



# Audit Attestation for

## MICROSEC Micro Software Engineering & Consulting Private Limited Company by Shares

Reference: AA2018121303

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 "**AA2018121303**" and consist of 11 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: [certuivit@tuvit.de](mailto:certuivit@tuvit.de)  
Phone: +49 (0) 201 / 8999-9

With best regards,

---

Matthias Wiedenhorst  
Reviewer

---

Péter Máté, Erdősi  
Leadauditor

TÜV Informationstechnik GmbH – Member of TÜV NORD GROUP

Langemarckstrasse 20  
45141 Essen, Germany  
Phone: +49 201 8999-9  
Fax: +49 201 8999-888  
info@tuvit.de  
www.tuvit.de

Court of jurisdiction:  
Essen HRB 11687  
VAT ID.: DE 176132277  
Tax No.: 111/57062251

Commerzbank AG  
SWIFT/BIC Code: DRES DEFF 360  
IBAN: DE47 3608 0080 0525 4851 00

Management Board  
Dirk Kretzschmar

Identification of the conformity assessment body (CAB):	TÜV Informationstechnik GmbH <sup>1</sup> , Langemarckstraße 20, 45141 Essen, Germany registered under HRB 11687, Amtsgericht Essen, Germany Accredited by DAkkS under registration D-ZE-12022-01 <sup>2</sup> 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	LCP, NCP, NCP+, OVCP, DVCP, IVCP of ETSI EN 319 411-1 QCP-I, QCP-I-qscd and QCP-n, QCP-n-qscd of ETSI EN 319 411-2 TSA of ETSI EN 319 421

<sup>1</sup> In the following termed shortly „TÜViT“

<sup>2</sup> <http://www.dakks.de/en/content/accredited-bodies-dakks?Regnr=D-ZE-12022-01-01>

The audit was performed as full period of time audit at the TSP's location in Budapest, Hungary. It took place from 2018-09-10 until 2018-09-14 and covered the period from September 29<sup>th</sup>, 2017 until September 14<sup>th</sup>, 2018. 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 "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. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Signature Certificate Policies, version: 2.7 as of 31.07.2018, Date of effect: 15.09.2018
2. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Seal Certificate Policies, version: 2.7 as of 31.07.2018, Date of effect: 15.09.2018
3. e-Szignó Certification Authority, Non eIDAS covered Certificate, Certificate Policies, version: 2.7 as of 16.08.2018, Date of effect: 15.09.2018
4. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Certificate Policies, version: 2.7 as of 31.07.2018, Date of effect: 15.09.2018
5. e-Szignó Certification Authority, eIDAS conform Qualified Time Stamping Policy, version: 2.7 as of 31.07.2018, Date of effect: 15.09.2018
6. e-Szignó Certification Authority, eIDAS conform, Qualified Long-Term Preservation Service, Long-Term Preservation Policy, version: 2.7 as of 31.07.2018, Date of effect: 15.09.2018
7. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Seal Certificate Policies, version: 2.7 as of 31.07.2018, Date of effect: 15.09.2018
8. e-Szignó Certification Authority, eIDAS conform, Qualified Certificate for Electronic Signature, Certificate Policies, version: 2.7 as of 31.07.2018, Date of effect: 15.09.2018
9. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic, Signature Certification Practice Statement, version: 2.7 as of 16.08.2018, Date of effect: 15.09.2018
10. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Seal Certification Practice Statement, version: 2.7 as of 16.08.2018, Date of effect: 15.09.2018
11. e-Szignó Certification Authority, Non eIDAS covered Certificates Certification Practice Statement, version: 2.7 as of 16.08.2018, Date of effect: 15.09.2018
12. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Certification Practice Statement, version: 2.8 as of 14.11.2018, Date of effect: 14.12.2018
13. e-Szignó Certification Authority, eIDAS conform Qualified Time Stamping Practice Statement, version: 2.7 as of 31.07.2018, Date of effect: 15.09.2018
14. e-Szignó Certification Authority, eIDAS conform Qualified Long-Term Preservation Service Preservation Practice Statement, version: 2.7 as of 31.07.2018, Date of effect: 15.09.2018

This template (version 2 as of 2018-03-05) was approved for use by ACAB-c. It may only be used to without modification.

Audit Attestation MICROSEC Micro Software Engineering & Consulting Private Limited Company by Shares AA2018121303

15. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Seal Certification Practice Statement, version: 2.7 as of 16.08.2018, Date of effect: 15.09.2018
16. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Signature Certification Practice Statement , version: 2.7 as of 16.08.2018, Date of effect: 15.09.2018
17. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic, Signature Disclosure Statement, version: 2.7 as of 31.07.2018, Date of effect: 15.09.2018
18. e-Szignó Certification Authority, eIDAS conform Non-Qualified Certificate for Electronic Seal Disclosure Statement, version: 2.7 as of 31.07.2018, Date of effect: 15.09.2018
19. e-Szignó Certification Authority, eIDAS conform Certificate for Website Authentication Disclosure Statement, version: 2.7 as of 31.07.2018, Date of effect: 15.09.2018
20. e-Szignó Certification Authority, eIDAS conform Qualified Time Stamping Disclosure Statement, version: 2.7 as of 31.07.2018, Date of effect: 15.09.2018
21. e-Szignó Certification Authority, eIDAS conform Qualified Long-Term Preservation Service Preservation Disclosure Statement, version: 2.7 as of 31.07.2018, Date of effect: 15.09.2018
22. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Seal Disclosure Statement, version: 2.7 as of 31.07.2018, Date of effect: 15.09.2018
23. e-Szignó Certification Authority, eIDAS conform Qualified Certificate for Electronic Signature Disclosure Statement, version: 2.7 as of 31.07.2018, Date of effect: 15.09.2018

