:82:e6:f0:ca:97:cb:b2: 39:ab:47:82:40:29:34:40:b4:90:2d:aa:7e:6b:3a:92: df:81:cd:07:67:0e:24:87:cb:4f:91:68:d5:ab:52:a2:d3 ASN1 OID: secp384r1 NIST CURVE: P-384
2024-07-17	ecstsaca2024	Subordinate CA	ECC / NIST P-384	e-Szigno ECC CodeSigning TSA CA 2024	pub: 04:27:f1:c6:3d:16:ec:41:1c:20:aa:d4:94:23:19:87: e5:6e:6d:fb:ba:d9:4a:57:18:25:76:b0:cf:db:8c:88: 66:d2:22:3e:6a:af:cc:09:ae:7d:73:c4:9d:13:bb:76: e7:23:45:19:82:84:9d:c0:66:5f:5a:14:71:8a:a6:52: c0:d3:ce:6e:28:c5:fc:58:e8:88:52:5c:e9:b2:ca:6f: 2e:b2:65:ca:43:22:1d:08:44:b6:3f:07:f0:81:7c:b2:2f ASN1 OID: secp384r1 NIST CURVE: P-384

Table 21: Key generation related to e-Szigno ECC TSA Root CA 2024

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

Root 8: e-Szigno TSA Root CA 2024

Standards considered:	<p>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)</p> <p>CA Browser Forum Requirements: Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, version 3.9.0</p> <p>For the Trust Service Provider Conformity Assessment: ETSI EN 319 403-1 V2.3.1 (2020-06)</p>
-----------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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 Non-Qualified Certificate for Electronic Seal Certificate Policies, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
4. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Seal Certification Practice Statement, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
5. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Seal 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.

There were no non-conformity 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., CN= e-Szigno TSA Root CA 2024	3D4FB84E009C3A6EDC4389DFE9BE9A22391DBD9A BA19417D0D2A9BA102F0BCC8	ETSI EN 319 411-1 V1.4.1, LCP

Table 22: Root-CA 8 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.

Distinguish ed Name	SHA-256 fingerprint	Applie d policy
C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno CodeSigning TSA CA 2024	5C8F9D101C35CF42CF01C74E1E6AA665188FE1C5E7BDED02D6A67E1 938D207A6	ETSI EN 319 411-1 V1.4.1, LCP

Table 23: Sub-CA’s issued by the Root-CA 8 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	tsarootca 2024	root CA	RSA 4096	e-Szigno TSA Root CA 2024	Public-Key: (4096 bit) Modulus: 00:b9:ae:f3:2f:2e:7d:85:f3:a7:00:2a:49:f9:90:4e: 1a:de:d9:2a:71:04:ee:52:8f:2d:f7:26:3d:d4:91:cb: f6:77:9b:c3:b0:15:0a:df:5f:1c:4a:81:3d:9e:19:6d: ef:84:53:40:cf:b3:ad:3f:77:80:82:09:65:b3:44:bd: 34:3e:20:28:f4:67:2a:8e:f7:8f:af:15:db:de:2d:01: 45:ab:66:7e:86:34:07:bb:d1:5f:4b:9c:1e:67:6f:fd: b9:27:18:c6:a7:46:c0:cf:ed:c1:e7:83:25:e8:a0:9d: be:fc:54:21:61:b6:07:0e:a3:ef:23:08:d4:69:b3:86: cb:bd:f3:9b:fc:1f:32:0b:4a:25:66:64:3e:e5:34:5f: 27:b8:ca:e8:0d:37:ea:a9:31:f5:fd:b2:7d:ff:08:15: f9:8c:57:de:8e:ae:58:07:2c:3a:99:83:02:15:db:a0: 4e:16:60:5b:06:39:fc:24:58:a3:d6:eb:99:6f:da:7a: c4:75:d5:94:07:a0:29:16:c9:3e:6e:8d:e5:71:0d:11: 98:e6:dd:b1:58:78:de:c1:42:8b:c6:0e:5e:4a:d6:85: 6e:08:8f:b0:77:c4:39:45:1a:79:34:c4:9c:6d:c9:6d: 18:80:fd:8b:29:2e:15:31:ad:be:45:3e:ba:40:07:bf: a9:13:86:f0:b6:c4:f5:5e:f8:f9:6d:b1:42:18:64:9e: a8:23:55:20:f8:72:04:52:f3:be:15:c0:9e:2b:68:36: fb:17:36:e9:91:37:22:06:bb:ab:e8:2f:53:fb:cf:b4: 09:9b:9b:fd:7d:7f:5b:1a:c1:23:9c:2c:52:fe:63:18: 29:80:f3:9f:0c:01:ad:27:7e:f8:e0:32:4e:75:bc:bf: 0b:35:10:17:57:1d:15:e8:33:2a:6e:47:bb:9d:b8:b3: 68:03:5f:bf:70:bf:22:b9:07:da:7e:70:78:59:66:4d: 63:a2:1c:11:e0:47:f3:9e:9a:e4:56:50:5d:a6:04:ce: 94:85:5c:ba:87:27:bb:62:f6:a7:54:82:d1:1b:7e:59: 7b:60:70:da:80:f7:19:20:cc:47:42:42:f1:cb:8d:2c: 34:d4:41:66:a0:8b:49:ce:dc:55:f0:d5:c1:5f:34:aa: c2:df:ea:27:3a:2b:c6:a0:32:e5:c2:1f:af:2b:dc:cd: 3c:fd:63:c5:9e:9a:03:42:95:77:94:15:41:00:c0:12:

					2e:82:32:be:63:7d:ef:2d:54:cb:b8:de :e7:a4:a4:fd: 4e:d1:70:82:51:77:cb:f8:d5:eb:03:3b :d5:94:55:8a: fe:3a:4b:54:8a:ee:ed:3d:c4:19:83:58 :a5:79:94:f3:ef Exponent: 65537 (0x10001)
2024-07-17	cstsaca2024	Subordinate CA	RSA 4096	e-Szigno CodeSigning TSA CA 2024	Public-Key: (4096 bit) Modulus: 00:da:9d:d9:2f:c3:cb:a6:60:93:65:bf :44:4e:57:a0: db:3d:2e:f2:58:52:d8:1b:a9:89:d3:a2 :3a:65:c9:14: 9b:1b:52:65:e8:0a:e5:b8:8e:9c:e1:42 :ce:9c:4c:af: 1e:e1:d7:c3:9b:e0:53:3f:5e:17:6d:81 :91:7e:33:a7: 3c:c0:ab:a5:24:e2:6c:36:9b:23:3b:9f :b9:2b:87:c2: 6f:30:65:b8:00:19:23:89:2f:9c:3d:9f :ef:bf:d2:5c: 3a:84:9b:52:ec:09:37:e4:94:8b:24:b9 :df:97:b7:ea: 03:b0:93:8c:c6:11:c0:8f:d8:3c:aa:d9 :2b:0f:c4:84: d3:47:76:b3:1a:66:2b:3e:1d:78:c7:3d :9a:4b:c9:53: 69:dd:3c:77:a6:ed:fc:10:14:74:6e:7a :db:ff:d3:2b: 9f:b0:1c:e7:d5:89:48:31:87:c8:65:2a :83:c4:b8:0b: 5d:44:29:16:cd:a3:f1:91:16:48:75:ce :b8:69:bb:38: ec:ff:b2:77:bd:3e:a0:84:6a:5b:e7:bb :f5:fc:03:98: 3c:c8:73:e8:ab:9a:2a:c3:58:7b:8f:89 :a4:78:86:b5: 3d:7c:2a:94:fe:22:37:4c:99:cd:3a:f0 :dc:56:3d:85: 18:78:80:50:ec:e6:1c:e4:a8:98:6d:21 :c5:c3:91:75: 43:08:14:89:bb:52:a1:6f:7f:7f:a5:03 :8c:ff:ab:e9: c7:12:e9:e6:9f:9e:0c:e8:a1:14:42:88 :bf:09:09:18: b9:ae:52:55:60:64:ed:67:31:a9:19:fa :13:86:82:7c: 8d:bb:a4:3b:95:23:63:a5:5a:5c:98:66 :d1:45:c0:b0: 1c:fe:8d:05:13:e8:d9:65:00:e3:aa:a7 :b8:4b:6b:58: cd:d9:93:52:68:13:4f:90:14:7a:a5:e2 :2e:60:de:93: 97:fc:18:86:c9:4f:e6:a1:cd:10:e8:ac :33:2d:43:b5: cd:0a:4d:0e:86:23:76:95:a8:e9:5d:50 :99:b1:bd:fe: d4:e2:0b:54:62:d9:35:89:ac:7b:ad:31 :f5:b6:5a:ab: b7:de:cc:d2:d1:9c:cb:df:cb:29:10:e7 :bb:0b:3a:86: ed:a8:c5:e2:4f:bf:ad:cd:15:39:d9:77 :6e:f7:a3:54: d2:95:c3:fc:38:f6:09:37:63:b4:47:ad :9d:8e:60:68: 65:97:0e:4c:7a:f0:b5:49:c2:5f:78:c4 :63:15:e6:10:

					47:eb:e5:cd:fb:e7:69:18:14:3b:65:aa :41:b6:51:60: fa:c5:5c:5c:cc:08:a1:83:6c:36:19:73 :ba:e5:7f:e7: 92:6e:5e:db:fa:c0:0c:7b:dd:b5:54:bb :a0:bc:63:0d:eb Exponent: 65537 (0x10001)

Table 24: Key generation related to e-Szigno TSA Root CA 2024

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

Timestamping Service for CodeSigning

Standards considered:	European Standards: ETSI EN 319 411-1 V1.4.1 (2023-10) ETSI EN 319 401 V3.1.1 (2024-06) ETSI EN 319 421 V1.2.1 (2023-05) CA Browser Forum Requirements: Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, version 3.9.0 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, eIDAS conform Non-Qualified Time Stamping Service, Time Stamping Policy, version: 3.14 as of 2024-08-27, Date of effect: 2024-09-01
- 2. e-Szignó Certification Authority, eIDAS conform Non-Qualified Time Stamping Service - Practice 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.

There were no non-conformity during the audit.

To the best of our knowledge, no incidents have occurred within this service during the audited period.

Key generation date	Key identifier (short name)	Key usage	Key type and parameters	TSU name	Public key
2024-01-15	ecstsa202401	TSU key	ECC NIST P-256	e-Szigno CodeSigning TSA 2024 01	Subject Public Key Info: Public Key Algorithm: id-ecPublicKey Public-Key: (256 bit) pub: 04:0a:29:d5:ce:42:ed:f6:1b:87:8c:ad:88:ae:9f: 5c:bf:37:b1:dd:35:70:dd:42:6f:80:b6:93:0d:83: 22:2f:29:1f:49:99:87:92:66:b9:a7:3b:a3:26:6d: 5b:9f:a9:ec:09:27:09:2c:5a:74:13:34:07:ec:21: d6:14:d2:51:5b ASN1 OID: prime256v1 NIST CURVE: P-256 Attributes: a0:00
2024-08-08	ecstsa202402	TSU key	ECC NIST P-256	e-Szigno ECC CodeSigning TSA 2024 02	Subject Public Key Info: Public Key Algorithm: id-ecPublicKey Public-Key: (256 bit) pub: 04:44:42:d9:63:df:fa:70:c3:08:ce:3e:97:b9:19: 46:e2:d9:90:8a:9c:0d:b8:7a:ff:01:2d:5b:6e:26: 10:fb:80:ff:d9:e8:3f:d6:5c:f8:86:f8:a5:1d:53: f8:34:71:54:40:15:77:b6:0a:b4:91:dd:6e:7c:5c: da:54:26:e3:59 ASN1 OID: prime256v1 NIST CURVE: P-256 Attributes: a0:00

Key generation date	Key identifier (short name)	Key usage	Key type and parameters	TSU name	Public key
2024-08-08	cstsa202401	TSU key	RSA 3072	e-Szigno RSA CodeSigning TSA 2024 01	Public Key Algorithm: rsaEncryption RSA Public-Key: (3072 bit) Modulus: 00:9a:31:ae:a1:a5:f9:a3:87:51:69:8f:45:5e:da: 79:e6:bf:3b:ad:d5:de:99:f7:3d:dc:b4:11:ed:b7: cf:06:9c:8c:96:c1:b3:a6:7e:b3:03:96:ea:1f:97: 7e:f5:f6:19:c9:92:fd:07:df:ce:72:4d:34:7c:60: 01:35:14:06:73:f8:10:46:c2:73:44:f5:73:26:a4: db:f0:cd:23:5e:8e:96:a0:6e:55:7c:49:30:4c:21: 4c:a3:8d:32:5e:7c:14:3e:32:21:03:a0:a9:a6:78: 0c:0b:2c:1b:5a:ba:5a:7e:68:b6:cb:2f:7a:ba:ac: 9e:02:e2:33:1a:1a:36:83:f0:e1:57:c0:8c:cd:d5: bf:a9:54:66:ca:ca:64:54:47:9d:98:c5:d2:78:80: 46:24:12:45:bc:33:66:fe:95:1b:96:a0:c7:17:08: 5a:d1:65:26:9a:36:8a:9a:66:94:5d:aa:4b:fe:60: e3:d0:5c:a0:85:fd:6c:c0:60:12:51:a1:80:84:6a: 35:17:39:ab:96:31:51:0f:48:af:95:b7:f7:fb:75: 2d:4f:21:4b:b8:7c:95:ae:a9:50:64:d8:ee:9a:9b: 61:15:98:45:48:8d:45:88:e6:ba:5d:70:4d:eb:cf: 4a:96:8e:ff:95:3b:5e:e1:e5:5b:05:30:4b:2d:50: 01:0a:9c:65:33:da:c1:8b:33:5a:ea:c2:35:e4:1c: 94:60:40:a6:21:e4:a9:3c:b5:25:b7:7a:40:20:ee: 63:05:de:ff:b4:f5:64:de:0e:11:17:62:df:ba:af: 91:6c:c4:05:20:30:1d:e1:2b:6a:ff:e2:f5:cd:52: 26:37:35:5b:6d:a7:49:34:b4:37:a3:1b:dc:2b:79: 4d:c6:8c:bb:dd:6e:7d:34:5b:72:b6:e6:62:1b:01: 07:06:49:a1:b8:8a:f4:03:48:60:0e:80:e1:d5:f7: 87:1d:2c:e2:81:1e:1d:ad:e0:d4:c1:3f:7b:30:2b: 9c:3a:24:af:7f:7b:00:c2:28:91 Exponent: 65537 (0x10001)

Table 25: Key generation related to timestamping service

Key generation date	Key destruction date	Key identifier (short name)	Key usage	Key type and parameters	TSU name
2022-12-20	2024-09-20	ecstsa202301	TSU key	ECC NIST P-256	e-Szigno CodeSigning TSA 2023 01

Table 26: Key destruction to timestamping service

Signing Service for CodeSigning

Standards considered:	<p>European Standards: ETSI EN 319 411-1 V1.4.1 (2023-10) ETSI EN 319 401 V3.1.1 (2024-06) ETSI TS 119-431-1 V1.2.1 (2021-05)</p> <p>CA Browser Forum Requirements: Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, version 3.9.0</p> <p>For the Trust Service Provider Conformity Assessment: ETSI EN 319 403-1 V2.3.1 (2020-06)</p>
-----------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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

1. e-Szignó Certification Authority, eIDAS conform Remote Key Management Service suitable for Creating Electronic Signatures/Seals - Practice 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.

There were no non-conformity during the audit.

To the best of our knowledge, no incidents have occurred within this service during the audited period.

There was no key generation in the period under review.

There was no 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

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
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.