Audit Attestation for

MICROSEC Micro Software Engineering & Consulting Private Limited Company by Shares

Reference: AA2018121304

Essen, 13.12.2018

To whom it may concern,

This is to confirm that “TÜV Informationstechnik GmbH” has successfully 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 “**AA2018121304**” and consist of 6 pages.

Kindly find here-below the details accordingly.

In case of any question, please contact:

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Certification Body
Langemarckstr. 20
45141 Essen, Germany
E-Mail: certuvit@tuvit.de
Phone: +49 (0) 201 / 8999-9

With best regards,

Matthias Wiedenhorst Reviewer	Péter Máté, Erdősi Leadauditor

Identification of the conformity assessment body (CAB):	TÜV Informationstechnik GmbH[1], Langemarckstraße 20, 45141 Essen, Germany registered under HRB 11687, Amtsgericht Essen, Germany Accredited by DAkkS under registration D-ZE-12022-01[2] for the certification of trust services according to "DIN EN ISO/IEC 17065:2013" and "ETSI EN 319 403 V2.2.2 (2015-08)".

Identification of the trust service provider (TSP):	MICROSEC Micro Software Engineering & Consulting Private Limited Company by Shares, Záhony utca 7, 1031 Budapest, Hungary registered under 01-10-047218.

Identification of the audited Root-CA:	e-Szigno Root CA 2017	
	Distinguished Name	CN = e-Szigno Root CA 2017 2.5.4.97 = VATHU-23584497 O = Microsec Ltd. L = Budapest C = HU
	SHA-256 fingerprint	be b0 0b 30 83 9b 9b c3 2c 32 e4 44 79 05 95 06 41 f2 64 21 b1 5e d0 89 19 8b 51 8a e2 ea 1b 99
	Certificate Serial number	00 01 54 48 ef 21 fd 97 59 0d f5 04 0a
	Applied policies	EVCP of ETSI EN 319 411-1 QCP-w of ETSI EN 319 411-2

[1] In the following termed shortly „TÜViT"
[2] http://www.dakks.de/en/content/accredited-bodies-dakks?Regnr=D-ZE-12022-01-01

The first audit was performed as a point-in-time audit at the TSP's location in Budapest, Hungary. It took place from 2018-09-10 until 2018-09-14.

The audit was performed according to the European Standards "ETSI EN 319 411-2, V2.1.1 (2016-02)", "ETSI EN 319 411-1, V1.1.1 (2016-02)" and "ETSI EN 319 401, V2.1.1 (2016-02)" as well as CA Browser Forum Requirements "EV SSL Certificate Guidelines, version 1.6.8" and "Baseline Requirements, version 1.6.0" considering the requirements of the "ETSI EN 319 403, V2.2.2 (2015-08)" for the Trust Service Provider Conformity Assessment.

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

1. CP e-Szignó Certification Authority eIDAS conform Qualified Certificates for Website Authentication Certificate Policy, version: 2.8 as of 14.11.2018, Date of effect: 14.12.2018,
2. CPS e-Szignó Certification Authority eIDAS conform Qualified Certificate for Website Authentication Certification Practice Statement, version: 2.8 as of 14.11.2018, Date of effect: 14.12.2018,
3. PDS e-Szignó Certification Authority eIDAS conform Qualified Certificate for Website Authentication Disclosure Statement, version: 2.8 as of 14.11.2018, Date of effect: 14.12.2018.

The following non-conformities have been identified during the audit:

- The TSP shall remove irrelevant and confusing information from each policy (e.g. explanation of how to create policy codes) [ETSI EN 319 401, REQ-6.1-01]
- The TSP shall clearly indicate which kind of documents are necessary for the application procedures of different types of certificates. [ETSI EN 319 401, REQ-6.1-01]
- The TSP shall maintain such asset list which can support the daily operation and does not cover unnecessary elements (e.g. mouse, keyboard) [ETSI EN 319 401, REQ-7.3.1-01, REQ-7.3.1-02]
- The TSP shall ensure that the password policy provisions are applied in all systems in the TSP and shall review them periodically. [ETSI EN 319 401, REQ-7.4-06]
- The TSP shall move the videoserver from the secondary data center to another secure location without IT administrator access and shall review the records on regular basis. [ISO27001], [ETSI EN 319 401, REQ-7.6-03]
- The TSP shall check operational state of the CCTV system regularly. [ETSI EN 319 401, REQ-7.6-03]
- The TSP shall extend the Termination Plan to all services mentioned in the CPSs. [ETSI EN 319 401, REQ-7.12-02]

- The TSP shall check the possibilities to store and review video logs for a longer period of time. [ETSI EN 319 411-1, OVR-6.4.2-07]
- The TSP shall maintain dual control for performing critical functions on the core systems (including Root CA, intermediate CAs, archiving system, TSA system, OCSP responders etc.) [ETSI EN 319 411-1, GEN-6.4.3-02, OVR-6.4.8-07, GEN-6.5.1-04, GEN-6.5.2-06]
- The TSP shall develop a restoration plan which schedules the restoration over time to cover every system. [ETSI 319 411-1, OVR-6.4.8-05]
- The TSP shall approve and publish the latest version of its CP und CPS documents. [ETSI EN 319 401, REQ-6.1-05]
- The TSP shall modify the web application form and the registration interface in such a way that it is clearly indicated what kind of information are required for the issuance of the given certificate in accordance with the policies. Misleading information shall be avoided. [ETSI EN 319 401, REQ-6.1-01]

The Sub-CAs that have been issued by the aforementioned Root-CA and that have been covered by this audit are listed in table 1 below. The TSP assured that all non-revoked Sub-CA's that are technically capable of issuing server or email certificates and that have been issued by this Root-CA are in the scope of regular audits.

Identification of the Sub-CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number OID	Applied policy	Service	EKU	Validity
e-Szigno Qualified TLS CA 2018	CN=e-Szigno Qualified TLS CA 2018, 2.5.4.97=VATHU-23584497, O=Microsec Ltd., L=Budapest, C=HU	7d f8 00 07 5f 52 03 c0 17 36 4e 81 19 5a 9a c9 ff 00 c5 07 d6 4a 70 f7 37 d8 d3 e8 cb 3f 08 45	00 b7 f3 3e b7 78 eb 63 1c be 7c 80 0a	QCP-w	server authentication	not defined	2018-07-31 until 2042-08-22

Table 1: Sub-CA's issued by the Root-CA

Modifications record

Version	Issuing Date	Changes
Version 1	13.12.2018	Initial attestation

End of the audit attestation letter.