Audit Attestation for

SK ID Solutions AS

Reference: AA2019051701

Essen, 17.05.2019

To whom it may concern,

This is to confirm that “TÜV Informationstechnik GmbH” has successfully audited the CAs of the “**SK ID Solutions AS**” without critical or non-critical non-conformities.

This present Audit Attestation Letter is registered under the unique identifier number “**AA2019051701**” 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. Anja Wiedemann Reviewer	Boryana Uri Lead Auditor

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):	SK ID Solutions AS, Pärnu avenue 141, 11314 Tallinn, Estonia registered in Commercial register of Estonia with registry code 10747013

Identification of the audited Root-CA:	EE Certification Centre Root CA	
	Distinguished Name	E = pki@sk.ee CN = EE Certification Centre Root CA O = AS Sertifitseerimiskeskus C = EE
	SHA-256 fingerprint	3e 84 ba 43 42 90 85 16 e7 75 73 c0 99 2f 09 79 ca 08 4e 46 85 68 1f f1 95 cc ba 8a 22 9b 8a 76
	Certificate Serial number	54 80 f9 a0 73 ed 3f 00 4c ca 89 d8 e3 71 e6 4a
	Applied policy	OVCP and NCP of ETSI EN 319 411-1 QCP-n, QCP-l, QCP-n-qscd and QCP-l-qscd of ETSI EN 319 411-2 Time stamp 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 Tallinn, Estonia. It took place from 2019-02-25 until 2019-03-01 and covered the period from September 25th, 2018 until March 1st, 2019. The audit was performed according to the European Standards "ETSI EN 319 411-2, V2.1.1 (2016-02)", "ETSI EN 319 411-2, V2.2.2 (2018-04)", "ETSI EN 319 411-1, V1.1.1 (2016-02)", "ETSI EN 319 411-1, V1.2.2 (2018-04)", "ETSI EN 319 401, V2.1.1 (2016-02)" and "ETSI EN 319 401, V2.2.1 (2018-04)" as well as CA Browser Forum Requirements "Baseline Requirements, version 1.6.3" 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. "SK ID Solutions AS – Certificate Policy for TLS Server Certificates", version 6.0 valid from 2019-05-22, SK ID Solutions AS;
2. "SK ID Solutions AS – Certification Practice Statement for KLASS3-SK", version 7.0 valid from 2019-05-22, SK ID Solutions AS;
3. "SK ID Solutions AS – Trust Services Practice Statement", version 6.0 as of 2018-10-17, SK ID Solutions AS;
4. "SK ID Solutions AS – Certificate Policy for Organisation Certificates", version 10.0 as of 2017-11-30, SK ID Solutions AS;
5. "SK ID Solutions AS - Certificate Policy for ID Card", version 8.0 as of 2019-05-01, SK ID Solutions AS;
6. "SK ID Solutions AS – Certificate Policy for Digi ID" Version 9.0 as of 2019-05-01, SK ID Solutions AS;
7. "SK ID Solutions AS - Certificate Policy for Mobile ID of the Republic of Estonia", version 7.0 as of 2019-05-01, SK ID Solutions AS;
8. "SK ID Solutions AS – ESTEID-SK Certification Practice Statement", version 6.0 as of 2019-05-01, SK ID Solutions AS;
9. "CP SK ID Solutions AS – Certificate Policy for non-qualified Smart-ID, version 1.1 as of 2017-02-09, SK ID Solutions AS;
10. CPS SK ID Solutions AS – NQ-SK Certification Practice Statement, version 4.0 as of 2019-05-01, SK ID Solutions AS;
11. "SK ID Solutions AS - EID-SK Certification Practice Statement", 7.0 as of 2018-11-08, SK ID Solutions AS;
12. "SK ID Solutions AS - Certificate Policy for Qualified Smart ID", version 5., as of 2018-11-08, SK ID Solutions AS;
13. "SK ID Solutions AS – Certificate Policy for Mobile-ID of Lithuania", version 1.0 as of 2018-03-01, SK ID Solutions AS;
14. "SK ID Solutions AS - Certificate Policy for the SEB Card", version 5.0, as of 2017-11-01, SK ID Solutions AS;
15. "Time-Stamping Authority Practice Statement", version 3.0, valid from 2019-02-01, SK ID Solutions AS.

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 certificates and that have been issued by this Root-CA are in the scope of regular audits.

The TSP has stopped the issuance of TLS certificates on September 1st, 2017, hence prior to the actual audit period. During the audit, it was verified that the CA's "KLASS3-SK 2010" and "KLASS3-SK 2016" are issuing revocation status information but not any new end entity TLS certificates.

The KLASS3-SK 2010 (sha1RSA) CA also has stopped the issuance of certificates since 2015.

