TÜV AUSTRIA CERT GMBH

Office:
TÜV AUSTRIA-Platz 1
2345 Brunn am Gebirge
www.tuv.at

Business Area
Business Assurance

Certification Body

TÜV ®

Audit Attestation for

SK ID Solutions AS
Pärnu mnt 141
11314 Tallinn, Estonia

Reference: AA2020052001

Your ref.:	Your message from:	Our ref.:	Date:
-	-	**TUV TRUST IT/wcl**	**2020-05-20**

To whom it may concern,

This is to confirm that TUV AUSTRIA CERT has successfully audited the CA of SK ID Solutions AS without critical findings.

This present Audit Attestation letter is registered under the unique identifier number AA2020052201 and consist of 6 pages. This audit attestation is issued based on the report number TA235203352_SR. Predecessor is Audit Attestation letter TUViT AA2019051701 as of 2019-05-17 which it supersedes.

Kindly find here below the details accordingly.

In case of any question, please contact:

Clemens Wanko
TÜV AUSTRIA CERT GmbH
Cologne office:
51069 Cologne / Germany
Fon: +49 221 96 97 89-0
Mobile: +49 170 80 20 20 7
Fax: +49 221 96 97 89-12
E-Mail: clemens.wanko@tuv-austria.com
https://www.it-tuv.com

With best regards,

i.A. Clemens Wanko

i.V. Andreas Dvorak

Certification Body

Managing director:
DI (FH) Andreas Dvorak, MSc

Registered office:
Deutschstraße 10
1230 Wien/Österreich

Further offices:
www.tuv.at/standorte

Company register court:
Wien / FN 288474 b

Banking details:
IBAN
AT141200052949025201
BIC BKAUATWW

IBAN
AT373100000104093274
BIC RZBAATWW

UID ATU63247169
DVR 3002477

Identification of the conformity assessment body (CAB):	*TÜV AUSTRIA CERT GmbH*[1] *TÜV AUSTRIA-Platz 1, 2345 Brunn am Gebirge,* Company registration: Vienna / Wien / FN 288474 b Accreditation Body: Federal Ministry for Digital and Economic Affairs 1010 Wien, Stubenring 1 mailto: akkreditierung@bmdw.gv.at https://www.bmdw.gv.at/ Accreditation: The CAB is accredited for the certification of trust services according to DIN EN ISO/IEC 17065 and ETSI EN 319 403. URL to accreditation: https://www.bmdw.gv.at/dam/jcr:ffe6b296-8c4c-4977-80de-d2566942a715/AA_0943_17065_TUEV_AUSTRIA_CERT_GMBH.pdf

Identification of the trust service provider (TSP/CA):	*SK ID Solutions AS* *Pärnu avenue 141* *11314 Tallinn, Estonia* *All relevant TSP sites are located in Tallinn, Estonia.* *Contact: Mrs. Katrin Laas-Mikko* *E-Mail: katrin.laas-mikko@skidsolutions.eu* *Company registration: registered in Commercial register of Estonia with registry code 10747013*

Identification of the audited Root-CA:	EE Certification Centre Root CA	
	Distinguished Name	CN = EE Certification Centre Root CA, O = AS Sertifitseerimiskeskus, C = EE
	SHA-256 fingerprint	3E84BA4342908516E77573C0992F0979CA084E4685681FF195CCBA8A229B8A76
	Certificate Serial number	5480F9A073ED3F004CCA89D8E371E64A
	Applied policy	ETSI EN 319 411-1, policy OVCP, NCP, ETSI EN 319 411-2, policy QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd, ETSI EN 319 421 (Time Stamp)

[1] in the following termed shortly „*CAB*“

The audit was performed as full annual audit at the TSP's location in Tallinn, Estonia. It took place between 2020-02-10 until 2020-02-28 and covered the period from 2019-03-02 until 2020-02-28 for all policies. The audit was performed according to the applicable European Standards "*ETSI EN 319 411-1, V1.2.2 (2018-04)", "ETSI EN 319 411-2, V2.2.2 (2018-04)", "ETSI EN 319 421, V1.1.1 (2016-03)" and "ETSI EN 319 401, V2.2.1 (2018-04)*" as well as CA Browser Forum Requirements "*Baseline Requirements, version 1.6.7*" considering the requirements of the "*ETSI EN 319 403, V2.2.2 (2015-08) for the Trust Service Provider Conformity Assessment*" as well as "*ETSI TS 119 403-2, V1.2.1 (2019-04), Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates*".

The full annual audit was based on the following policy and practice statement documents of the TSP:

TSPS	SK ID Solutions AS Trust Services Practice Statement Version 8.0 as of 2020-04-15
TSA_PS	Time Stamping Authority Practice Statement Version 4.0 valid as of 2020-05-01
CP_TLS	Certificate Policy for TLS Server Certificates Version 7.0 as of 2020-04-10
CP_D-ID	SK ID Solutions AS - Certificate Policy for Digi-ID Version 11.0 as of 2020-04-10
CP_ID	SK ID Solutions AS - Certificate Policy for ID card Version 9.0 as of 2020-04-10
CP_MID	SK ID Solutions AS - Certificate Policy for Mobile ID of the Republic of Estonia Version 8.0 as of 2020-04-10
CP_QSID	SK ID Solutions AS - Certificate Policy for Qualified Smart ID Version 6.0 as of 2020-02-21
CP_MIDLT	SK ID Solutions AS – Certificate Policy for Mobile-ID of Lithuania Version 2.0 as of 2020-04-10
CP_SEB	SK ID Solutions AS - Certificate Policy for the SEB Card Version 6.0 as of 2020-04-10
CP_OC	Certificate Policy for Organisational Certificates Version 11.0 as of 2019-08-15
CP_NQ_SmartID	SK ID Solutions AS - Certificate Policy for non-qualified Smart-ID Version 3.0 as valid of 2019-07-01
CPS_K3	Certification Practice Statement for KLASS3-SK Version 9.0 as of 2020-04-10
CPS_EE1	SK ID Solutions AS - ESTEID-SK Certification Practice Statement Version 8.0 as of 2020-04-10
CPS_EID	SK ID Solutions AS - EID-SK Certification Practice Statement Version 9.0 as of 2020-04-10
CPS_ NQ_SmartID	SK ID Solutions AS - NQ-SK Certification Practice Statement Version 5.0 as valid of 2019-07-01

In the following areas Non-Conformities affecting Publicly Trusted Certificates [PTC] have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:
7.7 Operation security
Documentation and use of trustworthy systems was required to be improved.
7.9 Incident management
Documentation and implementation of identified vulnerabilities treatment was required to be improved.

Findings with regard to ETSI EN 319 411-1/2:
5 General provisions on Certification Practice Statement and Certificate Policies

There was a couple certificates (non SSL) rated to be issued with incorrect data and pointed out to the CA for further treatment i.e. stop of further issuance of certificates with incorrect data, crosscheck as well as evaluation of all required further action.
6.6 Certificate, CRL, and OCSP profiles
Documentation and implementation of the OCSP profiles was required to be improved.

All Non-Conformities identified throughout the audit have been scheduled to be remediated within three month after the onsite audit and will be covered by a corresponding remediation audit report.

This Audit Attestation also covers the following incidents as documented under

- Any Policy: Bug *[1614449], [SK ID Solutions]: Audit Letter Validation failures on intermediate certificates]:*
  https://bugzilla.mozilla.org/show_bug.cgi?id=1614449.

The remediation measures taken by SK ID Solutions as described on Bugzilla (see link above) have been accompanied by the auditors and showed to properly address the incident.

The subordinated issuing-CA 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 subordinated issuing-CA 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	Subject Distinguished Name	SHA-256 fingerprint	Certificate serial number	Certificate Policies	KeyUsage	EKU	Validity
ESTEID-SK 2011 (used only for certificate status information)	CN = ESTEID-SK 2011, O = AS Sertifitseerimiskeskus, C = EE	41EC808E33CCA8659EAEA81670D6C7DC01446636E1F227561B6307B80BA63862	295293AAFD8CC6D44D8330A3C264510D	ETSI EN 319 411-2, policy QCP-n-qscd	Certificate Sign, CRL Sign	none	18 Mar 2011 101459 GMT to 18 Mar 2024 101459 GMT
ESTEID-SK 2015	CN = ESTEID-SK 2015, O = AS Sertifitseerimiskeskus, C = EE	74D992D3910BCF7E34B8B5CD28F91EAEB4F41F3DA6394D78B8C43672D43F4F0F	4548090B879CEF215672ACD3DE6C1B5B	ETSI EN 319 411-2, policy QCP-n-qscd	Certificate Sign, CRL Sign	OCSP Signing, TLS Web Client Authentication, E-mail Protection	17 Dec 2015 123843 GMT to 17 Dec 2030 235959 GMT
EID-SK 2011 (used only for certificate status information)	CN = EID-SK 2011, O = AS Sertifitseerimiskeskus, C = EE	7B1666A7991CFC28B64DA371F17141DBD6F5321F21B83A1A658D6A410D374E05	432BD44E62436B464D832FBF7D2D2F5A	ETSI EN 319 411-2, policy QCP-n, QCP-n-qscd	Certificate Sign, CRL Sign	none	18 Mar 2011 101111 GMT to 18 Mar 2024 101111 GMT
EID-SK 2016	CN = EID-SK 2016, O = AS Sertifitseerimiskeskus, C = EE	E73F1F19A4459A6067A45E84DB585D6C1DF8F12A739D733F5B28996546F1875A	3B803A6B69C12A8C57C55005311BC4DA	ETSI EN 319 411-2, policy QCP-n, QCP-n-qscd	Certificate Sign, CRL Sign	OCSP Signing, TLS Web Client Authentication, E-mail Protection	30 Aug 2016 092109 GMT to 17 Dec 2030 235959 GMT
KLASS3-SK 2010 (used only for certificate status information)	CN = KLASS3-SK 2010, O = AS Sertifitseerimiskeskus, C = EE	17F302219FCFCE8FD18CAC172F8B0D4496BA5DA8E49F871ABC1F9D0CAAA360E5	339D5A752DAC9AB4D832E9B37C7FD42	ETSI EN 319 411-1, policy OVCP, ETSI EN 319 411-2, policy QCP-l, QCP-l-qscd	Digital Signature, Non Repudiation, Certificate Sign, CRL Sign	none	18 Mar 2011 100618 GMT to 18 Mar 2024 100618 GMT
KLASS3-SK 2010 (used only for certificate status information)	CN = KLASS3-SK 2010, O = AS Sertifitseerimiskeskus, C = EE	00DB86A7087A750CE07B3255D0D3129E888CA9E0EECACF9E72BDB276B17147EF	A19B7E31F1A87705570579D96CD9CDA	ETSI EN 319 411-1, policy OVCP, ETSI EN 319 411-2, policy QCP-l, QCP-l-qscd	Digital Signature, Non Repudiation, Certificate Sign, CRL Sign	none	04 Jun 2015 135021 GMT to 17 Mar 2024 220000 GMT
KLASS3-SK 2016	CN = KLASS3-SK 2016, O = AS Sertifitseerimiskeskus, C = EE	A5A859CE0310A85F42A5411DA63F83B4144EB94BC8A65A9975AC8682F667DB77	5E533B132560342B584957308B3078DC	ETSI EN 319 411-1, policy OVCP, ETSI EN 319 411-2, policy QCP-l, QCP-l-qscd	Digital Signature, Non Repudiation, Certificate Sign, CRL Sign	none	08 Dec 2016 125056 GMT to 17 Dec 2030 235959 GMT
SK TIMESTAMPING AUTHORITY 2019	CN = SK TIMESTAMPING AUTHORITY 2019, O = SK ID Solutions AS, C = EE	25D45A834C1EA0E669A8A5882D741C96189FEFC08F8CAE9ACCABF77758330754	7ED7464EE8D30F4D5C1B5D048EB0126C	ETSI EN 319 421, time stamp	Digital Signature, Non Repudiation	Time Stamping	01 Jan 2019 210000 GMT to 01 Jan 2024 210000 GMT

SK TIMESTAMPING AUTHORITY 2020	CN = SK TIMESTAMPING AUTHORITY 2020, O = SK ID Solutions AS, C = EE	FD04122AD630AA0099878550D838EBFAEC5D0F33DA035D0D0976FA9670B172D9	62367D745AD943AB5DA450B95E3FFA6E	ETSI EN 319 421, time stamp	Digital Signature, Non Repudiation	Time Stamping	31 Dec 2019 220000 GMT to 31 Dec 2024 220000 GMT
NQ-SK 2016	CN = NQ-SK 2016, O = AS Sertifitseerimiskeskus, C = EE	B5CFE6B0B2AA861A0B367C0C05395A538AD493A9DF011544A8EFC4687FDB2CC8	57A9F3ECA22F0E2857C54EF56136E05A	ETSI EN 319 411-1, policy NCP	Certificate Sign, CRL Sign	OCSP Signing, TLS Web Client Authentication, E-mail Protection	30 Aug 2016 091637 GMT to 17 Dec 2030 235959 GMT

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

Modifications record

Version	Issuing Date	Changes
Version 1	2020-05-20	initial attestation

End of the attestation