Certificate and OCSP Profile for ID-1 Format Identity Documents Issued by the Republic of Estonia

Version 1.0

1.November 2018

Version History		
Date	**Version**	**Changes**
01.11.2018	1.0	First public version

1. Introduction

The document describes the profiles of the digital certificates loaded to the ID-1 format identity documents (comply to the ISO/IEC 7816 [3]),

issued by the Republic of Estonia and OCSP responses, issued by CA ESTEID2018. This document complements Certificate Policy [2] and Certification Practice Statement [1].

Chapter 2 describes the technical details and delivers the examples of the certificates.

This document does not address other data stored in the personal identification documents.

There are two types of certificates loaded to the Documents:

1. Qualified Electronic Signature Certificate is intended for:
   - creating Qualified Electronic Signatures compliant with eIDAS [11].

2. Authentication Certificate is intended for:
   - Authentication,
   - Encryption,
   - secure e-mail

The certificates are being issued by SK ID Solutions AS.

1.1. Terms and Abbrevations

Refer to p 1.6 in Certification Practice Statement [1] and Certificate policy [2].

2. Technical Profile of the Certificate

Natural person´s certificate is in compliance with the X.509 version 3, IETF RFC 5280 [5], ETSI EN 319 412-2 [7] and ETSI EN 319 411-2 (ch apter 6.6) [13].

2.1. Certificate Body

Field	OID	Mandatory	Value	Changeable	Description

Version		yes	V3	no	Certificate format version.
Serial Number		yes		no	Unique serial number of the certificate.
Signature Algorithm	1.2.840.10045.4.3.4	yes	ecdsa-with-sha512	no	Signature algorithm in accordance to RFC 5480 [10] .
Issuer Distinguished name					
Common Name (CN)	2.5.4.3	yes	ESTEID2018		Certificate authority name.
Organisation Identifier	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 [6] .
Organisation (O)	2.5.4.10	yes	SK ID Solutions AS		Issuer organisation name.
Country (C)	2.5.4.6	yes	EE		Country code: EE - Estonia (2 character ISO 3166 country code [4]).
Valid from		yes			First date of certificate validity.
Valid to		yes			The last date of certificate validity. 1826 days.
Subject Distinguished Name		yes		yes	Unique subject name in the infrastructure of certificates.
Serial Number (S)	2.5.4.5	yes		yes	Personal identity code as specified in clause 5.1.3 of ETSI EN 319 412-1 [6].

Given Name (G)	2.5.4.42	yes		yes	Person´s given name(s) in UTF8 format. Given Name lenght does not meet the RFC5280 [5] standard (ub-given-name-length INTEGER ::= 16) Name shortening process is managed by Estonian Police and Border Guard Board.
Surname (SN)	2.5.4.4	yes		yes	Person's surname(s) in UTF8 format according to RFC5280 [5]. Name shortening process is managed by Estonian Police and Border Guard Board.
Common Name (CN)	2.5.4.3	yes		yes	Comma-separated surnames, given names and personal identity code. Common Name lenght does not meet the RFC5280 [5] standard (ub-common-name-length INTEGER ::= 64) Example: JÕEORG, JAAK-KRISTJAN,38001085718
Country (C)	2.5.4.6	yes		yes	Country of origin in accordance with ISO 3166 [4].
Subject Public Key		yes	NIST P-384, brainpool P512r1	yes	ECC algorithm created in accordance with RFC 5480 [10] or brainpoolP512r1 in accordance with RFC 5639 [14]

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
Basic Constraints	2.5.29.19	Subject Type=End Entity Path Length Constraint=None	Non-critical	yes
Certificate Policies	2.5.29.32	Refer to p 2.2.3 "Certificate policy".	Non-critical	yes

Subject Alternative Name	2.5.29.17	The e-mail address (rfc822Name, according to RFC5280 [5]) of the certificate owner is presented in this field. The e-mail address is included only in the certificate facilitating digital authentication. E-mail address form and logic is managed by Estonian Police and Border Guard Board.	Non-critical	yes
Key Usage	2.5.29.15	Refer to p 2.2.2 "Variable Extensions".	Critical	yes
Extended Key Usage	2.5.29.37	Refer to p 2.2.2 "Variable Extensions".	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
Authority Information Access	1.3.6.1.5. 5.7.1.1		Non-critical	yes
ocsp	1.3.6.1.5. 5.7.48.1	http://aia.sk.ee/esteid2018		yes
calssuers	1.3.6.1.5. 5.7.48.2	http://c.sk.ee/esteid2018.der.crt		yes

2.2.2. Variable Extensions

Extension	DIGITAL AUTHENTICATION	DIGITAL SIGNATURE
Key Usage	DigitalSignature, KeyAgreement	nonRepudiation
Extended Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)	-
Qualified Certificate Statement [17]	-	-
id-etsi-qcs-QcCompliance	-	yes
id-etsi-qcs-QcSSCD	-	yes
id-etsi-qcs-QcType [18]	-	1
id-etsi-qcs-QcPDS	https://sk.ee/en/repository/conditions-for-use-of-certificates/	https://sk.ee/en/repository/conditions-for-use-of-certificates/

