



CERTIFICATE

The certification body of TÜV AUSTRIA CERT GMBH herewith grants certification to

SK ID Solutions AS
Pärnu mnt 141
11314 Tallinn
Estonia

confirming that the trust service

ESTEID qualified certificates for electronic signatures

for the scope of

creation of qualified electronic certificates for qualified electronic signatures

is compliant with the relevant requirements as of the regulation
Reg. (EU) No. 910/2014(eIDAS).

The certification statement is valid only with the Conformity Assessment Report
TA235223859_CAR.

The certificate comprises an appendix of 9 pages.

Certificate-Reg.-Nr. TA235223859

begin of certificate validity: 2022-05-28

end of certificate validity: 2024-05-28

Certification body
of TÜV AUSTRIA CERT GMBH

Vienna, 2022-03-18

This certification was carried out in accordance with TÜV AUSTRIA CERT
procedures for auditing and certification and is regularly monitored.
TÜV AUSTRIA CERT GMBH Deutschstraße 10 A-1230 Wien www.tuv.at



Online Verification



www.tuv.at/certcheck

1. Assessment and Certification Details

Subject of this conformity assessment as of 18.03.2022 for the service "ESTEID qualified certificates for electronic signatures" documented with assessment report No. TA235223859_CAR, version 2.1 as of 2022-03-18 were the following documents of the operator and the PKI structure as listed in the following:

1.1. Operator Documents

TSPS	SK ID Solutions AS Trust Services Practice Statement Version 10.0 as of 2021-12-15
CP_EE	Police and Border Guard Board - Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card OID: 1.3.6.1.4.1.51361.1 (PBGB) and 1.3.6.1.4.1.51455.1 (MFA) Version 1.2 as of 2021-04-08
CP_D-ID	SK ID Solutions AS - Certificate Policy for Digi-ID OID: 1.3.6.1.4.1.10015.1.2 Version 11.0 as of 2020-04-10
CP_ID	SK ID Solutions AS - Certificate Policy for ID card OID: 1.3.6.1.4.1.10015.1.1 Version 9.0 as of 2020-04-10
CP_MID	SK ID Solutions AS - Certificate Policy for Mobile ID of the Republic of Estonia OID: 1.3.6.1.4.1.10015.1.3 Version 10.0 as of 2021-05-27
CPS_EE1	SK ID Solutions AS - ESTEID-SK Certification Practice Statement Version 10.0 as of 2021-05-27
CPS_EE2	SK ID Solutions AS - ESTEID2018 Certification Practice Statement Version 5.0 as of 2021-05-12
CPR_EE2	Certificate, CRL and OCSP Profile for ID-1 Format Identity Documents Issued by the Republic of Estonia Version 1.3 as of 2022-02-17
CPR_EE1	Certificate, CRL and OCSP Profile for Personal Identification Documents of the Republic of Estonia Version 8.5 as of 2022-02-17
TAC_EE2	Terms and Conditions for Use of Certificates for ID-1 Format Identity Documents of the Republic of Estonia Version as of 2021-05-12
TAC_EE1	Terms and Conditions for Use of Certificates of Personal Identification Documents of the Republic of Estonia Version as of 2019-07-03

CPR_CA	Certificate, OCSP and CRL Profile for intermediate CA Version 3.3 as of 2022-02-17
--------	---

1.2 Issuing CA covered, representing the service:

Identification of the Sub-CA	Issuer Distinguished Name	Subject Distinguished Name	SHA-1 fingerprint	SHA-256 fingerprint	Certificate serial number	Signature algorithm	Key length	Certificate Policies	KeyUsage	EKU	Validity
ESTEID-SK 2015	E = pki@sk.ee , CN = EE Certification Centre Root CA, O = AS Serfititseerimiskeskus, C = EE	CN = ESTEID-SK 2015, OI = NTREE-10747013, O = AS Serfititseerimiskeskus, C = EE	7223A347FFB E80715B28AF BE1F7369752 5F39B94	74D992D3910 BCF7E34B8B5 CD28F91EAE B4F41F3DA63 94D78B8C436 72D43F4F0F	4548090B879 CEF215672AC D3DE6C1B5B	sha384WithRSAEncryption	4096	Policy: 0.4.0.2042.1.2 Policy: 0.4.0.194112.1.2 Policy: 1.3.6.1.4.1.100 15.1.1 CPS: https://www.sk.ee/CPS Policy: 1.3.6.1.4.1.100 15.1.2 Policy: 1.3.6.1.4.1.100 15.1.3 Policy: 1.3.6.1.4.1.100 15.1.4	Certificate Sign, CRL Sign	OCSP Signing, TLS Web Client Authentication, E-mail Protection	17 Dec 2015 12:38:43 GMT to 17 Dec 2030 23:59:59 GMT
ESTEID2018	CN = EE-GovCA2018, O = SK ID Solutions AS, C = EE, OI = NTREE-10747013	CN = ESTEID2018, O = SK ID Solutions AS, C = EE, OI = NTREE-10747013	26DFC32284C 20462BB632D 1F03AA82EE0 0B5F170	C45AE81AC8 B5ED5D80652 13FD3DC250 C7B3277368A 3E97BD8299E FFAF8B65E31	7547FAAC147 44B8B5BA366 D4FE6655ED	ecdsa-with-SHA512	521	Policy: 0.4.0.2042.1.2 Policy: 0.4.0.194112.1.2 Policy: 1.3.6.1.4.1.513 61.1.1.1 CPS: https://www.sk.ee/CPS Policy: 1.3.6.1.4.1.513 61.1.1.2 Policy: 1.3.6.1.4.1.514 55.1.1.1 Policy:	Certificate Sign, CRL Sign	OCSP Signing, TLS Web Client Authentication, E-mail Protection	20 Sep 2018 09:22:28 GMT to 05 Sep 2033 09:11:03 GMT

								1.3.6.1.4.1.513 61.1.1.5 Policy: 1.3.6.1.4.1.513 61.1.1.6 Policy: 1.3.6.1.4.1.513 61.1.1.7 Policy: 1.3.6.1.4.1.513 61.1.1.3 Policy: 1.3.6.1.4.1.513 61.1.1.4 Policy: 1.3.6.1.4.1.513 61.1.1.8 Policy: 1.3.6.1.4.1.513 61.1.1.9 Policy: 1.3.6.1.4.1.513 61.1.1.10 Policy: 1.3.6.1.4.1.513 61.1.1.11 Policy: 1.3.6.1.4.1.513 61.1.1.12 Policy: 1.3.6.1.4.1.513 61.1.1.13 Policy: 1.3.6.1.4.1.513 61.1.1.14 Policy: 1.3.6.1.4.1.513 61.1.1.15 Policy: 1.3.6.1.4.1.513 61.1.1.16 Policy: 1.3.6.1.4.1.513 61.1.1.17 Policy:			
--	--	--	--	--	--	--	--	--	--	--	--

								1.3.6.1.4.1.513 61.1.1.18 Policy: 1.3.6.1.4.1.513 61.1.1.19 Policy: 1.3.6.1.4.1.513 61.1.1.20 Policy: 1.3.6.1.4.1.514 55.1.1.2 Policy: 1.3.6.1.4.1.514 55.1.1.3 Policy: 1.3.6.1.4.1.514 55.1.1.4 Policy: 1.3.6.1.4.1.514 55.1.1.5 Policy: 1.3.6.1.4.1.514 55.1.1.6			
--	--	--	--	--	--	--	--	--	--	--	--

1.3 Root CA:

Identification of the Sub-CA	Issuer Distinguished Name	Subject Distinguished Name	SHA-1 fingerprint	SHA-256 fingerprint	Certificate serial number	Signature algorithm	Key length	Certificate Policies	KeyUsage	EKU	Validity
EE Certification Centre Root CA	E = pki@sk.ee , CN = EE Certification Centre Root CA, O = AS Sertifitseerimiskeskus, C = EE	E = pki@sk.ee , CN = EE Certification Centre Root CA, O = AS Sertifitseerimiskeskus, C = EE	C9A8B9E755805E58E35377A725EBAFC37B27CCD7	3E84BA4342908516E77573C0992F0979CA084E4685681FF195CCBA8A229B8A76	5480F9A073ED3F004CCA89D8E371E64A	sha1WithRSA-Encryption	2048		Certificate Sign, CRL Sign	TLS Web Client Authentication, TLS Web Server Authentication, Code Signing, E-mail Protection, Time Stamping, OCSP Signing	30 Oct 2010 10:10:30 GMT to 17 Dec 2030 23:59:59 GMT
EE-GovCA2018	CN = EE-GovCA2018, O = SK ID Solutions AS, C = EE, OI = NTREE-10747013	CN = EE-GovCA2018, O = SK ID Solutions AS, C = EE, OI = NTREE-10747013	A79E631B21C902BD4C14C01D2C7D721A635D888E	F164ABE507407408292AF1FA368842B7482DD0D346D79EE8ECB94467D57579A0	30B3B0957A11D2815B8F9DA7991B277B	ecdsa-with-SHA512	521	Policy: 0.4.0.2042.1.2 Policy: 0.4.0.194112.1.2 Policy: 1.3.6.1.4.1.513.61.1.1.1 CPS: https://www.sk.ee/CPS Policy: 1.3.6.1.4.1.513.61.1.1.2 Policy: 1.3.6.1.4.1.514.55.1.1.1 Policy: 1.3.6.1.4.1.513.61.1.1.5 Policy: 1.3.6.1.4.1.513.61.1.1.6 Policy: 1.3.6.1.4.1.513.61.1.1.7 Policy: 1.3.6.1.4.1.513	Certificate Sign, CRL Sign	OCSP Signing, TLS Web Client Authentication, E-mail Protection, TLS Web Server Authentication	05 Sep 2018 09:11:03 GMT to 05 Sep 2033 09:11:03 GMT

								61.1.1.3 Policy: 1.3.6.1.4.1.513 61.1.1.4 Policy: 1.3.6.1.4.1.513 61.1.1.8 Policy: 1.3.6.1.4.1.513 61.1.1.9 Policy: 1.3.6.1.4.1.513 61.1.1.10 Policy: 1.3.6.1.4.1.513 61.1.1.11 Policy: 1.3.6.1.4.1.513 61.1.1.12 Policy: 1.3.6.1.4.1.513 61.1.1.13 Policy: 1.3.6.1.4.1.513 61.1.1.14 Policy: 1.3.6.1.4.1.513 61.1.1.15 Policy: 1.3.6.1.4.1.513 61.1.1.16 Policy: 1.3.6.1.4.1.513 61.1.1.17 Policy: 1.3.6.1.4.1.513 61.1.1.18 Policy: 1.3.6.1.4.1.513 61.1.1.19 Policy: 1.3.6.1.4.1.513 61.1.1.20 Policy: 1.3.6.1.4.1.514			
--	--	--	--	--	--	--	--	---	--	--	--

								55.1.1.2 Policy: 1.3.6.1.4.1.514 55.1.1.3 Policy: 1.3.6.1.4.1.514 55.1.1.4 Policy: 1.3.6.1.4.1.514 55.1.1.5 Policy: 1.3.6.1.4.1.514 55.1.1.6 Policy: 1.3.6.1.4.1.513 61.10.1 CPS: https://www.sk.ee/CPS			
--	--	--	--	--	--	--	--	--	--	--	--

2. Certification Scheme

TÜV AUSTRIA CERT GMBH has been accredited as Conformity Assessment Body according to eIDAS Regulation¹, Article 3(18) competent to carry out conformity assessments of qualified trust service provider and the qualified trust services they provide. The accreditation is issued by "Akkreditierung Austria" with registration No. 0943 according to EN ISO/IEC 17065 for products, processes and services taking into consideration ETSI EN 319 403-1 V2.3.1:2020 (successor of ETSI EN 319 403 V2.2.2:2015), covering the Conformity Assessment Requirements as listed under 3. below.

The conformity assessment for this certification has been performed by TÜV TRUST IT which is a registered audit body at TÜV AUSTRIA CERT, following the Conformity Assessment Scheme of TÜV AUSTRIA CERT, Rev 05 as of 2021-11-11.

3. Conformity Assessment Requirements

As defined in the eIDAS Regulation¹ the following requirements were identified as relevant for the trust service stated on the front page of this certificate and assessed during the conformity assessment.

Requirements as stated in REGULATION (EU) No 910/2014 (eIDAS) valid for trust services:

- Data processing and protection:
Art. 5 (1),
- General provisions:
Art. 13 (2) and (3), Art. 15,
- Supervision:
Art. 19 (1), Art. 19 (2),

Qualified trust services:

- General:
Art. 20, Art. 21 (1) and (3), Art. 23 (1), Art. 23 (2),
- Requirements for qualified trust service provider:
Art. 24 (1)a, (2)a-j, (3) and (4),

Service specific requirements:

- Qualified certificates for electronic signatures:
Art. 28 (1) to (5), Art. 29 (1), Art. 30 (1), Annex I.

Furthermore, the requirements of para. 4,5,16,17,18,19 as well as para. 20 of the Estonian eIDAS implementation law "Electronic Identification and Trust Services for Electronic Transactions Act" (as of 2016-10-12, updated and in force from 2021-10-25) have been considered.

4. Conformity Assessment Result Summary

The following results were gained throughout the Conformity Assessment of the services listed in section 1. above:

- The services covered fulfil the applicable conformity assessment requirements.
- The certification requirements defined in the certification scheme are fulfilled.

END OF CERTIFICATE

¹ REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS)