Audit Attestation for

MICROSEC Micro Software Engineering & Consulting Private Limited Company by Shares

Reference: AA2019121301

Essen, 2020-05-26

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 “**AA2019121301**” and consists of 14 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,

Dr. Silke Keller	Péter Máté Erdősi
Reviewer	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, Ángel Sanz Briz út 13, 1033 Budapest, Hungary registered under 01-10-047218

Identification of the audited Root-CA1:	Microsec e-Szigno Root CA 2009	
	Distinguished Name	E = info@e-szigno.hu CN = Microsec e-Szigno Root CA 2009 O = Microsec Ltd. L = Budapest C = HU
	SHA-256 fingerprint	3C5F81FEA5FAB82C64BFA2EAECAFCDE8E077FC8620A7CAE537163DF36EDBF378
	Certificate Serial number	00C27E43044E473F19
	Applied policy	LCP, NCP, NCP+, OVCP, DVCP, IVCP and EVCP of ETSI EN 319 411-1 QCP-l, QCP-l-qscd, QCP-n, QCP-n-qscd and QCP-w of ETSI EN 319 411-2 TSA of ETSI EN 319 421 Preservation of ETSI TS 102 573

Additional Certificates for this Root-CA (not used anymore):

Identification of the audited Root-CA2:	Microsec e-Szigno Root CA 2009	
	Distinguished Name	E = info@e-szigno.hu CN = Microsec e-Szigno Root CA 2009 O = Microsec Ltd. L = Budapest C = HU

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

	SHA-256 fingerprint	8E8C6EBF77DC73DB3E38E93F4803E62B6B5933BEB51EE4152F68D7AA14426B31
	Certificate Serial number	00C27E43044E473F18
	Applied policy	LCP, NCP, NCP+, OVCP, DVCP, IVCP and EVCP of ETSI EN 319 411-1 QCP-l, QCP-l-qscd, QCP-n, QCP-n-qscd and QCP-w of ETSI EN 319 411-2 TSA of ETSI EN 319 421 Preservation of ETSI TS 102 573

Identification of the audited Root-CA3:	Microsec e-Szigno Root CA 2009	
	Distinguished Name	E = info@e-szigno.hu CN = Microsec e-Szigno Root CA 2009 O = Microsec Ltd. L = Budapest C = HU
	SHA-256 fingerprint	72F9AF2158181BAF16D60C9B4E6F4BD7CA8D2341AD48AFDB67CB4C8332D546F6
	Certificate Serial number	00E8849639AB66105A
	Applied policy	LCP, NCP, NCP+, OVCP, DVCP, IVCP and EVCP of ETSI EN 319 411-1 QCP-l, QCP-l-qscd, QCP-n, QCP-n-qscd and QCP-w of ETSI EN 319 411-2 TSA of ETSI EN 319 421 Preservation of ETSI TS 102 573

Note: After issuance of version 1.0 of this attestation, the conformity assessment body has been informed that additional certificates for the audited root CA are existing and had not been requested to be in scope of the performed audit.

All three certificates, the active root certificate as well as both predecessors that are not used anymore, share the identical public key, subject DN and SPKI. As all certificates share the same key pair, the audit results with regard to CA key pair security can equally be applied to the two unused doppelganger certificates.

Details are given in the following thread of the mozilla.dev.security.policy mailing list https://groups.google.com/forum/#!topic/mozilla.dev.security.policy/QqYm4BhFMHs and a corresponding Bugzilla entry at https://bugzilla.mozilla.org/show_bug.cgi?id=1625767.

The audit was performed as full period of time audit at the TSP's location in Budapest, Hungary. It took place from 2019-09-16 until 2019-09-19 and covered the period from 2018-09-15 until 2019-09-14. The audit was performed according to the European Standards "ETSI EN 319 411-2, V2.2.2 (2018-04)", "ETSI EN 319 411-1, V1.2.2 (2018-04)" and "ETSI EN 319 401, V2.2.1 (2018-04)" as well as CA Browser Forum Requirements "EV SSL Certificate Guidelines, version 1.6.8" and "Baseline Requirements, version 1.6.6" 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. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Signature Certificate Policies, version: 2.11 as of 2019-09-23, Date of effect: 2019-09-25
2. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Seal Certificate Policies, version: 2.11 as of 2019-09-23, Date of effect: 2019-09-25
3. e-Szignó Certification Authority, Non eIDAS covered Certificate, Certificate Policies, version: 2.11 as of 2019-09-23, Date of effect: 2019-09-25
4. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Certificate Policies, version: 2.11 as of 2019-09-23, Date of effect: 2019-09-25
5. e-Szignó Certification Authority, eIDAS conform Qualified Certificates for Website Authentication Certificate Policy, version: 2.11 as of 2019-09-23, Date of effect: 2019-09-25
6. e-Szignó Certification Authority, eIDAS conform Qualified Time Stamping Policy, version: 2.11 as of 2019-09-23, Date of effect: 2019-09-25
7. e-Szignó Certification Authority, eIDAS conform, Qualified Long-Term Preservation Service, Long-Term Preservation Policy, version: 2.11 as of 2019-09-23, Date of effect: 2019-09-25
8. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Seal Certificate Policies, version: 2.11 as of 2019-09-23, Date of effect: 2019-09-25
9. e-Szignó Certification Authority, eIDAS conform, Qualified Certificate for Electronic Signature, Certificate Policies, version: 2.11 as of 2019-09-23, Date of effect: 2019-09-25
10. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic, Signature Certification Practice Statement, version: 2.11 as of 2019-09-23, Date of effect: 2019-09-25
11. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Seal Certification Practice Statement, version: 2.11 as of 2019-09-23, Date of effect: 2019-09-25

12. e-Szignó Certification Authority, Non eIDAS covered Certificates Certification Practice Statement, version: 2.11 as of 2019-09-23, Date of effect: 2019-09-25
13. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Certification Practice Statement, version: 2.11 as of 2019-09-23, Date of effect: 2019-09-25
14. e-Szignó Certification Authority ,eIDAS conform Qualified Certificate for Website Authentication Certification Practice Statement, version: 2.11 as of 2019-09-23, Date of effect: 2019-09-25
15. e-Szignó Certification Authority, eIDAS conform Qualified Time Stamping Practice Statement, version: 2.11 as of 2019-09-23, Date of effect: 2019-09-25
16. e-Szignó Certification Authority, eIDAS conform Qualified Long-Term Preservation Service Preservation Practice Statement, version: 2.11 as of 2019-09-23, Date of effect: 2019-09-25
17. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Seal Certification Practice Statement, version: 2.11 as of 2019-09-23, Date of effect: 2019-09-25
18. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Signature Certification Practice Statement, version: 2.11 as of 2019-09-23, Date of effect: 2019-09-25
19. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Signature Disclosure Statement, version: 2.11 as of 2019-09-23, Date of effect: 2019-09-25
20. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Seal Disclosure Statement, version: 2.11 as of 2019-09-23, Date of effect: 2019-09-25
21. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Disclosure Statement, version: 2.11 as of 2019-09-23, Date of effect: 2019-09-25
22. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Website Authentication Disclosure Statement, version: 2.11 as of 2019-09-23, Date of effect: 2019-09-25
23. e-Szignó Certification Authority, eIDAS conform Qualified Time Stamping Disclosure Statement, version: 2.11 as of 2019-09-23, Date of effect: 2019-09-25
24. e-Szignó Certification Authority, eIDAS conform Qualified Long-Term Preservation Service Preservation Disclosure Statement, version: 2.11 as of 2019-09-23, Date of effect: 2019-09-25
25. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Seal Disclosure Statement, version: 2.11 as of 2019-09-23, Date of effect: 2019-09-25

26. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Signature Disclosure Statement, version: 2.11 as of 2019-09-23, Date of effect: 2019-09-25

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.

In the following areas, non-conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:

6.1 Trust Service Practice statement

The TSP shall not issue non-compliant test certificates from the live environment. As this has been occurred in the past, the TSP shall provide evidences of the changed testing procedures to avoid further occurrence of such events. [ETSI EN 319 401, REQ-6.1-07]

Findings with regard to ETSI EN 319 411-1:

6.2 Identification and authentication

The TSP shall ensure that all issuance of a qualified signature comply with eIDAS Article 24 in each case. [ETSI EN 319 411-1, REG-6.2.3-01]

The TSP shall ensure that all issuance of a qualified certificate comply with eIDAS Article 24 when TSP accepts certificate re-keying requests as written mail with handwritten (wet) signatures via postal services and any of the subject's data is changed. [ETSI EN 319 411-1, REG-6.2.3-01]

The TSP shall review the re-keying procedure in the CPS and shall align the CPS with the real processes and the relating standards. [ETSI EN 319 411-1, REG-6.2.3-02]

The TSP shall ensure that the reusing procedure of all data fulfills the EVCG 11.14 and the CPS corresponds to these reusing requirements. [ETSI EN 319 411-1, REG-6.2.3-03]

6.5 Technical security control

There are conflicts between Hungarian law and EV Guideline regarding to the witnessing the root ca key generation by a Qualified Auditor, the TSP must inform the CAB/Forum about this fact. [ETSI 319 411-1 GEN-6.5.1-14], [BRG, 9.16.3], [EVCG, 8.1], [EVCG, 17.7]

The TSP shall present a mitigation plan to revoke and replace the non-conforming certificates with exponent 101. [ETSI EN 319 411-1, SDP-6.5.1-18]

Findings with regard to ETSI EN 319 411-2:
None

Findings with regard to ETSI EN 319 421:
none

For all minor non-conformities, the remediation has been successfully checked by provided evidences.

This Audit Attestation also covers the following incident as documented under

- *Bug [1512270], [MICROSEC]: [Validity period greater than 825 days]: https://bugzilla.mozilla.org/show_bug.cgi?id=1512270.*

The remediation measures taken by Microsec as described on Bugzilla (see link above) have been accompanied by the auditors and showed to properly address the incident. The long-term effectiveness of the measures will be rechecked at the next regular audit.

Identification of the Sub-CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number OID	Applied policy	Service	EKU	Validity
Advanced Class 3 e-Szigno CA 2009	emailAddress=info@e-szigno.hu, CN=Advanced Class 3 e-Szigno CA 2009, O=Microsec Ltd., L=Budapest, C=HU	B0A6EF0350E7C4C6056BEEA7AF9D2D860B9ED102137B9729D3C23216D195546A	19	NCP, NCP+, Preservation		not defined	2009-12-02 until 2029-12-29
Advanced Code Signing Class3 e-Szigno CA 2016	CN=Advanced Code Signing Class3 e-Szigno CA 2016, 2.5.4.97= VATHU-23584497-2-41, O=Microsec Ltd., L=Budapest, C=HU	283CA6939530C1B5503915051936378AE36871967B03E4C2E7C243F14967DEB1	008C55D86652702EF11B33AE0A	NCP, NCP+	code signing	not defined	2016-06-22 until 2029-12-29
Advanced Pseudonymous e-Szigno CA 2009	emailAddress=info@e-szigno.hu, CN=Advanced Pseudonymous e-Szigno CA 2009, O=Microsec Ltd., L=Budapest,	D0E39AA7D2FA53581008A15D825C57D25BD49247834431F8A227A29C280A1C0C	1A	LCP, NCP, NCP+		not defined	2009-12-02 until 2029-12-29

	C=HU						
Class3 KET e-Szigno CA 2018	CN=Class3 KET e-Szigno CA 2018, 2.5.4.97= VATHU-23584497, O=Microsec Ltd., L=Budapest, C=HU	7BCF1C8A12EE0B2854A1B41070652B0325E7D0C20B9C44D4ACE9C643387F1431	00 BD AC 3D 35 98 4F 42 E5 56 0E 22 0A	NCP, NCP+		not defined	2018-09-06 until 2029-12-29
Advanced Class 2 e-Szigno CA 2009	E = info@e-szigno.hu, CN = Advanced Class 2 e-Szigno CA 2009, O = Microsec Ltd., L = Budapest, C = HU	C63543729A370C26952B47E1D1D1AEA84CB1B07F1B0F964C2FEDDC523FD7C795	18	LCP		not defined	2009-12-02 until 2029-12-29
Advanced eIDAS Class2 e-Szigno CA 2016	CN = Advanced eIDAS Class2 e-Szigno CA 2016, 2.5.4.97 = VATHU-23584497-2-41, O = Microsec Ltd., L = Budapest, C = HU	A29C104B100C3A7933473E62E4BE6371D653A1604D04EDAAD02C95806065CEE3	008B288ADD98AF791B02207F0A	LCP		not defined	2016-02-22 until 2029-12-29

Advanced Code Signing Class2 e-Szigno CA 2016	CN = Advanced Code Signing Class2 e-Szigno CA 2016, 2.5.4.97 = VATHU-23584497-2-41, O = Microsec Ltd., L = Budapest, C = HU	A98C8CED93F9A43631ABE4573864E06C5192900723E97D1EED2C0D7C68B2D079	008D8DD221EED2535B843E1E0A	LCP	code signing	not defined	2016-08-29 until 2029-12-29
Qualified e-Szigno QCP CA 2012	E = info@e-szigno.hu CN = Qualified e-Szigno QCP CA 2012 O = Microsec Ltd. L = Budapest C = HU	CFCB60C1F0180C68E3EA5D24B4A05E9D9900D87C3D83D503CE1690B3C1656458	2EEBA3B3AF911A4B31BDB10A	Preservation, QCP-l-NCP+, QCP-n-NCP+, QCP-l, QCP-n	signature	not defined	2012-03-30 until 2029-12-29
Online e-Szigno SSL CA 2016	CN=Online e-Szigno SSL CA 2016, 2.5.4.97= VATHU-23584497-2-41, O=Microsec Ltd., L=Budapest, C=HU	31DAA25D142D08B90E640D4BC50B249F0FE39785C98D5E53E233259C0FAE9398	008F816ED551C9924ED78FB10A	OVCP, DVCP, IVCP	server authentication	not defined	2016-08-29 until 2029-12-29

e-Szigno SSL CA 2014	emailAddress=info@e-szigno.hu, CN=e-Szigno SSL CA 2014, O=Microsec Ltd., L=Budapest, C=HU	EAC241C0440A36830111383336BC20CAC7409C20F6E88D4F84F4827BE919E338	00535CD2A3AC13D9DC4A4B830A	OVCP, DVCP, IVCP	server authentication	not defined	2014-07-08 until 2029-12-29
Class2 e-Szigno SSL CA 2016	CN= Class2 e-Szigno SSL CA 2016, 2.5.4.97= VATHU-23584497-2-41, O=Microsec Ltd., L=Budapest, C=HU	3912C585E727F2B077888F678F043FD8DDCEE9E91E6628A6245B1B8EBBCC3912	008E5F46EF1EC4E10FCA08160A	OVCP, DVCP, IVCP	server authentication	not defined	2016-08-29 until 2029-12-29
e-Szigno TSA CA 2017	CN = e-Szigno TSA CA 2017 2.5.4.97 = VATHU-23584497 O = Microsec Ltd. L = Budapest C = HU	4DE7CCACB5099942644950F2CC86134012565C614D51AA7D3087FAC196958A14	00C87EA0E9453B319854F24E0A	TSA	time stamping	1.3.6.1.5.5.7.3.8 1.3.6.1.5.5.7.3.9	2019-09-10 until 2029-09-29
Qualified e-Szigno Organization CA 2016	CN=Qualified e-Szigno Organization CA 2016,	60AF9E5F39D873B236BE142BC706DA571849AED7FAE635FC5A1461A0CF7459C5	0090274984CBF0D2D9AFAFF30A	QCP-l-qscd	signature	not defined	2016-08-29 until 2029-12-29

	2.5.4.97=VATHU-23584497-2-41, O=Microsec Ltd., L=Budapest, C=HU						
Qualified KET e-Szigno CA 2018	CN=Qualified KET e-Szigno CA 2018, 2.5.4.97= VATHU-23584497, O=Microsec Ltd., L=Budapest, C=HU	D9E445B22C6FCB37B296FCD1331486569651A8DB98071753FEFC73D2C97BF732	00BC3D9A56D441A2BB5987620A	QCP-l-qscd, QCP-l, QCP-n-qscd, QCP-n	signature	not defined	2018-09-06 until 2029-12-29
Qualified e-Szigno CA 2009	emailAddress=info@e-szigno.hu, CN=Qualified e-Szigno CA 2009, O=Microsec Ltd., L=Budapest, C=HU	B884ED6527433687627D35157E904690D2DFF6A5DCD3CE267BBAF159C06F5054	16	QCP-n-qscd	signature	not defined	2009-12-02 until 2029-12-29
Qualified Pseudonymous e-Szigno CA 2009	emailAddress=info@e-szigno.hu, CN= Qualified Pseudonymous e-Szigno CA 2009, O=Microsec Ltd., L=Budapest, C=HU	F8684D2812BA98A52FE94528C4CB152378A2D73A828810A8C7B8529875C64674	17	QCP-n	signature	not defined	2009-12-02 until 2029-12-29

Qualified e-Szigno TLS CA 2018	CN=Qualified e-Szigno TLS CA 2018, 2.5.4.97=VATHU-23584497, O=Microsec Ltd., L=Budapest, C=HU	F7C7E28FB5E79F314AAAC6BBBA932F15E1A72069F435D4C9E707F93CA1482EE3	00B86EDF27D8F6967C6470630A	EVCP, QCP-w	Server authentication	not defined	2018-07-31 until 2029-12-29

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

Modifications record

Version	Issuing Date	Changes
Version 1.0	2019-12-13	Initial attestation
Version 1.1	2020-02-03	Addition of issuing CAs of the root. Addition of an additional Certificate for this Root-CA.
Version 1.2	2020-05-07	Addition of an additional Certificate for this Root-CA.

End of the audit attestation letter.