ANNEX OF THE CERTIFICATION

(I-MS21T_TAN-V2X.EN)

Document ID	**I-MS21T_TAN-V2X.EN.ME-01**	
Project ID	**I-MS21T**	**Microsec ltd. V2X PKI service certification 2021.**
MATRIX director of Certification	**Ádám Molnár**	
Date of Issue	**Budaörs, 3. december, 2021**	

1. INTRODUCTION

The certification body of MATRIX Ltd. (henceforth: MATRIX) is accredited by National Accreditation Authority based on NAH-6-0054/2019/K accreditation document according to eIDAS (REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC) as an independent certification body.

Microsec ltd. is a company engaged in the development and distribution of electronic signature products, the provision of trust services and other PKI related services.

During the conformity assessment, MATRIX ltd. carried out a point-by-point evaluation of the normative documents.

2. CONFORMITY ASSESSMENT REQUIREMENTS

Normatives for the target of evaluation:

- Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) RELEASE 1.1 JUNE 2018
- COMMISSION DELEGATED REGULATION (EU) …/… of 13.3.2019 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems, C(2019) 1789 final

3. CONFORMITY ASSESSMENT TARGET

3.1. Identification of the product

The Target of Evaluation is the Microsec V2X PKI services with the following main services:

- Root CA,
- Enrolment Authority (EA),
- Authorization Authority (AA),

- Registration Authority (RA),
- Distribution Centre (DC),
- Trust List Manager (TLM),
- C-ITS point of contact (CPOC).

In V2X PKI, the main source of trust is the Root CA and the TLM. The public keys for these units are as follows:

Public keys of the units:	
Name of the unit	Public key (EC)
1_Microsec-V2X-RootCA-2021-1_L2 (Root)	Public Key: EC Public Key [aa:86:e6:06:2b:db:15:38:20:c2:d1:ce:52:3f:d0:1d:6a:dd:01:f1] X: 196eca529b2fb68b4f4545a66573b4c649044598c218a203627a88f3ae5a486f32e40d57de19bcd5daa8419795a0f12d Y: 5afee248c0141ca218aafbff90f712282cda75aa320c9fda14f4068a055ae76bba00d8b63e1416bf5a5a5c3ee335e26f
2_Microsec-V2X-RootCA-2021-2_L2 (Root)	Public Key: EC Public Key [71:f6:6a:76:72:ce:c6:7d:a7:39:75:41:9e:75:af:66:58:c5:35:a2] X: 770595d64de1d750b4f82426301f5b9f3716619397cde8b95664fb4cd71b670780c1e9c1d9806e9c640e5de56a552aba Y: 2f5850674fba7fcc8d282dafb1c775e723f1c4a3d4b96ac35eb14efcf9f81e21403ca79102e2b6925b4ba388d98285a9
1_AG-V2X-RootCA-2021-1_L2 (Root)	Public Key: EC Public Key [81:34:4e:09:4d:e7:36:a5:05:c5:53:b5:ec:36:d7:76:40:f6:67:64] X: 5cac866247ac1e86ecf7fa65a7dd02383571036e8e8725c76b19197b41da8f50dc1f801f5d7c0b13cf90a6bd49ccd489 Y: 46a3b419cf4928a79e61bd8f2687c7630d6808fc0288e6d58d6b3c24853221cdce8bc0cae58a7d211c2ec5e5a8e4f37e
1_AG-V2X-RootCA-2021-1_L1 (Root)	Public Key: EC Public Key [26:e1:27:2d:67:e3:f3:03:94:2e:37:a9:34:6f:7b:c0:0a:cc:d3:ff] X: 80a8ef7633cc97ecd9938e7e6f7281750a0fac8c9e4dafc055fd13dd42b12c969977ef40f8e6f9be77e9dd94c0956bf3 Y: 45d1916464a0bf661a2be5049d28fbf3ada18a0755c9f492e2d0f356fe8de4eb266eaee536a89f22fea4adc75fbe8035

Microsec-TLM-2021_L2 (TLM)	Public Key: EC Public Key [fa:89:db:3f:5b:a7:08:48:5b:ed:5f:c1:52:b1:d7:05:d5:76:57:e1] X: 46509254b8ee157583056c6336215b7d6fd4dbb4eb5e636bfbbba08c848092ae63f30fe53a5a85b4841c7db53c04bf7b Y: 2b0f1a690df52588f0fb0740b75fa7a97a7eb6f663f23760a3a80f4da06a15ec872ac1158721b49ed095baebf543d4cb
AG-TLM-2021_L2 (TLM)	Public Key: EC Public Key [e4:d7:5f:4e:aa:f1:96:6a:69:c0:7e:c3:d2:57:44:fd:3d:8d:31:67] X: 5db44e6c505cc775add0ddad5509a4750c72ee246273d5b7e7c90f6fb81949485ea6ea3790ad6f1fc873c4c199723b16 Y: a5a7827133bd076cea7654d38553659182ee29ca43e4ec5a8d7f1232574120baea63d4d6d83ab663c9a8a5b318c8c4b

3.2. Documentation of the TOE

Típus	Cím	OID	Dátuma
Public	General Terms and Conditions for the CCMS V2X PKI Service	1.3.6.1.4.1.21528.1.2.1.905	2021/05/14
Public	V2X Cooperative Intelligent Transport Systems ROOT CA Certification Practice Statement	1.3.6.1.4.1.21528.4.1.1.1	2021/10/25
Public	V2X Cooperative Intelligent Transport Systems Enrolment Authority Certification Practice Statement	1.3.6.1.4.1.21528.4.1.1.2	2021/10/25
Public	V2X Cooperative Intelligent Transport Systems Authorisation Authority Certification Practice Statement	1.3.6.1.4.1.21528.4.1.1.3	2021/10/25
Public	V2X Cooperative Intelligent Transport Systems - Trust List Manager Certification Practice Statement	1.3.6.1.4.1.21528.4.1.1.4	2021/10/30
Public	Minőségpolitika	1.3.6.1.4.1.21528.1.2.1.103	2019/02/20
Public	Információbiztonsági politika	1.3.6.1.4.1.21528.1.2.1.104	2019/02/20
Internal	Minőség- és információbiztonság irányítási kézikönyv	1.3.6.1.4.1.21528.1.2.1.101	2021/03/16
Internal	Szervezeti és működési szabályzat	1.3.6.1.4.1.21528.1.2.1.102	2021/11/08
Internal	V2X PKI szolgáltatás működési szabályzat	1.3.6.1.4.1.21528.1.2.1.901	2021/11/22
Internal	V2X PKI szolgáltatás rendszerterv	1.3.6.1.4.1.21528.1.2.1.902	2021/11/22
Internal	V2X PKI szolgáltatás üzletmenet-folytonossági terv	1.3.6.1.4.1.21528.1.2.1.903	2021/11/22
Internal	V2X PKI szolgáltatás rendszervizsgálati útmutató	1.3.6.1.4.1.21528.1.2.1.904	2021/05/14

Internal	V2X Cooperative Intelligent Transport Systems - Certificate Profiles	1.3.6.1.4.1.21528.4.1.1.5	2021/11/22
Internal	V2X Szolgáltatói kulcsok kezelése	1.3.6.1.4.1.21528.1.2.1.911	2021/11/22
Internal	V2X Kulcsgenerálási forgatókönyv szolgáltatói kulcspárok számára	1.3.6.1.4.1.21528.1.2.1.912	2021/11/22
Internal	V2X Kulcsmegsemmisítési forgatókönyv szolgáltatói kulcspárok számára	1.3.6.1.4.1.21528.1.2.1.913	2021/11/22
Internal	V2X Szolgáltatás leállítási terve	1.3.6.1.4.1.21528.1.2.1.914	2021/11/22
Internal	V2X Üzemeltetési és biztonsági szabályzat	1.3.6.1.4.1.21528.1.2.1.915	2021/11/22

3.3. Customer of the certification

Organization name: Microsec ltd.

Address: Hungary, H-1033 Budapest, Ángel Sanz Briz str. 13.

Company registration number: 01-10-047218

Tax number: 23584497-2-41

4. AUDIT METHODOLOGY

The conformity assessment perfomed by the audit team was the auditing method.

Auditing: Systematic, independent, documented process based on records, claims or other important informations acquisition and their objective evaluation in order to determine to what extent the requirements are met.

The objective evidencees were collected by the audit team with the following techinuques:

- Documentation evaluation
- Visual inspection
- Interviewing
- Technical review

Documentation evaluation: Policies from the organization, certificate policies and evaluation of regulatory documents.

Visual inspection: During the on-site audit, the basis of administrative security measures and physical security measures were assessed on the basis of visual inspection, in accordance with the audit process.

Interviewing: Observation persons involved in the certificate policies and in the process they have done, evaluation in targeted areas of assessment issues related to information security.

Technical review: The logical security provisions, technical configuration regulations evaluation of the IT system.

4.1. Audit time interval

Audit interval: 2021.10.25. – 2021.12.03.

4.2. Description of the changes to the audit plan

During the audit, the audit team members worked in accordance with the audit plan, so the audit did not differ from the planned schedule.

5. CONFORMITY

5.1. Conformity of the normative documents

The target of evaluation fulfills the requirements of the following normative documents:

- Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) RELEASE 1.1 JUNE 2018

- COMMISSION DELEGATED REGULATION (EU) …/… of 13.3.2019 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems, C(2019 1789 final

No further examination is required during the present certification.

6. ABBREVIATIONS

Rövidítés	Tartalom
TOE	Target of Evaluation
C-ITS	Corporate Intelligent Transportation System
OID	Object Identifier
CN	Certificate Name
V2X	Vehicle to Everything
PKI	Public Key Infrastructure
CA	Certificate Authority
EA	Enrolment Authority
AA	Authorization Authority
RA	Registration Authority
TLM	Trust List Manager
DC	Distribution Centre
CPOC	C-ITS point of contact
EC	Elliptic Curve

End of document.