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

Audit Report Summary

for

Microsec V2X PKI service

Reference: HUNG-AA-011-2025

"Budapest, 10 April, 2025"

To whom it may concern,

This is to confirm that "HUNGUARD Ltd." has audited the Microsec V2X PKI service defined by the following CPS documents:

- Microsec ltd. V2X C-ITS Root CA Certification Practice Statement
- Microsec ltd. V2X C-ITS Enrolment Authority Certification Practice Statement
- Microsec ltd. V2X C-ITS Authorisation Authority Certification Practice Statement

The conformity assessment and audit results were detailed in audit report, with document identifier number C435-13/P/E/EUCP30/2025.

The summary of the audit report and the main findings are contained in this present Audit Report Summary.

This present Audit Report Summary is registered under the unique identifier number HUNG-AA-011-2025.

This Audit Report summary consists of 6 pages.

In case of any questions, please contact:

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

Digitally signed:
Endrődi Zsolt Attila

Zsolt Attila Endrődi
Audit Quality Manager

Digitally signed:
Németvári Tibor

Tibor Németvári
Lead Auditor

Digitally signed:
HUNGUARD

General audit information

Identification of the conformity assessment body (CAB) and assessment organization acting as auditor
• HUNGUARD Informatics and IT R&D and General Service Provider Ltd., • Seat address: 6 Kékgolyó Street, Budapest, 1123 Hungary • Company registration number: 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)". • Accredited by National Accreditation Authority (Hungary) under registration NAH-1-1578/2021[2] for the certification of Systems implementing V2X PKI service according to Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) EU C-ITS Certificate Policy • 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 (CAB) 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. In addition, all team members are trained to demonstrate adequate competence in: a) knowledge of the C-ITS standards and other relevant publicly available policies and specifications; b) understanding functioning of V2X PKI 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/hu/szervezet/hunguard-szamitastechnikai-informatikai-kutato-fejleszto-es-altalanos-szolgaltato-kft-6dd84c89-f635-4155-8231-392b9a4d7aaf-1/

2 https://nah.gov.hu/hu/szervezet/hunguard-szamitastechnikai-informatikai-kutato-fejleszto-es-altalanos-szolgaltato-kft-ertekelesi-divizio-1/

d) technical knowledge of the activity to be audited; e) general knowledge of regulatory requirements relevant to C-ITS, CCMS; 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 for 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 CA/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 319 403-1 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 Audit Quality Managers fulfils the requirements as described for the Audit Team Members above.

Identification of the audited Service Provider (SP):	MICROSEC Micro Software Engineering & Consulting Private Limited Company by Shares (Microsec ltd.) Seat address: 13 Ángel Sanz Briz Road, Budapest,1033 Hungary Company registration number: 01-10-047218

Audit interval:	2025-02-13 to 2025-04-04
Audit dates (on site):	2025-03-19 to 2025-03-20
Audit locations:	Facility #1 (Microsec office building): 13 Ángel Sanz Briz Road, Budapest, 1033 Hungary. Facility #2 (Microsec Data Center): 7 Záhony Street, Budapest, 1031 Hungary Facility #3 (T-Systems Cloud & Data Center): 13 Asztalos Sándor Road, Budapest, 1087 Hungary
Audit methodology:	Examine (Specifications, Mechanisms, Activities) Interview (Individuals or groups of individuals) Test (Mechanisms, Activities) (based on NIST SP 800-53A Rev5 Appendix C)

Target of audit: Microsec V2X PKI service

The audit was based on the following practice statement documents of the Service Provider:

1. Microsec ltd. V2X Cooperative Intelligent Transport Systems Root CA Certification Practice Statement, version 4.0, date of effect: 2025-04-09, OID: 1.3.6.1.4.1.21528.4.1.1.1
2. Microsec ltd. V2X Cooperative Intelligent Transport Systems Enrolment Authority Certification Practice Statement, version 4.0, date of effect: 2025-04-09, OID: 1.3.6.1.4.1.21528.4.1.1.2
3. Microsec ltd. V2X Cooperative Intelligent Transport Systems Authorization Authority Certification Practice Statement, version 4.0, date of effect: 2025-04-09, OID: 1.3.6.1.4.1.21528.4.1.1.3

The audited PKI hierarchies of the Microsec V2X service are detailed on the following page.

The conformity assessment was performed against the following normative document: *Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) EU C-ITS Certificate Policy Release 3.0 May 2024*. (hereinafter: EU CP 3.0)

For general IT security compliance, the *US National Institute of Standards and Technology (NIST) Special Publication "Security and Privacy Controls for Information Systems and Organizations 800-53 revision 5"* document was used by the Audit team.

Audit results, main findings, non-compliances, deficiencies

Main findings, conformity:	Microsec V2X PKI service fully complies with the requirements of the EU CP 3.0 for the ECTL L1 PKI and ECTL L2 PKI hierarchies. For the [Non-ECTL] Autobahn Level 1-Ready PKI and [Non-ECTL] Microsec Joint PKI hierarchies, Microsec V2X PKI service meets the requirements with some deviation.
Non-compliances, deficiencies	For the [Non-ECTL] Autobahn Level 1-Ready PKI and [Non-ECTL] Microsec Joint PKI hierarchies, the Microsec V2X PKI service complies with the requirements of EU CP 3.0 listed below with some deviations, and only partial compliance can be determined: • Clause 3.1.1.1 §2 • Clause 3.2.2.4 §1 • Clause 6.1.5.2 §2 • Clause 6.1.5.2 §3 • Clause 6.1.5.2 §4 • Clause 6.1.5.2 §5 • Clause 6.1.5.2 §6 • Clause 6.1.5.2 §7 On this basis, the [Non-ECTL] Autobahn Level 1-Ready PKI and [Non-ECTL] Microsec Joint PKI hierarchies received a non-compliant rating for the above requirements. No non-compliances, deviations or observations were made for the ECTL Level 1 PKI and ECTL Level 2 PKI hierarchies.

Audited PKI hierarchies within the Microsec V2X service

ECTL Level 1 PKI

Root CA:	Name	3_Microsec-CCMS-RCA-2024_L1
	hashedId8	e9076bd01b73dade
Distribution Centre (DC):	http://microsec-ccms-dc-2024-l1.v2x-pki.com	
Enrolment Authority (EA):	Name	3_Microsec-CCMS-EA-2024_L1
	hashedId8	792849e5c59a2b00
Authorization Authority (AA):	Name	3_Microsec-CCMS-AA-2024_L1
	hashedId8	e2e843c19be5437d

ECTL Level 2 PKI

Root CA:	Name	3_Microsec-CCMS-RCA-2024_L2
	hashedId8	b1fc75cd5a80c630
Distribution Centre (DC):	http://microsec-ccms-dc-2024-l2.v2x-pki.com	
Enrolment Authority (EA):	Name	3_Microsec-CCMS-EA-2024_L2
	hashedId8	2bea96b710b1143d
Authorization Authority (AA):	Name	3_Microsec-CCMS-AA-2024_L2
	hashedId8	f69e74a0936108a1

[Non-ECTL] Autobahn Level 1-Ready PKI

Trust List Manager (TLM):	Name	Autobahn-TLM-2021_L1
	hashedId8	2283642847d00b72
CITS point of contact (CPOC):	https://autobahn-cpoc.v2x-pki.com	
Root CA:	Name	1_Autobahn-V2X-RootCA-2021-1_L1
	hashedId8	4c9abd467cf2fc0d
Distribution Centre (DC):	http://autobahn-dc2021-1-L1.v2x-pki.com	
Enrolment Authority (EA):	Name	1_Autobahn-V2X-EA-2025-1_L1
	hashedId8	c58c6ec29a65f9ee
Authorization Authority (AA):	Name	1_Autobahn-V2X-AA-2025-1_L1
	hashedId8	d6521c5732980be6

[Non-ECTL] Microsec Joint PKI

Trust List Manager (TLM):	Name	Microsec-CCMS-TLM-2024-Joint
	hashedId8	3b88b8d8f218dec5
CITS point of contact (CPOC):	https://microsec-cpoc-joint.v2x-pki.com	
Root CA:	Name	Microsec-CCMS-RCA-2024-Joint
	hashedId8	503348da43a41d72
Distribution Centre (DC):	http://microsec-ccms-dc-2024-joint.v2x-pki.com	
Enrolment Authority (EA):	Name	Microsec-CCMS-EA-2024-Joint
	hashedId8	8b9f0b12a0bf284a
Authorization Authority (AA):	Name	Microsec-CCMS-AA-2024-Joint
	hashedId8	6344f8d8da09899d

Modifications record

Version	Issuing Date	Changes
Version 1	2025-04-10	Initial version

End of the audit report summary.