Pending major non-conformities have been closed, if any.

In the following areas minor non-conformities have been identified during the audit:

Findings with regard to ETSI EN 319 401:

7.2 Human resources

Documentation and implementation of the maintenance process for training evidences shall be improved. [ETSI EN 319 401, 7.2 b)]

7.5 Cryptographic controls

Documentation and implementation of the HSM life cycle process and its information shall be improved. [ETSI EN 319 401, 7.5]

7.6 Physical and environmental security

Documentation and implementation of physical access rights to the TSP facilities shall be improved. [ETSI EN 319 401, 7.6 a)]

7.7 Operation security

Documentation and implementation of adequate measures instead of dual control for administration of technical components and critical network components shall be improved. [ETSI EN 319 401, 7.7 c)]

7.8 Network security

Documentation and implementation of vulnerability scans shall be improved. [ETSI EN 319 401, 7.8 g)]

Documentation and implementation of penetrations tests shall be improved. [ETSI EN 319 401, 7.8 h)]

7.9 Incident management

Documentation and implementation of monitoring activities shall be improved. [ETSI EN 319 401, 7.9 g)]

Documentation and implementation of system logs and critical IT components shall be improved. [ETSI EN 319 401, 7.9 g)]

Findings with regard to ETSI EN 319 411-1:

6.5 Technical security controls

Documentation and implementation of HSMs in historic state shall be improved. [ETSI EN 319 411-1, 6.5.2 a)]

All minor non-conformites have been scheduled to be remediated within three months after the onsite audit and will be covered by a corresponding audit.

Identification of the Sub-CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number	Applied policy	Service	EKU	Validy
KLASS3-SK 2010	CN = KLASS3-SK 2010 OU = Sertifitse-erimisteenused O = AS Sertifitse-erimiskeskus C = EE	00 db 86 a7 08 7a 75 0c e0 7b 32 55 d0 d3 12 9e 88 8c a9 e0 ee ca cf 9e 72 bd b2 76 b1 71 47 ef	0a 19 b7 e3 1f 1a 87 70 55 70 57 9d 96 cd 9c da	OVCP of ETSI EN 319 411-1 QCP-l and QCP-l-qscd of ETSI EN 319 411-2	server authentication, qualified electronic seal	Not defined.	2015-06-04 until 2024-03-17, does not issue any certificates from 2016
KLASS3-SK 2010 (sha1RSA)	CN = KLASS3-SK 2010 OU = Sertifitseerimisteenused O = AS Sertifitseerimiskeskus C = EE	17 f3 02 21 9f cf ce 8f d1 8c ac 17 2f 8b 0d 44 96 ba 5d a8 e4 9f 87 1a bc 1f 9d 0c aa a3 60 e5	03 39 d5 a7 52 da c9 ab 4d 83 2e 9b 37 c7 fd 42	OVCP of ETSI-EN 319-411-1 QCP-l and QCP-l-qscd of ETSI EN 319 411-2	server authentication, qualified electronic seal	Not defined.	2011-18-03 until 2024-18-03
KLASS3-SK 2016	CN = KLASS3-SK 2016 2.5.4.97 = NTREE-10747013 OU = Sertifitse-erimisteenused O = AS Sertifitse-erimiskeskus C = EE	a5 a8 59 ce 03 10 a8 5f 42 a5 41 1d a6 3f 83 b4 14 4e b9 4b c8 a6 5a 99 75 ac 86 82 f6 67 db 77	5e 53 3b 13 25 60 34 2b 58 49 57 30 8b 30 78 dc	OVCP of ETSI EN 319 411-1 QCP-l and QCP-l-qscd of ETSI EN 319 411-2	server authentication (certificates issuing only until 01.10.2017), qualified electronic seal	Not defined.	2016-12-08 until 2030-12-17

Identification of the Sub-CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number	Applied policy	Service	EKU	Validy
EID-SK 2011	E = pki@sk.ee CN = EID-SK 2011 O = AS Sertifitse-erimiskeskus C = EE	7b 16 66 a7 99 1c fc 28 b6 4d a3 71 f1 71 41 db d6 f5 32 1f 21 b8 3a 1a 65 8d 6a 41 0d 37 4e 05	43 2b d4 4e 62 43 6b 46 4d 83 2f bf 7d 2d 2f 5a	QCP-n and QCP-n-qscd of ETSI EN 319 411-2	qualified electronic signature	Not defined.	2011-03-18 until 2024-03-18, does not issue any certificates from 2016
EID-SK 2016	CN = EID-SK 2016 2.5.4.97 = NTREE-10747013 O = AS Sertifitse-erimiskeskus C = EE	e7 3f 1f 19 a4 45 9a 60 67 a4 5e 84 db 58 5d 6c 1d f8 f1 2a 73 9d 73 3f 5b 28 99 65 46 f1 87 5a	3b 80 3a 6b 69 c1 2a 8c 57 c5 50 05 31 1b c4 da	QCP-n and QCP-n-qscd of ETSI EN 319 411-2	qualified electronic signature	OCSP signing (1.3.6.1.5.5.7.3.9), client auth (1.3.6.1.5.5.7.3.2) secure email (1.3.6.1.5.5.7.3.4)	2016-08-30 until 2030-12-17
SK TIME_STAMPING AUTHORITY	CN = SK TIMESTAMPING AUTHORITY OU = TSA O = AS Sertifitseerimiskeskus C = EE	1e 49 f4 97 d8 9d 43 0a ad 53 4b 62 2d 82 bd 9b 9d 0d 4a fd b7 b7 d3 69 86 c5 df 09 81 d9 06 7d	24 af ec eb 12 68 d0 02 54 17 f7 86 ed 6f 01 59	Time stamp of ETSI EN 319 421	time stamping	time stamping (1.3.6.1.5.5.7.3.8)	2014-09-16 until 2019-09-16

Identification of the Sub-CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number	Applied policy	Service	EKU	Validy
SK TIMESTAMPING AUTHORITY 2019	C = EE O = SK ID Solutions AS OU = TSA 2.5.4.97 = NTREE-10747013 CN = SK TIMESTAMPING AUTHORITY 2019	25 d4 5a 83 4c 1e a0 e6 69 a8 a5 88 2d 74 1c 96 18 9f ef c0 8f 8c ae 9a cc ab f7 77 58 33 07 54	7e d7 46 4e e8 d3 0f 4d 5c 1b 5d 04 8e b0 12 6c	Time stamp of ETSI EN 319 421	time stamping	time stamping (1.3.6.1.5.5.7.3.8)	2019-01-01 until 2024-01-01

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

The following issuing CA certificates have been generated under the audited Root-CA. It has been ensured by SK that the Sub-CAs (Issuing CAs) were audited and certified by the conformity assessment body of TÜV AUSTRIA CERT. Corresponding evidences (audit reports) have been reviewed by the auditors:

Identification of the Sub-CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number	Applied policy	Service	EKU	Validy
NQ-SK 2016	CN = NQ-SK 2016 2.5.4.97 = NTREE-10747013 O = AS Sertifitseerimiskeskus C = EE	b5 cf e6 b0 b2 aa 86 1a 0b 36 7c 0c 05 39 5a 53 8a d4 93 a9 df 01 15 44 a8 ef c4 68 7f db 2c c8	57 a9 f3 ec a2 2f 0e 28 57 c5 4e f5 61 36 e0 5a	NCP of ETSI EN 319 411-1	non-qualified electronic signature	OCSP signing (1.3.6.1.5.5.7.3.9) client auth (1.3.6.1.5.5.7.3.2) secure email (1.3.6.1.5.5.7.3.4)	2016-08-30 until 2030-12-18
ESTEID-SK 2011	E = pki@sk.ee CN = ESTEID-SK 2011 O = AS Sertifitse-erimiskeskus C = EE	41 ec 80 8e 33 cc a8 65 9e ae a8 16 70 d6 c7 dc 01 44 66 36 e1 f2 27 56 1b 63 07 b8 0b a6 38 62	29 52 93 aa fd 8c c6 d4 4d 83 30 a3 c2 64 51 0d	QCP-n-qscd of ETSI EN 319 411-2	qualified electronic signature	Not defined.	2011-03-18 until 2024-03-18, does not issue any certificates from 2015
ESTEID-SK 2015	CN = ESTEID-SK 2015 2.5.4.97 = NTREE-10747013 O = AS Sertifitse-erimiskeskus	74 d9 92 d3 91 0b cf 7e 34 b8 b5 cd 28 f9 1e ae b4 f4 1f 3d a6 39 4d 78 b8 c4 36 72 d4 3f 4f 0f	45 48 09 0b 87 9c ef 21 56 72 ac d3 de 6c 1b 5b	QCP-n-qscd of ETSI EN 319 411-2	qualified electronic signature	OCSP signing (1.3.6.1.5.5.7.3.9), client auth (1.3.6.1.5.5.7.3.2),	2015-12-17 until 2030-12-17

Identification of the Sub-CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number	Applied policy	Service	EKU	Validy
	C = EE					secure email (1.3.6.1.5.5.7.3.4)	

Modifications record

Version	Issuing Date	Changes
Version 1.0	2019-05-17	Initial attestation

End of the audit attestation letter.