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 videosever 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]

This template (version 2 as of 2018-03-05) was approved for use by ACAB-c. It may only be used to without modification.

Audit Attestation MICROSEC Micro Software Engineering & Consulting Private Limited Company by Shares AA2018121303

- 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 Class3 CA 2017	CN = e-Szigno Class3 CA 2017 2.5.4.97 = VATHU-23584497 O = Microsec Ltd. L = Budapest C = HU	4f 83 84 2f 1f 04 ab 1e 04 d4 d8 e7 51 66 6f ca 82 e5 19 1c af c2 40 62 bf d1 fe 77 c0 2c a4 b4	00 a2 a6 92 bf 8e 59 6b 56 02 ea 8b 0a	NCP, NCP+		not defined	2017-09-17 until 2042-08-22
e-Szigno Class3 CodeSigning CA 2017	CN = e-Szigno Class3 CodeSigning CA 2017 2.5.4.97 = VATHU-23584497 O = Microsec Ltd. L = Budapest C = HU	db 65 55 fa 1d 98 34 52 74 69 09 5f 93 46 9f 7a f3 fb 29 ce c5 55 de d1 48 a5 b0 20 7c ec 7f 43	00 ab 5b 68 15 64 a5 20 93 18 f6 ab 0a	NCP, NCP+	code signing	not defined	2017-09-17 until 2042-08-22
e-Szigno Pseudonymous CA 2017	CN=e-Szigno Pseudonymous CA 2017, 2.5.4.97=VATHU-23584497, O=Microsec Ltd., L=Budapest, C=HU	6a 6f 2f a1 3b 2d 9d bb b4 09 80 20 02 d3 37 06 72 76 0a 21 78 d9 b8 d5 69 4d 66 04 74 23 1f a4	00 a8 a6 20 7e 07 5c e7 8d 92 3a f7 0a	LCP, NCP, NCP+		not defined	2017-09-17 until 2042-08-22
e-Szigno Class2 CA 2017	CN = e-Szigno Class2 CA 2017	42 dc 82 7f 46 fb 5e 85 df fa e4 7d 3c 69 0f 50 1e	00 a1 5a 22 e9 dc 03 5b ef e8 fd 99 0a	LCP		not defined	2017-09-17 until 2042-08-22

This template (version 2 as of 2018-03-05) was approved for use by ACAB-c. It may only be used to without modification.

Audit Attestation MICROSEC Micro Software Engineering & Consulting Private Limited Company by Shares AA2018121303

Identification of the Sub-CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number OID	Applied policy	Service	EKU	Validity
	2.5.4.97 = VATHU-23584497 O = Microsec Ltd. L = Budapest C = HU	ce 25 d5 75 d5 97 a5 0d 8f 87 8f a4 2a fc ea					
e-Szigno Class2 CodeSigning CA 2017	CN = e-Szigno Class2 CodeSigning CA 2017 2.5.4.97 = VATHU-23584497 O = Microsec Ltd. L = Budapest C = HU	e9 48 89 66 22 f9 27 06 b1 91 e7 e0 66 42 83 1a 63 b5 f3 92 b7 8f 92 f0 2e 0d 69 6e 74 74 00 d9	00 aa 7d b8 ee 27 7d aa c2 e3 e5 cb 0a	LCP		not defined	2017-09-17 until 2042-08-22
e-Szigno Qualified QCP CA 2017	CN= e-Szigno Qualified QCP CA 2017, 2.5.4.97=VATHU-23584497, O=Microsec Ltd., L=Budapest, C=HU	60 81 be e5 b0 df 19 1a c4 e2 65 ac 0f 6f 78 99 f0 78 b8 c8 9f 06 05 5a e1 66 af 91 df 70 d6 e0	00 9e 2c 5e b9 59 fd 77 4c dd 86 6a 0a	QCP-I-NCP+, QCP-n-NCP+, QPC-I, QCP-n	signature	not defined	2017-09-17 until 2042-08-22
e-Szigno Online SSL CA 2017	CN=e-Szigno Online SSL CA 2017, 2.5.4.97= VATHU-23584497,	97 4b 82 07 61 54 ce ff 56 ed 4d b5 62 18 6f 73 94 a0 2f f3 87 aa	00 a7 99 e9 a1 b9 f1 90 5b 9b 8c e6 0a	OVCP, DVCP, IVCP	server authentication	not defined	2017-09-17 until 2042-08-22

This template (version 2 as of 2018-03-05) was approved for use by ACAB-c. It may only be used to without modification.

