



Audit Attestation for

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

Reference: AA2019121302

Essen, 2019-12-13

To whom it may concern,

This is to confirm that "TÜV Informationstechnik GmbH" has successfully audited the CAs of the "**name of the audited company**" without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number "**AA20191213**" 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: certuvit@tuvit.de
Phone: +49 (0) 201 / 8999-9

With best regards,

Dr. Silke Keller
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 Kretschmar

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-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	BEB00B30839B9BC32C32E44479059506 41F26421B15ED089198B518AE2EA1B99
	Certificate Serial number	00015448EF21FD97590DF5040A
	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

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 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 "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.

1. The audit was based on the following policy and practice statement documents of the TSP: 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 Time Stamping Policy, version: 2.11 as of 2019-09-23, Date of effect: 2019-09-25
6. 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
7. 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
8. 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
9. 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
10. 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
11. 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
12. 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

13. 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
14. 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
15. 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
16. 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
17. 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
18. 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
19. 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
20. 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
21. 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
22. 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
23. 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 process-es 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 has not recorded any incident.

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	4F83842F1F04AB1E04D4D8E751666FCA82E5191CAFC24062BFD1FE77C02CA4B4	00A2A692BF8E596B5602EA8B0A	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	DB6555FA1D9834527469095F93469F7AF3FB29CEC555DED148A5B0207CEC7F43	00AB5B681564A5209318F6AB0A	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	6A6F2FA13B2D9DBBB409802002D3370672760A2178D9B8D5694D660474231FA4	00A8A6207E075CE78D923AF70A	LCP, NCP, NCP+		not defined	2017-09-17 until 2042-08-22

e-Szigno Class2 CA 2017	CN = e-Szigno Class2 CA 2017 2.5.4.97 = VATHU-23584497 O = Microsec Ltd. L = Budapest C = HU	42DC827F46FB5E85DFFAE47D3C690F501ECE25D575D597A50D8F878FA42AFCEA	00A15A22E9DC035BEFE8FD990A	LCP		not defined	2017-09-17 until 2042-08-22
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	E948896622F92706B191E7E06642831A63B5F392B78F92F02E0D696E747400D9	00AA7DB8EE277DAAC2E3E5CB0A	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	6081BEE5B0DF191AC4E265AC0F6F7899F078B8C89F06055AE166AF91DF70D6E0	009E2C5EB959FD774CDD866A0A	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, O=Microsec Ltd., L=Budapest, C=HU	974B82076154CE FF56ED4DB5621 86F7394A02FF38 7AA205D6367A8 B08FF7FAA0	00A799E9A1B9F 1905B9B8CE60A	OVCP, DVCP, IVCP	server authentication	not defined	2017-09-17 until 2042-08- 22
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	BCBC18C463B61 F3A033B10C7497 4ED8A2C328AFC D67A338D987150 6A3515419F	00A3F1C99D525 69D8D992E4C0A	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	2A0E3F2A77A80 DCBE5CD52D50 D65076EBD37FA D531DB10D6A13 85A557F7B725D	00A6E94D04B3B CA2DC1AD69D0 A	OVCP, DVCP, IVCP	server authentication	not defined	2017-09-17 until 2042-08- 22

e-Szigno TSA CA 2017	CN = e-Szigno TSA CA 2017 2.5.4.97 = VATHU-23584497 O = Microsec Ltd. L = Budapest C = HU	AE41954DAACBF D3E5B9FD7078F 7B6FAAE61B559 ECE79EF8ED858 AD8C022A7A3C	00C779B0241770 FB6DEF355F0A	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 2042-08-22
e-Szigno TSA CA 2017	CN = e-Szigno TSA CA 2017 2.5.4.97 = VATHU-23584497 O = Microsec Ltd. L = Budapest C = HU	9E94BB8ADAD7A 6CE4DCB1208F1 239DC1E43483F 1B7E81F74A90A 20FB5E5C49B7	00A98958CFD80 1AF006F1E690A	TSA	time stamping	1.3.6.1.5.5.7.3. 8	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	12EA26F6EEFE C76AB859254540 3AB88515B00E27 5D9888713407A8 6FC5C7FD7	009D6D3EFF75E 60FFF2CA1060A	QCP-l-qscd	signature	not defined	2017-09-17 until 2042-08-22
e-Szigno Qualified Pseudonymous CA 2017	CN=e-Szigno Qualified Pseudonymous CA 2017,	1648CE4AB1BB6 5C485CB2236C7 68FABB865147D 426915B92AFBC A81E9B2EE3BC	009F1D566220B1 E414FB913D0A	QCP-n	signature	not defined	2017-09-17 until 2042-08-22

This template (version 2.2 as of 2019-05-28) was approved for use by ACAB-c.

	2.5.4.97= VATHU-23584497, O=Microsec Ltd., L=Budapest, C=HU						
e-Szigno Qualified CA 2017	CN = e-Szigno Qualified CA 2017 2.5.4.97 = VATHU-23584497 O = Microsec Ltd. L = Budapest C = HU	5ABE5818F6D02 F05106C6C35554 0E1BE217C2354 B535CF2507BF8 515E1A6044A	009C68095849E0 8BEAB447EF0A	QCP-n-qscd	signature	not defined	2017-09-17 until 2042-08-22

Table1:Sub-CA's issued by the Root-CA

Modificationsrecord

Version	IssuingDate	Changes
Version1.0	2019-12-13	Initialattestation

Endoftheauditattestationletter.