17 - qcStatements according to clause 6.6.1 specified in ETSI EN 319 411-2 [13]

18 - Types according to clause 4.2.3 specified in ETSI EN 319 412-5 [12]

2.2.3. Certificate Policy

Profile	PolicyIdentifier * (authentification)	PolicyIdentifier * (digital signature)	PolicyQualifier
Identity card of Estonian citizen	1.3.6.1.4.1.51361.1.1.1 0.4.0.2042.1.2	1.3.6.1.4.1.51361.1.1.1 0.4.0.194112.1.2	https://www.sk.ee/CPS
Identity card of European Union citizen	1.3.6.1.4.1.51361.1.1.2 0.4.0.2042.1.2	1.3.6.1.4.1.51361.1.1.2 0.4.0.194112.1.2	https://www.sk.ee/CPS
Diplomatic identity card	1.3.6.1.4.1.51455.1.1.1 0.4.0.2042.1.2	1.3.6.1.4.1.51455.1.1.1 0.4.0.194112.1.2	https://www.sk.ee/CPS
Residence card of long-term resident	1.3.6.1.4.1.51361.1.1.5 0.4.0.2042.1.2	1.3.6.1.4.1.51361.1.1.5 0.4.0.194112.1.2	https://www.sk.ee/CPS
Residence card of temporary residence citizen	1.3.6.1.4.1.51361.1.1.6 0.4.0.2042.1.2	1.3.6.1.4.1.51361.1.1.6 0.4.0.194112.1.2	https://www.sk.ee/CPS
Residence card of family members of citizen of European Union	1.3.6.1.4.1.51361.1.1.7 0.4.0.2042.1.2	1.3.6.1.4.1.51361.1.1.7 0.4.0.194112.1.2	https://www.sk.ee/CPS
Digital identity card	1.3.6.1.4.1.51361.1.1.3 0.4.0.2042.1.2	1.3.6.1.4.1.51361.1.1.3 0.4.0.194112.1.2	https://www.sk.ee/CPS
Digital identity card of e-resident	1.3.6.1.4.1.51361.1.1.4 0.4.0.2042.1.2	1.3.6.1.4.1.51361.1.1.4 0.4.0.194112.1.2	https://www.sk.ee/CPS

* Object identifier 1.3.6.1.4.1.51361 represents Police and Border Guard Board of Estonia, and OID 1.3.6.1.4.1.51455 represents Estonian Ministry of Foreign Affairs,

which are private enterprises OID registered under Internet Assigned Numbers Authority (IANA). Other OID's are defined according to the ETSI standards EN 319 411-2 [13] and EN 319 411-1 [15].

1.3.6.1.4.1.51361.1 - Sub-OID type: identity document = 1

1.3.6.1.4.1.51361.1.{1 or 2} - System Sub-OID: production = 1; test = 2

1.3.6.1.4.1.51361.1.{1 or 2}.{1 to 7} - System Sub-OID document type: 1 to 7 (*refer to 2.2.3 profile names*)

Example OID 1:Identity card of Estonian citizen (test): 51361.1.2.1
Example OID 1: Residence card of temporary residence citizen (production): 51361.1.1.6

3. Profile of OCSP Response

OCSP v1 according to RFC 6960 [8]

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	CN = ESTEID2018 AIA OCSP RESPONDER YYYYMM OU = OCSP 2.5.4.97 = NTREE-10747013 O = SK ID Solutions AS C = EE	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 [8] 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 [5].
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 [8] clause 4.4.4
Extended Revoked Definition	no	NULL	Identification that the semantics of certificate status in OCSP response conforms to extended definition in RFC6960 clause 2.2
Nonce	no		Value is copied from request if it is included. Pursuant to RFC 6960 [8] clause 4.4.1
Signature Algorithm	yes	Sha256WithRSAEncryption or Sha512WithRSAEncryption	Signing algorithm pursuant to RFC 5280 [5].
signature	yes		
Certificate	yes		Certificate corresponding to the private key used to sign the response.

4. Referred and Related Documents

1. "SK ID Solutions AS - ESTEID2018 Certification Practice Statement", published: https://sk.ee/en/repository/CPS/;
2. "Police and Border Guard Board - Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card", published: https://www.id.ee/;
3. ISO/IEC 7816, Parts 1-4, published: http://iso.org;
4. ISO 3166 Codes http://www.iso.org/iso/country_codes;

5. RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
6. ETSI EN 319 412-1 v1.1.1 Electronic Signatures and Infrastructures (ESI) Certificate Profiles; Part 1: Overview and common data structures;
7. ETSI EN 319 412-2 v2.1.1 Electronic Signatures and Infrastructures (ESI) Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;
8. RFC 6960 – X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP;
9. 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;
10. RFC 5480 - Elliptic Curve Cryptography Subject Public Key Information;
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 in the internal market and repealing Directive 1999/93/EC;
12. ETSI EN 319 412-5 v2.1.1 Electronic Signatures and Infrastructures (ESI) Certificate Profiles; Part 5: QCStatements;
13. ETSI EN 319 411-2 v2.1.1 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 ;
14. RFC 5639 - Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation
15. ETSI EN 319 411-1 v.1.1.1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements