CERTIFICATE

TÜV AUSTRIA

The certification body of TÜV AUSTRIA GMBH herewith grants certification to

SK ID Solutions AS
Pärnu mnt 141
11314 Tallinn
Estonia

confirming that the trust service

EID-SK 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
TA235224388_CAR_A2.

The certificate comprises an appendix of 6 pages.

Certificate-Reg.-Nr. TA235224388   begin of certificate validity: 2024-05-28
                                          end of certificate validity: 2026-05-28

Certification body   Vienna, 2024-09-30
of TÜV AUSTRIA GMBH

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

Akkreditierung Austria
A
0944
ISO/IEC 17065

Online Verification

www.tuv.at/certcheck

045914-23-9

Amendment to the certificate appendix

This is an amendment to the already existing certification. Reason of the amendment is:

Amendment reason:	☐ Surveillance Conformity Assessment
	☒ Issuance of two new Issuing CAs to be used for new Smart-ID accounts. (further details are available in the CAR).

The details of the amendment are described in the following sections.

1. Assessment and Certification Details

Subject of this amendment conformity assessment as of 06.06.2024 for the service "EID-SK qualified certificates for electronic signatures" documented with assessment report No. TA235224388_CAR, version 2.1 as of 2024-03-20, TA235224388_CAR_A1, version 2.2 as of 2024-06-06 and this current amendment assessment report No. TA235224388_CAR_A2, version 2.3 as of 2024-09-30, were the following documents of the operator and the PKI structure as listed below:

1.1. Operator Documents assessed during the amendment conformity assessment (Amendment 2)

TSPS	SK ID Solutions AS Trust Services Practice Statement
	Version 12.0 as of 2024-01-15
CPS EID	SK ID Solutions AS - EID-Q SK Certification Practice Statement
	Version 15.0 as of 2024-11-27
CP_QSID	SK ID Solutions AS - Certificate Policy for Qualified Smart-ID
	OID: 1.3.6.1.4.1.10015.17.2
	Version 10.0 as of 2024-04-15
CPR_SID	Certificate and OCSP Profile for Smart-ID
	Version 4.7 as of 2024-11-27
TAC_QSID	Terms and Conditions for Use of Certificates of qualified Smart-ID
	Version as of 2024-04-15
TAC_SA	General Terms of Subscriber Agreement
	Version 4.1 as of 2023-07-01
CPR_CA	Certificate, OCSP and CRL Profile for Root, Intermediate CA and timestamping service Issued by SK
	Version 3.4 as of 2023-11-08

1.2. Operator Documents assessed during the amendment conformity assessment (Amendment 1)

The public documents were not changed as the update of the Smart-ID QSCD with new HSMs did not require any update in the documents provided for the conformity assessment for Amendment 1.

1.3. Operator Documents assessed during the re-certification conformity assessment

(documented with report No. TA235223860_CAR, version 2.1 as of 2022-03-18)

TSPS	SK ID Solutions AS Trust Services Practice Statement Version 12.0 as of 2024-01-15
CP MID	SK ID Solutions AS - Certificate Policy for Mobile-ID OID 1.3.6.1.4.1.10015.18.1 Version 4.1 as of 2024-04-15
CPS EID	SK ID Solutions AS - EID-Q SK Certification Practice Statement Version 14.0 as of 2024-04-15
CPR MID	SK ID Solutions - Certificate and OCSP Profile for Mobile-ID Version 2.1 as of 2024-04-15
TAC MID	Terms and Conditions for Use of Certificates of Mobile-ID valid as of 2022-07-02
CP_QSID	SK ID Solutions AS - Certificate Policy for Qualified Smart-ID OID: 1.3.6.1.4.1.10015.17.2 Version 10.0 as of 2024-04-15
CPR_SID	Certificate and OCSP Profile for Smart-ID Version 4.6 as of 2024-04-15
TAC_QSID	Terms and Conditions for Use of Certificates of qualified Smart-ID Version as of 2024-04-15
TAC_SA	General Terms of Subscriber Agreement Version 4.1 as of 2023-07-01
CPR_CA	Certificate, OCSP and CRL Profile for Root, Intermediate CA and timestamping service Issued by SK Version 3.4 as of 2023-11-08

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
EID-SK 2016	CN = EE Certification Centre Root CA, O = AS Sertifitseerimis keskus, C = EE	CN = EID-SK 2016, O = AS Sertifitseerimis keskus, C = EE	9F73385C30A 4D023CC1DD A47031FC583 7B01C1E7	E73F1F19A44 59A6067A45E 84DB585D6C1 DF8F12A739D 733F5B28996 546F1875A	3B803A6B69C 12A8C57C550 05311BC4DA	sha384WithRS AEncryption	4096	Policy 0.4.0.194112.1 .2 Policy 0.4.0.194112.1 .0 Policy 0.4.0.2042.1.2	Certificate Sign, CRL Sign	OCSP Signing, TLS Web Client Authentication, E-mail Protection	30 Aug 2016 09:21:09 GMT to 17 Dec 2030 23:59:59 GMT
SK ID Solutions EID-Q 2021E	CN = SK ID Solutions ROOT G1E, O = SK ID Solutions AS, C = EE, OI =NTREE-10747013	CN = SK ID Solutions EID-Q 2021E, O = SK ID Solutions AS, C = EE, OI = NTREE-10747013	2ABBC0536D2 20FC3CF85D3 E37D29C451F 0B80B2F	3B355E9B664 DF0FA3FCC9 222725A9411 D72207E318A C9EF1028B21 1FE03A1052	79CB98F10B4 84AAA615AEE E0235060E3	ecdsa-with-SHA384	384	Policy X509v3 Any Policy	Certificate Sign, CRL Sign		04 Oct 2021 12:09:04 GMT to 04 Oct 2036 12:09:04 GMT
SK ID Solutions EID-Q 2021R	CN = SK ID Solutions ROOT G1R, O = SK ID Solutions AS, C = EE, OI =NTREE-10747013	CN = SK ID Solutions EID-Q 2021R, O = SK ID Solutions AS, C = EE, OI = NTREE-10747013	E1B72C83EB1 2380E88AFE8 0096E17A456 13EE0F3	089DD33525C CB996C5F1D EBEDDC17F1 B3C0C4DF17 C9A993A32CA 05570147BF0 3	3828C481F7E 3DE7F615AF1 C21A8F1A15	sha384WithRS AEncryption	4096	Policy X509v3 Any Policy	Certificate Sign, CRL Sign		04 Oct 2021 12:21:22 GMT to 04 Oct 2036 12:21:22 GMT
SK ID Solutions EID-Q 2024E	CN = SK ID Solutions ROOT G1E, O = SK ID Solutions AS, C = EE, OI =NTREE-10747013	CN = SK ID Solutions EID-Q 2024E, O = SK ID Solutions AS, C = EE, OI = NTREE-10747013	41949AC7C02 A614F32D80B F6C972F712A 78A8F68	95C4E7E2B5C 2617E877442 F4276146F889 5CEE8BAA33 340EFA03E45 A66D62D25	2459A405C42 F43440E86F7 1E52CF2CB77 25A148E	ecdsa-with-SHA384	384	Policy: X509v3 Any Policy Policy: X509v3 Certificate Policies	Certificate Sign, CRL Sign		02 Jul 2024 08:34:58 GMT to 29 Jun 2039 08:34:57 GMT

| SK ID Solutions EID-Q 2024R | CN = SK ID Solutions ROOT G1R, O = SK ID Solutions AS, C = EE, OI =NTREE-10747013 | CN = SK ID Solutions EID-Q 2024R, O = SK ID Solutions AS, C = EE, OI = NTREE-10747013 | 04B89D840DD E461C47B395 C66156652AD 76D53A8 | C66244D29CF 8033B1D4A6F 16D8B0F9DB7 B27CDABCE5 AD0C05EFF70 EDA1257235 | 5CCCBFCF81 DA307221547 880B9FB4A04 87C7A89C | sha384WithRS AEncryption | 4096 | Policy: X509v3 Any Policy Policy: X509v3 Certificate Policies | Certificate Sign, CRL Sign | | 02 Jul 2024 08:40:24 GMT to 29 Jun 2039 08:40:23 GMT |

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 Sertifitseerimis keskus, C = EE	E = pki@sk.ee, CN = EE Certification Centre Root CA, O = AS Sertifitseerimis keskus, C = EE	C9A8B9E7558 05E58E35377 A725EBAFC37 B27CCD7	3E84BA43429 08516E77573 C0992F0979C A084E468568 1FF195CCBA8 A229B8A76	5480F9A073E D3F004CCA89 D8E371E64A	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
SK ID Solutions ROOT G1R	CN = SK ID Solutions ROOT G1R, O = SK ID Solutions AS, C = EE, OI =NTREE-10747013	CN = SK ID Solutions ROOT G1R, O = SK ID Solutions AS, C = EE, OI = NTREE-10747013	2D1A83D4559 7EAC6E21CA BA2CBCD0B5 69C9009D4	D012DA1A621 93928C5B4D8 9D2A72495B1 F77EA5D54F2 3956BC1DF2F 75528FEFB	7465CC9B184 F0EED615AE AB5E6CF4B29	sha384WithRS AEncryption	4096		Certificate Sign, CRL Sign		04 Oct 2021 11:51:17 GMT to 04 Oct 2041 11:51:17 GMT
SK ID Solutions ROOT G1E	CN = SK ID Solutions ROOT G1E, O = SK ID Solutions AS, C = EE, OI =NTREE-10747013	CN = SK ID Solutions ROOT G1E, O = SK ID Solutions AS, C = EE, OI = NTREE-10747013	4AAB4198821 89B965B782D FB6A5241104 8EA9E9A	A272DE102A8 038F7E100EA CFB6DB1C93 0D3CB9F51D7 6B218DE3A4A 433BCFD182	4A668BD6E6E 20B71615AE9 42221277FB	ecdsa-with-SHA512	521		Certificate Sign, CRL Sign		04 Oct 2021 11:45:06 GMT to 04 Oct 2041 11:45:06 GMT

2. Certification Scheme

TÜV AUSTRIA GMBH has been accredited as Conformity Assessment Body according to eIDAS Regulation[1], 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 initial conformity assessment for this certification has been performed by TÜV TRUST IT which is a registered audit body at TÜV AUSTRIA GMBH, following the Conformity Assessment Scheme of TÜV AUSTRIA GMBH, Rev 06 as of 2023-06-14.

The amendment conformity assessment A1 for this certification has been performed by TÜV TRUST IT which is a registered audit body at TÜV AUSTRIA GMBH, following the Conformity Assessment Scheme of TÜV AUSTRIA GMBH, Rev 07 as of 2024-01-29.

The amendment conformity assessment A2 for this certification has been performed by TÜV TRUST IT which is a registered audit body at TÜV AUSTRIA GMBH, following the Conformity Assessment Scheme of TÜV AUSTRIA GMBH, Rev 07 as of 2024-01-29.

3. Conformity Assessment Requirements

As defined in the eIDAS Regulation[1] 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. 23 (1), Art. 23 (2),
- Requirements for qualified trust service provider:
  Art. 24 (2)a–j,

Service specific requirements:
- Qualified certificates for electronic signatures:
  Art. 24 (1) a, c and d, Art. 24 (2) k, Art. 24 (3) and (4), Art. 28 (1) to (5), Art. 29 (1), Annex II.

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 2023-03-13) 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)