Document Information	
Name	**Certificate and OCSP Profile for Smart-ID**
Version number	**4.5**
Version No. and date	Changes
17.02.2022 4.5	• Chapter 2.1 - added random to certificate serial number description
12.05.2021 4.4	• Chapter 2.2 - changed sk.ee domain to skidsolutions.eu; • chapter 2.1 - change of the Issuer Distinguished Name attribute CN value and description; • Subject Distinguished Name attribute CN may not contain serial number; • chapter 2.2.2 - added extension Subject Directory Attributes using dateOfBirth; Specified QCP-n-qscd issuance enforce date; • chapter 6 Appendix A – removed country list for natural identity types PNO, PAS and IDC; • amended document overall wording and references.
30.06.2020 4.3	• Chapter 2.1 - updated Serial Number, surname, given name and common name attribute description in Subject DN; • Chapter 2.2.2 - specified QCP-n-qscd status date; • Added Chapter 3 - Profile of Certificate Revocation List; • Chapter 4 - removed OU field from OCSP ResponderID value; • Added Chapter 4 - "Appendix A" describes allowed country codes; • Changed sk.ee domain to skidsolutions.eu
17.10.2019 4.2	• Chapter 2 - improved certificate subject DN descriptions • Chapter 3 - added nonce extension support for OCSP; corrected OCSP • Responder ID value • Chapter 4 - updated ETSI document versions in "Referred and Related Documents"
24.10.2018 4.1	• AuthorityKeyIdentifier and SubjectKeyIdentifier descriptions. • Chapter 3 - new extensions are added: Archive Cutoff and Extended Revoked Definition; CertStatus description is renewed. • Chapter 2.1 – added additional RSA key sizes 4095, 4094;
06.07.2018 4.0	• Clause 2.2.2 - added id-etsi-qcs-QcSSCD attribute under Qualified • Certificate Statement extension, as the digital signature certificate is in accordance with eIDAS; • Clause 2.1 – added additional RSA key sizes; • Clause 2.2.3 - changed policy OID 0.4.0.194112.1.0 (QCP-n) to 0.4.0.194112.1.2 (QCP-n-qscd) in digital signing certificate; • Added reference to ETSI EN 411-1 standard to clauses 2 and 4 of this profile.
03.05.2017 3.0	• Changed Chapter 2.1 – removed O and OU attributes from certificate subject.
01.04.2017 2.0	• Clause 2.2.1 – changed caIssuers URL's; • Clause 2.2.2 – removed qcStatements from Qualified certificate, digital authentication profile; added attribute idqcs-pkixQCSyntax-v2.
09.02.2017 1.1	• Changed Chapter 2.1 added certificate validity • Changed Chapter 2.1 "Organisation" field description and added certificate validity period; • Changed Chapter 2.2.2 structure and removed qcStatements from Non-Qualified Smart-ID profile • Changed name AS Sertifitseerimiskeskus to SK ID Solutions AS throughout the document • Removed QCP-n-qscd; • Changed Smart-ID Advanced certificate to Non-qualified Smart-ID certificate
01.01.2017 1.0	• Initial document.
Effective from date	17.02.2022

1. Introduction

The document in hand describes the profiles of the digital certificates used by the Smart-ID System.

Terms and Abbrevations

Refer to Certification Practice Statement [1].

2. Technical Profile of the Certificate

Natural person certificate is compiled in accordance with the X.509 version 3, IETF RFC 5280 [4], ETSI EN 319 412-2 [6], ETSI EN 411-1 [12] and ETSI EN 411-2 (chapter 6.6) [10]

2.1. Certificate Body

Field	OID	Mandatory	Value	Changeable	Description
Version		yes	V3	no	Certificate format version
serialNumber		yes		no	Unique and random serial number of the certificate
Signature Algorithm	1.2.840.113549.1.1.11	yes	sha256WithRSAEncryption	no	Signature algorithm in accordance to RFC 5280
Issuer Distinguished name					
common Name (CN)	2.5.4.3	yes	EID-SK 2016 or NQ-SK 2016		Certificate authority name
organizationIdentifier	2.5.4.97	yes	NTREE-10747013	no	Identification of the issuer organisation different from the organisation name. Certificates may include one or more semantics identifiers as specified in clause 5.1.4 of ETSI EN 319 412-1.
Organization (O)	2.5.4.10	yes	AS Sertifitseerimiskeskus		Issuer organisation name. Both names mark the same legal entity. Name “AS Sertifitseerimiskeskus” is used only in issuing CA’s certified by EE Certification Centre Root CA.
Country (C)	2.5.4.6	yes	EE		Country code: EE - Estonia (2 character ISO 3166 country code [3])
notBefore		yes			First date of certificate validity.

notAfter		yes			The last date of certificate validity. Generally date of issuance + 1095 days (3 years).
Subject Distinguished Name		yes		yes	Unique subject name in the infrastructure of certificates.
serialNumber (S)	2.5.4.5	yes		yes	Certificate holder's identifier as specified in clause 5.1.3 of ETSI EN 319 412-1 [5]. Allowed country codes are described in chapter 6 [17]. Examples: PASUA-PU12345 PNOEE-47101010033 IDCUA- 47101010033
givenName (G)	2.5.4.42	yes		yes	Person given names in UTF8 format according to RFC5280. When subscriber given name is not present, it's replaced with hyphen-minus "-" (Unicode character U+2212)
surname (SN)	2.5.4.4	yes		yes	Person surnames in UTF8 format according to RFC5280. Wh en subscriber surname is not present, it's replaced with hyphen- minus "-" (Unicode character U+2212)
commonN me (CN)	2.5.4.3	yes	CN=SN, G, S or CN=SN, G	yes	Common name structure may vary depending on the issued certificate. Comma-separated surnames, given name and serial number or surnames, given name without serial number. See examples below: Example 1: CN=JÕEORG, JAAK-KRISTJAN,38001085718 Example 2: CN=JÕEORG, JAAK-KRISTJAN

Country (C)	2.5.4.6	yes		yes	Country of origin in accordance with ISO 3166 [3] . Allowed countries in accordance with identity types are described in Appendix A [17]
Subject Public Key		yes	RSA 6144, 6143, 6142	yes	RSA algorithm in accordance with RFC 4055 [8]

2.2. Certificate Extensions

2.2.1. Extensions

The following table describes the extensions used in the certificates:

Extension	OID	Values and Limitations	Criticality	Mandatory
BasicConstraints	2.5.29.19	Subject Type=End Entity Path Length Constraint=None	Non- critical	yes
CertificatePolicies	2.5.29.32	Refer to p 2.2.3 "Certificate policy"	Non- critical	yes
SubjectAltName	2.5.29.17	Refer to p 2.2.2 "Variable Extensions"	Non- critical	yes
KeyUsage	2.5.29.15	Refer to p 2.2.2 "Variable Extensions"	Critical	yes
ExtendedKeyUsage	2.5.29.37	Refer to p 2.2.2 "Variable Extensions"	Non- critical	yes
Qualified Certificate Statement	1.3.6.1.5.5.7.1.3	Refer to p 2.2.2 "Variable Extensions	Non- critical	yes
AuthorityKeyIdentifier	2.5.29.35	SHA-1 hash of the public key	Non- critical	yes
SubjectKeyIdentifier	2.5.29.14	SHA-1 hash of the public key	Non- critical	yes
authorityInfoAccess	1.3.6.1.5.5.7.1.1		Non- critical	yes
id-ad-ocsp	1.3.6.1.5.5.7.48.1	http://aia.sk.ee/eid2016 or http://aia.sk.ee/nq2016		yes
id-ad-calssuers	1.3.6.1.5.5.7.48.2	https://c.sk.ee/EID-SK_2016.der.crt or http://c.sk.ee/NQ-SK_2016.der.crt		yes

2.2.2. Variable Extensions

Following variable extensions for Smart-ID.

	Smart-ID Qualified certificate		**Smart-ID Non-Qualified certificate**	
Extension	**DIGITAL AUTHENTICATION**	**DIGITAL SIGNATURE [14]**	**DIGITAL AUTHENTICATION**	**DIGITAL SIGNATURE**
subjectAltName	-			
directoryName	CN=<*Smart-ID account number*>			
SubjectDirectoryAttributes [1]	According to ETSI EN 319 412-2 V2.2.1 [12]			
dateOfBirth	The extension attributes according to RFC3739 clausel 3.2.2 [13]			
KeyUsage	digitalSignature, keyEncipherment ,dataEncipherment	nonRepudiation	digitalSignature , keyEncipherment, dataEncipherment	nonRepudiation
ExtendedKeyUsage	id-kp-clientAuth(1.3.6.1.5.5.7.3.2)		id-kp-clientAuth(1.3.6.1.5.5.7.3.2)	
Qualified Certificate Statement [12]	-	yes	-	-
id-etsi-qcs-QcComplian ce	-	yes	-	-
id-etsi-qcs-QcSSCD [15]	-	yes	-	-
id-etsi-qcs-QcType [13]	-	1	-	-
id-etsi-qcs-QcPDS	-	https://skidsolutions.eu/en/repository/conditions-for-use-of-certificates/	-	-
id-qcs-pkixQCSynta x-v2	-	id-etsi-qcs-semanticsId-Natural	-	

[12] - qcStatements according to clause 6.6.1 specified in ETSI EN 319 411-2 [10]

[13] - Types according to clause 4.2.3 specified in ETSI EN 319 412-5 [9]

[14] - Qualified Electronic Signatures compliant with eIDAS [11]

[15] - QCP-n policy used until 07.11.2018. Since 08.11.2018 QCP-n-qscd is used accordingly ETSI EN 319 411-2 [10]

[1] Extension is optional.