Audit Attestation MICROSEC Micro Software Engineering & Consulting Private Limited Company by Shares AA2018121303

Identification of the Sub-CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number OID	Applied policy	Service	EKU	Validity
	O=Microsec Ltd., L=Budapest, C=HU	20 5d 63 67 a8 b0 8f f7 fa a0					
e-Szigno Class3 SSL CA 2017	CN=e-Szigno Class3 SSL CA 2017, 2.5.4.97= VATHU- 23584497, O=Microsec Ltd., L=Budapest, C=HU	bc bc 18 c4 63 b6 1f 3a 03 3b 10 c7 49 74 ed 8a 2c 32 8a fc d6 7a 33 8d 98 71 50 6a 35 15 41 9f	00 a3 f1 c9 9d 52 56 9d 8d 99 2e 4c 0a	OVCP, DVCP, IVCP	server authentication	not defined	2017-09-17 until 2042- 08-22
e-Szigno Class2 SSL CA 2017	CN=e-e-Szigno Class2 SSL CA 2017, 2.5.4.97= VATHU- 23584497, O=Microsec Ltd., L=Budapest, C=HU	2a 0e 3f 2a 77 a8 0d cb e5 cd 52 d5 0d 65 07 6e bd 37 fa d5 31 db 10 d6 a1 38 5a 55 7f 7b 72 5d	00 a6 e9 4d 04 b3 bc a2 dc 1a d6 9d 0a	OVCP, DVCP, IVCP	server authentication	not defined	2017-09-17 until 2042- 08-22
e-szigno Qualified TSA 2018 01	CN = e-Szigno Qualified TSA 2018 01 2.5.4.97 = VATHU- 23584497 O = Microsec Ltd. L = Budapest C = HU	e7 5a 6d 7c d0 f8 4f 12 d4 86 f6 d3 12 53 57 be f9 ed f5 4e e6 94 30 7b 3e d8 26 46 08 72 13 c0	00 01 15 03 1c 8b 0a ac ad 50 44 f2 7f 07 0a	TSA	time stamping		2018-08-29 until 2030- 08-29

This template (version 2 as of 2018-03-05) was approved for use by ACAB-c. It may only be used to without modification.



Audit Attestation MICROSEC Micro Software Engineering & Consulting Private Limited Company by Shares AA2018121303

Identification of the Sub-CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number OID	Applied policy	Service	EKU	Validity
e-Szigno TSA CA 2017	CN = e-Szigno TSA CA 2017 2.5.4.97 = VATHU-23584497 O = Microsec Ltd. L = Budapest C = HU	9e 94 bb 8a da d7 a6 ce 4d cb 12 08 f1 23 9d c1 e4 34 83 f1 b7 e8 1f 74 a9 0a 20 fb 5e 5c 49 b7	00 a9 89 58 cf d8 01 af 00 6f 1e 69 0a	TSA	time stamping	not defined	2017-09-17 until 2042-08-22
e-Szigno Qualified Organization CA 2017	CN e-Szigno Qualified Organization CA 2017, 2.5.4.97=VATHU-23584497, O=Microsec Ltd., L=Budapest, C=HU	12 ea 26 f6 ee ef ec 76 ab 85 92 54 54 03 ab 88 51 5b 00 e2 75 d9 88 87 13 40 7a 86 fc 5c 7f d7	00 9d 6d 3e ff 75 e6 0f ff 2c a1 06 0a	QCP-I-qscd	signature	not defined	2017-09-17 until 2042-08-22
e-Szigno Qualified Pseudonymous CA 2017	CN=e-Szigno Qualified Pseudonymous CA 2017, 2.5.4.97= VATHU-23584497, O=Microsec Ltd., L=Budapest, C=HU	16 48 ce 4a b1 bb 65 c4 85 cb 22 36 c7 68 fa bb 86 51 47 d4 26 91 5b 92 af bc a8 1e 9b 2e e3 bc	00 9f 1d 56 62 20 b1 e4 14 fb 91 3d 0a	QCP-n	signature	not defined	2017-09-17 until 2042-08-22

This template (version 2 as of 2018-03-05) was approved for use by ACAB-c. It may only be used to without modification.

Identification of the Sub-CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number OID	Applied policy	Service	EKU	Validity
e-Szigno Qualified CA 2017	CN = e-Szigno Qualified CA 2017 2.5.4.97 = VATHU- 23584497 O = Microsec Ltd. L = Budapest C = HU	5a be 58 18 f6 d0 2f 05 10 6c 6c 35 55 40 e1 be 21 7c 23 54 b5 35 cf 25 07 bf 85 15 e1 a6 04 4a	00 9c 68 09 58 49 e0 8b ea b4 47 ef 0a	QCP-n-qscd	signature	not defined	2017-09-17 until 2042- 08-22

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

**Modifications record**

<b>Version</b>	<b>Issuing Date</b>	<b>Changes</b>
Version 1	13.12.2018	Initial attestation

**End of the audit attestation letter.**