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

HUNGUARD

Key Generation Ceremony Report for

Microsec Micro Software Engineering & Consulting

Private Limited Company by Shares

as a Qualified Trusted Service Provider

Reference: HUNG-KG-001-TLSROOT-2025

“Budapest, 1 August, 2025”

To whom it may concern,

This is to confirm that “HUNGUARD Kft.” has audited a key generation ceremony of “Microsec Micro Software Engineering & Consulting Private Limited Company by Shares”. The ceremony was followed in its entirety, completed successfully and without non-conformities in accordance with the applicable requirements.

This Key Generation Ceremony Report is registered under the unique identifier number “HUNG-KG-001-TLSROOT-2025” and consists of 9 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

HUNGUARD Kft.,
6 Kékgolyó Street,
1123 Budapest, Hungary
Tel: +36 1 792 0880; Fax: +36 1 445 0414
e-mail: iroda@hunguard.hu

With best regards,

Digitally signed:
HUNGUARD

Zsolt Attila Endrődi reviewer	*Tibor Németvári* 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: 1
- 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;
  d) technical knowledge of the activity to be audited;

[1] https://nah.gov.hu/admin/staticmedia/Reszletezo_okiratok/Rugalmas_terulet_nyilvantartas/RT-NAH-6-0048-2023-B1_BNN_a.pdf

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 of key and certificate generation ceremony
Point in time date:	2025-07-30
Audit location:	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

A key generation script has been prepared in accordance with the normative requirements and with the rules stated in the policy and practice statement documents of the certification service provider. During generation of the keys and certificates, this script has been followed.

In particular:

- The key generation ceremony was performed by 2 individuals of the CA Owner acting in Trusted Roles
- The key generation ceremony was observed by 1 individual of the Conformity Assessment Body with independence from the CA Owner
- Principles of multiparty control and split knowledge were observed.
- The CA key pairs were generated in a physically secured environment as described in the CA’s [CP / CPS].
- The CA key pairs were generated within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA’s [CP / CPS].
- CA key pair generation activities were logged.
- Effective controls were maintained to provide reasonable assurance that the private key was generated and protected in conformance with the procedures described in its [CP / CPS] and the Key Generation Script.

The key generation ceremony has been witnessed in person.

No non-conformities have been identified during the audit.

Root 1: e-Szigno RSA TLS Root CA 2025

Standards considered: (Only with regard to key generation and key protection requirements)	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 V3.3.1 (2024-06) CA Browser Forum Requirements: • Guidelines for the Issuance and Management of Extended Validation Certificates, version 2.0.1 • Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, version 2.1.5 • Network and Certificate System Security Requirements, version 2.0.5 Browser Policy Requirements: • CCADB Policy version 2.0, July 15, 2025 • Apple Root Certificate Program, August 15, 2023 • Chrome Root Program Policy, Version 1.7, 2025-07-15 • Program Requirements – Microsoft Trusted Root Program, 10/28/2024 • Mozilla Root Store Policy Version 3.0, March 15, 2025 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:

- e-Szignó Certification Authority, Unified Certificate Policies, version: 3.16 as of 2025-05-20, Date of effect: 2025-05-20
- e-Szignó Certification Authority, Unified Certification Practice Statement, version: 3.16 as of 2025-05-20, Date of effect: 2025-05-20
- e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Certificate Policies, version: 3.15 as of 2025-03-12, Date of effect: 2025-03-12
- e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Certification Practice Statement, version: 3.15 as of 2025-03-12, Date of effect: 2025-03-12
- e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Disclosure Statement, version: 3.15 as of 2025-03-12, Date of effect: 2025-03-12
- e-Szignó Certification Authority, eIDAS conform Certificates for Website Authentication Certificate Policy & Certification Practice Statement, version: 3.15.1 as of 2025-05-15, Date of effect: 2025-05-15

This report covers the generation of the key pairs and certificates of the Root-CA and Sub-CAs referenced in the following tables.

This report covers the generation of the key pair and certificate of the Root-CA referenced in the following table. No Sub-CAs were generated during the ceremony.

Distinguished Name	SHA-256 fingerprint of the certificate	Applied policy

C = HU
L = Budapest
O = Microsec Ltd.
CN = e-Szigno RSA TLS Root CA 2025
	SHA-256 fingerprint of the certificate:
	
	A01C4F8F68112FA9DAC50B96809A791480168C8ACB9E51C5482D8D3819688557
		ETSI EN 319 411-1 V1.4.1
		LCP, NCP, OVCP, DVCP, EVCP
		ETSI EN 319 411-2 V2.5.1
		QEVCP-w, QCP-w-psd2

	SHA-256 fingerprint of Subject Public Key Info	
	SHA-256 fingerprint of the subject public key info: 9EEF0C66D1D20340E4E504701D3B872B598A65ED7D59826D59E65C5EDD2B921B	

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 of the certificate	Applied policy
	SHA-256 fingerprint of Subject Public Key Info	

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

Key pairs generated without issuance of a corresponding certificate

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 V3.3.1 (2024-06) CA Browser Forum Requirements: • Guidelines for the Issuance and Management of Extended Validation Certificates, version 2.0.1 • Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, version 2.1.5 • Network and Certificate System Security Requirements, version 2.0.5 Browser Policy Requirements: • CCADB Policy version 2.0, July 15, 2025 • Apple Root Certificate Program, August 15, 2023 • Chrome Root Program Policy, Version 1.7, 2025-07-15 • Program Requirements – Microsoft Trusted Root Program, 10/28/2024 • Mozilla Root Store Policy Version 3.0, March 15, 2025 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:

- e-Szignó Certification Authority, eIDAS conform Certificates for Website Authentication Certificate Policy & Certification Practice Statement, version: 3.15.1 as of 2025-05-15, Date of effect: 2025-05-15

This report covers the generation of the private keys referenced in the following table(s). For these keys, no certificates were generated during the ceremony.

Key #	**Subject Public Key Info Field Hash (SHA-256)**

Table 3: Key pairs generated without issuance of a corresponding certificate

Modifications record

Version	Issuing Date	Changes
Version 1	2025-07-31	Initial attestation
Version 1.1	2025-08-01	1st amended version: formal correction by Hunguard

End of the audit attestation letter.