2.2.3. Certificate Policy

Profile	PolicyIdentifier (authentification)	PolicyIdentifier (digital signature)	PolicyQualifier
Smart-ID Qualified certificate	1.3.6.1.4.1.10015.17.2 0.4.0.2042.1.2	1.3.6.1.4.1.10015.17.2 0.4.0.194112.1.2 *[16]*	https://skidsolutions.eu/en/repository/CPS/
Smart-ID Non-Qualified certificate	1.3.6.1.4.1.10015.17.1 0.4.0.2042.1.1	1.3.6.1.4.1.10015.17.1 0.4.0.2042.1.1	https://skidsolutions.eu/en/repository/CPS/

[16] -Issuance of the Certificates for Q Smart-ID under the Policy QCP-n was performed until 07.11.2018. After that, qualified certificate is compiled in accordance with the Policy QCP-n-qscd.

3. Profile of Certificate Revocation List

Certificate Revocation List (CRL) for issuing CA's EID-SK 2016 and NQ-SK 2016 is not applicable.

4. OCSP Profile

OCSP v1 according ETSI EN 319 411-1 (chapter 6.6.3) [12] and RFC 6960 [7].

Field	Mandatory	Value	Description
ResponseStatus	yes	0 for successful or error code	Result of the query.
ResponseBytes			
ResponseType	yes	id-pkix-ocsp-basic	Type of the response.
Response Data	yes		
Version	yes	1	Version of the response format.
Responder ID	yes	C = EE O = SK ID Solutions AS 2.5.4.97 = NTREE-10747013 CN=EID-SK 2016 AIA OCSP RESPONDER YYYYMM or CN=NQ-SK 2016 AIA OCSP RESPONDER YYYYMM	Distinguished name of the OCSP responder. Note: the Common Name will vary each month and includes the month in YYYYMM format.
Produced At	yes		Date when the OCSP response was signed.
Responses	yes		
CertID	yes		CertID fields accordance with RFC 6960 [7] clause 4.1.1.
Cert Status	yes		Status of the certificate as follows: *Good* - certificate is issued and has not been revoked or suspended *Revoked* - certificate is revoked, suspended or not issued by this CA *Unknown* - the issuer of certificate is unrecognized by this OCSP responder
Revocation Time	no		Date of revocation of certificate, for non-issued certificate revocation time is January 1, 1970.
Revocation Reason	no		Code for revocation Reason according to RFC 5280 [4].
This Update	yes		Date when the status was queried from database.
Archive Cutoff	no	CA's certificate "valid from" date.	ArchiveCutOff date - the CA's certificate "valid from" date. Pursuant to RFC 6960 [7] clause 4.4.4.

Extended Revoked Definition	no	NULL	Identification that the semantics of certificate status in OCSP response conforms to extended definition in RFC 6960 clause 2.2 [7]
Nonce	no		Value is copied from request if it is included. Pursuant to RFC 6960 [7] clause 4.4.1.
Signature Algorithm	yes	Sha256WithRSAEncryption or Sha512WithRSAEncryption	Signing algorithm pursuant to RFC 5280 [4].
Signature	yes		
Certificate	yes		Certificate corresponding to the private key used to sign the response.

5. Referred and Related Documents

1. SK ID Solutions AS - EID-SK Certification Practice Statement, published https://www.skidsolutions.eu/en/repository/CPS/;
2. SK ID Solutions AS- Certificate Policy for Qualified Smart-ID, published https://www.skidsolutions.eu/en/repository/CP/;
3. ISO 3166 Codes, published: http://www.iso.org/iso/country_codes;
4. RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and CertificateRevocation List (CRL) Profile;
5. ETSI EN 319 412-1 v1.4.4 Electronic Signatures and Infrastructures (ESI) Certificate Profiles; Part 1: Overview and common data structures;
6. ETSI EN 319 412-2 v2.2.1 Electronic Signatures and Infrastructures (ESI) Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;
7. RFC 6960 – X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP;
8. RFC 4055 - Additional Algorithms and Identifiers for RSA Cryptography for use in the

   Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
9. ETSI EN 319 412-5 v2.3.1 Electronic Signatures and Infrastructures (ESI) Certificate Profiles; Part 5: QCStatements.
10. ETSI EN 319 411-2 v2.4.1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates;
11. eIDAS - 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 inthe

    internal market and repealing Directive 1999/93/EC;
12. ETSI EN 319 411-1 v1.3.1 Electronic Signatures and Infrastructures (ESI);Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
13. Internet X.509 Public Key Infrastructure: Qualified Certificates Profile

6. Appendix A

6.1. Allowed countries in semantics identifiers

The serialNumber attribute can contain a national identity card number, personal number or passport number. The semantics identifier (clause 5.1.3 of ETSI EN 319 412-1 [5]) in the following clauses uses ISO 3166 [3] country codes to specify the country where the identifier is registered.

Natural identity type „**PNO**“ is used when national level personal identity number is available.

Natural identity type „**PAS**“ is used for passport number and identity type „**IDC**“ is used for national identity card number