



Audit Attestation for

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

Reference: AA2018121301

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 "**AA2018121301**" 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
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 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:	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	3c 5f 81 fe a5 fa b8 2c 64 bf a2 ea ec af cd e8e0 77 fc 86 20 a7 ca e5 37 16 3d f3 6e db f3 78
	Certificate Serial number	00 c2 7e 43 04 4e 47 3f 19
	Applied policy	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 Preservation of ETSI TS 102 573

¹ In the following termed shortly „TÜViT“

² <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 29th, 2017 until September 14th, 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 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. 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.

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
24. e-Szignó Certification Authority - eIDAS conform Non-Qualified Time Stamping Practice Statement, version: 2.7 as of 16.08.2018, Date of effect: 15.09.2018
25. e-Szignó Certification Authority - eIDAS conform Non-Qualified Time Stamping Policy, version: 2.7 as of 16.08.2018, 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]
- 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
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	b0 a6 ef 03 50 e7 c4 c6 05 6b ee a7 af 9d 2d 86 0b 9e d1 02 13 7b 97 29 d3 c2 32 16 d1 95 54 6a	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	28 3c a6 93 95 30 c1 b5 50 39 15 05 19 36 37 8a e3 68 71 96 7b 03 e4 c2 e7 c2 43 f1 49 67 de b1	00 8c 55 d8 66 52 70 2e f1 1b 33 ae 0a	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, C=HU	d0 e3 9a a7 d2 fa 53 58 10 08 a1 5d 82 5c 57 d2 5b d4 92 47 83 44 31 f8 a2 27 a2 9c 28 0a 1c 0c	1a	LCP, NCP, NCP+		not defined	2009-12-02 until 2029-12-29
Class3 KET e-Szigno CA 2018	CN=Class3 KET e-Szigno CA 2018, 2.5.4.97= VATHU-23584497,	7b cf 1c 8a 12 ee 0b 28 54 a1 b4 10 70 65 2b 03 25 e7 d0 c2 0b	00 bd ac 3d 35 98 4f 42 e5 56 0e 22 0a	NCP, NCP+		not defined	2018-09-06 until 2029-12-29

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

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	9c 44 d4 ac e9 c6 43 38 7f 14 31					
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	c6 35 43 72 9a 37 0c 26 95 2b 47 e1 d1 d1 ae a8 4c b1 b0 7f 1b 0f 96 4c 2f ed dc 52 3f d7 c7 95	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	a2 9c 10 4b 10 0c 3a 79 33 47 3e 62 e4 be 63 71 d6 53 a1 60 4d 04 ed aa d0 2c 95 80 60 65 ce e3	00 8b 28 8a dd 98 af 79 1b 02 20 7f 0a	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	a9 8c 8c ed 93 f9 a4 36 31 ab e4 57 38 64 e0 6c 51 92 90 07 23 e9 7d 1e ed 2c 0d 7c 68 b2 d0 79	00 8d 8d d2 21 ee d2 53 5b 84 3e 1e 0a	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.	cf cb 60 c1 f0 18 0c 68 e3 ea 5d 24 b4 a0 5e 9d 99 00 d8 7c 3d 83 d5 03 ce 16	2e eb a3 b3 af 91 1a 4b 31 bd b1 0a	Preservation, QCP-I-NCP+, QCP-n-NCP+, QCP-I, QCP-n	signature	not defined	2012-03-30 until 2029-12-29

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

Identification of the Sub-CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number OID	Applied policy	Service	EKU	Validity
	L = Budapest C = HU	90 b3 c1 65 64 58					
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	31 da a2 5d 14 2d 08 b9 0e 64 0d 4b c5 0b 24 9f 0f e3 97 85 c9 8d 5e 53 e2 33 25 9c 0f ae 93 98	00 8f 81 6e d5 51 c9 92 4e d7 8f b1 0a	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	ea c2 41 c0 44 0a 36 83 01 11 38 33 36 bc 20 ca c7 40 9c 20 f6 e8 8d 4f 84 f4 82 7b e9 19 e3 38	00 53 5c d2 a3 ac 13 d9 dc 4a 4b 83 0a	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	39 12 c5 85 e7 27 f2 b0 77 88 8f 67 8f 04 3f d8 dd ce e9 e9 1e 66 28 a6 24 5b 1b 8e bb cc 39 12	00 8e 5f 46 ef 1e c4 e1 0f ca 08 16 0a	OVCP, DVCP, IVCP	server authentication	not defined	2016-08-29 until 2029- 12-29

Audit Attestation MICROSEC Micro Software Engineering & Consulting Private Limited Company by Shares AA2018121301

Identification of the Sub-CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number OID	Applied policy	Service	EKU	Validity
Qualified eIDAS e-Szigno TSA 2017 02	CN = Qualified eIDAS e-Szigno TSA 2017 02 2.5.4.97 = VATHU-23584497 O = Microsec Ltd. L = Budapest C = HU	f5 89 e3 af b7 9b b3 55 76 f5 af f4 77 3d 30 6a 26 91 4f 43 a9 5b 28 2d f6 3f f3 a4 6c fd 89 25	00 b4 f5 45 57 fc fe aa 87 89 be 1f 0a	TSA	time stamping	2.5.29.37.8	2018-05-31 until 2029-12-15
Qualified e-Szigno Organization CA 2016	CN=Qualified e-Szigno Organization CA 2016, 2.5.4.97=VATHU-23584497-2-41, O=Microsec Ltd., L=Budapest, C=HU	60 af 9e 5f 39 d8 73 b2 36 be 14 2b c7 06 da 57 18 49 ae d7 fa e6 35 fc 5a 14 61 a0 cf 74 59 c5	00 90 27 49 84 cb f0 d2 d9 af af f3 0a	QCP-I-qscd	signature	not defined	2016-08-29 until 2029-12-29
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	d9 e4 45 b2 2c 6f cb 37 b2 96 fc d1 33 14 86 56 96 51 a8 db 98 07 17 53 fe fc 73 d2 c9 7b f7 32	00 bc 3d 9a 56 d4 41 a2 bb 59 87 62 0a	QCP-I-qscd, QCP-I, 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,	b8 84 ed 65 27 43 36 87 62 7d 35 15 7e 90 46	16	QCP-n-qscd	signature	not defined	2009-12-02 until 2029-12-29

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

Identification of the Sub-CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number OID	Applied policy	Service	EKU	Validity
	CN=Qualified e-Szigno CA 2009, O=Microsec Ltd., L=Budapest, C=HU	90 d2 df f6 a5 dc d3 ce 26 7b ba f1 59 c0 6f 50 54					
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	f8 68 4d 28 12 ba 98 a5 2f e9 45 28 c4 cb 15 23 78 a2 d7 3a 82 88 10 a8 c7 b8 52 98 75 c6 46 74	17	QCP-n	signature	not defined	2009-12-02 until 2029-12-29

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.