



Audit Attestation for SK ID Solutions AS

Reference: AA2018112301

Essen, 23.11.2018

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 "**AA2018112301**" and consist of 6 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,

Matthias Wiedenhorst
Reviewer

Dr. Bernd Kirsig
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):	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	NCP and OVCP of ETSI EN 319 411-1 QCP-n, QCP-l, QCP-n-qscd and QCP-l-qscd of ETSI EN 319 411-2

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 2018-07-02 until 2018-07-06 as well as on 2018-09-24 and 2018-09-25 and covered the period from October 28th, 2017 until September 25th, 2018. The audit was performed according to the European Standards "ETSI EN 319 411-2, V2.1.1 (2016-02)" and "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. "SK ID Solutions AS – Certificate Policy for TLS Server Certificates", version 5.0 as of 2017 11-30, SK ID Solutions AS;
2. "SK ID Solutions AS – Certification Practice Statement for KLASS3-SK", version 5.0 as of 2017-11-30 and version 6.0 valid from 04.01.2019, SK ID Solutions AS;
3. "SK ID Solutions AS – Trust Service 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, valid from 2017-11-30, SK ID Solutions AS;
5. "SK ID Solutions AS - Certificate Policy for ID Card", Version 8.0 as of 2017-11-01, SK ID Solutions AS;
6. "Certificate Policy for Digi ID" Version 7.0 as of 2017-11-01, SK ID Solutions AS;
7. "SK ID Solutions AS - Certificate Policy for Mobile ID of the Republic of Estonia", Version 6.0 as of 2017-10-24, SK ID Solutions AS;
8. "ESTEID-SK Certification Practice Statement", Version 5.0 as of 2018-11-01, SK ID Solutions AS;
9. "SK ID Solutions AS - EID-SK Certification Practice Statement", Version: 6.2, as of 2018-10-24 and 7.0 2018-11-08, SK ID Solutions AS
10. "SK ID Solutions AS - Certificate Policy for Qualified Smart ID", Version: 4.1, as of 2018-07-06, SK ID Solutions AS;
11. "SK ID Solutions AS – Certificate Policy for Mobile-ID of Lithuania", Version 1.0 as of 2018-03-01;
12. "SK ID Solutions AS - Certificate Policy for the SEB Card", Version: 5.0, as of 2017-11-01, 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-SK2016" are issuing revocation status information but not any new end entity TLS certificates.

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	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-I and QCP-I-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 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-I and QCP-I-qscd of ETSI EN 319 411-2	server authentication (certificates issuing ony until 01.10.2017), qualified electronic seal	Not defined.	2016-12-08 until 2030-12-17
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

Audit Attestation SK ID Solutions AS AA2018112301

ESTEID-SK 2015	CN = ESTEID-SK 2015 2.5.4.97 = NTREE- 10747013 O = AS Sertifitse- erimiskeskus C = EE	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), secure email (1.3.6.1.5.5.7.3.4)	2015-12-17 until 2030-12-17
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

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

Modifications record

Version	Issuing Date	Changes
Version 1	2018-11-23	Initial attestation

End of the audit attestation letter.