Certificate, CRL and OCSP Profile for Personal Identification Documents of the Republic of Estonia

Version 7.0

1.November 2016

Version History		
Date	**Version**	**Changes**
01.11.2016	7.0	Document name change; Document structure change; Chapter 2 - improved “Technical Profile of the Certificate”; Chapter 2.2 - improved certificate extensions table; Chapter 2.2.3 - new OID’s added in certificate policies; Chapter 4 - added OCSP profile description Removed certificate examples
01.01.2016	6.0	In clause 3.2 changed certificate owner details ASN.1 types. In clause 4 renewed Referred and Related Documents. In appendix A in clause A.2.3 complemented the list of the certificate signing algorithms with RSA. In appendix A in clause A.2.5 complemented key lengths of Public Key in the Certificate. In appendix A in clause A.3 renewed Certificate Extensions. In appendix A in clause A.3.4 complemented Certificate Policies. In appendix A in clause A.3.7 complemented CSP Additional Data. In appendix A in clause A.3.10 changed Identification of Qualified Certificate. In appendix A in clauses A.5.1 ja A.5.2 prenewed Sample Certificates.
01.01.2015	5.0	Chapter 4.1 - updated references to Legal Acts of Republic of Estonia. Chapter A.2.3 of appendix A removed SHA-1 from the list of certificate signing algorithms
01.12.2014	4.0	Changed the name of the document. Editorial corrections and improvements to document formatting. Document is aligned with RFC5280. Chapter 1 - adjusted the document content description. Chapter 1.2.1 - updated with new terms of Resident digi-ID, Eresident digi-ID, E-resident mobile-ID, Document; removed terms Identity document and Validity period of identity document. Chapter 3.1 updated certificate issuer details. Chapter 3.2 updated certificate owner details. Chapter A.2.3 of appendix A updated list of certificate signing algorithms. Chapter A.2.4 of appendix A specified the certificate validity period. Chapter A.2.5 of appendix A updated list of public keys in the certificate and its presentation algorithms. Chapter A.5.1 and A.5.2 of appendix A updated sample Certificates.
01.06.2014	3.5	All changes planned into version 3.4 will take effect in version 3.5 except limitation of validity of Mobile-ID certificates.

01.05.2014	3.4	Amended with version information table; referred and related documents are now described in dedicated chapter 4; editorial corrections and improvements to document formatting; Adjusted the document content description in chapter 1; Chapter 1.2.1 updated with new terms of RP-card, Digi-ID, Mobile-ID and updated the definitions of ID-card and Identity document; Certificate validity periods of different documents are now described in chapter A.2.4 of appendix A; In chapter A.3.6 of appendix A, the rules of e-mail address creation updated regarding handling dots (in effect since 28.02.2013); The identificators of the qualified certificate extensions updated in chapter A.3.10 of appendix A (in effect since 28.02.2013); The identificators of the qualified certificates updated in examples described in chapters A.5.1 and A.5.2 of appendix A (in effect since 28.02.2013). This version never took effect because the decree of the Government of the Republic of Estonia describing the issuance details of the digital identity document in the form of MobileID which changing the validity period of the Mobile-ID certificates issued from May 1st 2014 until December 31st 2014 was not adopted.
01.01.2010	3.3	Version to be published.

1. Introduction
    1.1. Terms and Abbrevations
2. Technical Profile of the Certificate
    2.1. Certificate Body
    2.2. Certificate Extensions
        2.2.1. Extensions
        2.2.2. Variable Extensions
        2.2.3. Certificate Policy
3. Profile of Certificate Revocation List
    3.1. CRL Main Fields
    3.2. CRL Extensions
4. OCSP Profile
5. Referred and Related Documents
6. Appendix A - Additional Certificate-specific Technical Information
    6.1. (Subject Alternative Name)

1. Introduction

The document in hand describes the profiles of the digital certificates loaded to the personal identification documents of Republic of Estonia (with the exception of travel documents),

CRL-s and OCSP responses, issued by ESTEID[1] . This document complements Certificate Policies [2][3][4] 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 [13].

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

The certificates are being issued by SK

[1] Intermediate CA can be ESTEID-SK 2011 and ESTEID-SK 2015

1.1. Terms and Abbrevations

Refer to p 1.6 in Certification Practice Statement [1] and Certificate policies [2], [3], [4].

2. Technical Profile of the Certificate

Natural person certificate is compiled in accordance with the X.509 version 3, IETF RFC 5280 [6], ETSI EN 319 412-2 [8] and ETSI EN 411-2 (chapter 6.6) [15].

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	1.2.840.113549.1.1.11	yes	sha256WithRSAEncryption	no	Signature algorithm in accordance to RFC 5280
Issuer Distinguished name					
Common Name (CN)	2.5.4.3	yes	ESTEID-SK 2015		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 [7].
Organisation (O)	2.5.4.10	yes	AS Sertifitseerimiskeskus		Issuer organisation name
Country (C)	2.5.4.6	yes	EE		Country code: EE - Estonia (2 character ISO 3166 country code [5])
Valid from		yes			First date of certificate validity.
Valid to		yes			The last date of certificate validity.
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
Given Name (G)	2.5.4.42	yes		yes	Person given names in UTF8 format according to RFC5280. Also pursuant to IDA [12], international letters SHALL be encoded according to ICAO transcription rules where neccessary.
SurName (SN)	2.5.4.4	yes		yes	Person surnames in UTF8 format according to RFC5280. Also pursuant to IDA [12], international letters SHALL be encoded according to ICAO transcription rules where neccessary.
Common Name (CN)	2.5.4.3	yes		yes	Comma-separated surnames, first names and personal identity code.
Organisational Unit (OU)	2.5.4.11	yes		yes	Area of use of the certificate. The following values are used depending on certificate type: "authentication" or "digital signature"
Organisation Name (O)	2.5.4.10	yes		yes	Type of the certificate [2]
Country (C)	2.5.4.6	yes		yes	Country of origin in accordance with ISO 3166 [5].
Subject Public Key		yes	RSA 2048, NIST P-256	yes	RSA algorithm in accordance with RFC 4055 [10] and ECC algorithm created in accordance with RFC 5639 [11]

[2] ID-card and RP-card O = ESTEID

Digi-ID: O = ESTEID (DIGI-ID)

Mobile-ID: O = ESTEID (MOBIIL-ID)

E-resident digi-ID: O = ESTEID (DIGI-ID E-RESIDENT)

E-resident mobile-ID: O = ESTEID (MOBIIL-ID E-RESIDENT)

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	Refer to p 2.2.2 "Variable Extensions"	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 used to sign the ceritificate	Non-critical	yes
CRL distribution Points	2.5.29.31	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.sk.ee/crls/esteid/esteid2015.crl	Non-critical	yes
SubjectKeyIdentifier	2.5.29.14	SHA-1 hash of the public key used to sign the ceritificate	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/esteid2015		yes
caIssuers	1.3.6.1.5. 5.7.48.2	https://sk.ee/upload/files/ESTEID-SK_2015.der.crt		yes

2.2.2. Variable Extensions

Following variable extensions for ID-card, RP-card, Digi-ID (also for E-resident) and Mobile-ID (also for E-resident)

Extension	DIGITAL AUTHENTICATION	DIGITAL SIGNATURE
Subject Alternative Name	Refer to p 6.1 "Appendix A"	
Key Usage	DigitalSignature, KeyEncipherment, dataEncipherment	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[3]		
id-etsi-qcs-QcCompliance		yes
id-etsi-qcs-QcSSCD		yes

id-etsi-qcs-QcType[4]		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/

[3] qcStatements according to clause 6.6.1 specified in ETSI EN 319 411-2 [15]
[4] Types according to clause 4.2.3 specified in ETSI EN 319 412-5 [14].

2.2.3. Certificate Policy

Profile	PolicyIdentifier (authentification)	PolicyIdentifier (digital signature)	PolicyQualifier
ID-card ; RP-card	1.3.6.1.4.1.10015.1.1 0.4.0.2042.1.2	1.3.6.1.4.1.10015.1.1 0.4.0.194112.1.2	https://www.sk.ee/repositoorium/CPS
Digi-ID ; E-resident digi-ID	1.3.6.1.4.1.10015.1.2 0.4.0.2042.1.2	1.3.6.1.4.1.10015.1.2 0.4.0.194112.1.2	https://www.sk.ee/repositoorium/CPS
Mobile-ID ; E-resident mobile-ID	1.3.6.1.4.1.10015.1.3 0.4.0.2042.1.2	1.3.6.1.4.1.10015.1.3 0.4.0.194112.1.2	https://www.sk.ee/repositoorium/CPS

3. Profile of Certificate Revocation List

SK issues CRLs in accordance to the guides of RFC 5280 [6]

3.1. CRL Main Fields

Field	OID	Mandatory	Value	Description
Version		yes	Version 2	CRL format version pursuant to X.509.
Signature Algorithm		yes	sha256WithRSA Encryption	CRL signing algorithm pursuant to RFC 5280
Issuer Distinguished Name		yes		Distinguished name of crl issuer
Common Name (CN)	2.5.4.3	yes	ESTEID-SK 2015 or ESTEID-SK 2011	Name of certification authority
Organisation Identifier	2.5.4.97	yes	NTREE-10747013	Identification of the issuer organisation different from the organisation name (Does not apply to ESTEID-SK 2011 certificate). Certificates may include one or more semantics identifiers as specified in clause 5.1.4 of ETSI EN 319 412-1 [7]
Organisation (O)	2.5.4.10	yes	AS Sertifitseerimiskeskus	Organisation name

Country (C)	2.5.4.6	yes	EE	Country code: EE – Estonia (2 character ISO 3166 country code [5])
Last Update		yes		Date and time of CRL issuance.
Next Update		yes		Date and time of issuance of the next CRL. The conditions are also described ESTEID CPS chapter 4.9.7
Revoked Certificates				List of revoked certificates.
Serial Number		yes		Serial number of the certificate revoked.
CRL Reason Code	2.5.29.21	yes		Reason code for certificate revocation.
Invalidity Date	2.5.29.24	yes		An X.509 CRL entry extension that "indicates the date at which it is known or suspected that the [revoked certificate's private key] was compromised or that the certificate should otherwise be considered invalid." [X509].

3.2. CRL Extensions

Field	OID	Values and Limitations	Criticality
CRL Number	2.5.29.20	CRL sequence number	no
Authority Key Identifier	2.5.29.35	Matching the subject key identifier of the certificate	no
Issuing Distribution Point	2.5.29.28	Identifies the CRL distribution point http://www.sk.ee/crls/esteid/esteid2015.crl	yes

4. OCSP Profile

OCSP v1 according to [RFC 6960] [9]

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, ST = Harjumaa, L = Tallinn, O = AS Sertifitseerimiskeskus, OU = OCSP, CN = SK OCSP RESPONDER 2011, emailAddress = pki@sk.ee	Distinguished name of the OCSP responder
Produced At	yes		Date when the OCSP response was signed

Responses	yes		
CertID	yes		Serial number of the certificate
Cert Status	yes		Status of the certificate [5]
Revocation Time	no		Date of revocation or expiration of certificate
Revocation Reason	no		Code for revocation Reason according to RFC5280 [6]
This Update	yes		Date when the status was queried from database
Signature Algorithm	yes	sha256WithRSAEncryption	Signing algorithm pursuant to RFC 5280
signature	yes		
Certificate	yes		Certificate corresponding to the private key used to sign the response.

[5] Exceptions: In case of expired certificate „revoked“ status is used and Revocation Time is set to notAfter value of the certificate if the responder has access to the full certificate.

5. Referred and Related Documents

1. AS Sertifitseerimiskeskus - Certification Practice Statement for ESTEID, published:https://sk.ee/en/repository/CPS/;
2. Certificate Policy for ID card: https://sk.ee/en/repository/CP/;
3. Certificate Policy for Digi-ID : https://sk.ee/en/repository/CP/;
4. Certificate Policy for Mobile-ID : https://sk.ee/en/repository/CP/;
5. ISO 3166 Codes http://www.iso.org/iso/country_codes ;
6. RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile ;
7. ETSI EN 319 412-1 v1.1.1 Electronic Signatures and Infrastructures (ESI) Certificate Profiles; Part 1: Overview and common data structures ;
8. 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 ;
9. RFC 6960 – X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP ;
10. 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;
11. RFC 5639 - Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation;
12. Identity Documents Act, RT I 1999, 25, 365, published: https://www.riigiteataja.ee/en/eli/511042016001/consolide/current
13. 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
14. ETSI EN 319 412-5 v2.1.1 Electronic Signatures and Infrastructures (ESI) Certificate Profiles; Part 5: QCStatements
15. ETSI EN 319 411-2 v2.6.1 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

6. Appendix A - Additional Certificate-specific Technical Information

6.1. (Subject Alternative Name)

The e-mail address of the certificate owner is presented in this field. The e-mail address is included only in the certificate facilitating digital authentication.
The e-mail address is composed of person's given- and surnames (forenames.surnames@eesti.ee) in accordance to the values of the G and SN fields of the certificate. The character substitutions shall be made as necessary in accordance to this chapter. In case of repeated names, if the basic form is already issued, an incremental decimal number is added to the name in form of forenames.surnames.N@eesti.ee. The subdomain for the addresses is eesti.ee.
In the address, the dot (.) character is used to separate name parts. If the name contains a dash, a dash is also present in the e-mail address. All other characters besides dash are replaced with the dot character.
If the replacement of characters results in more than one sequent dot, they will be replaced with one dot (for example, person named as ANTS E. PALUSAAR shall have an e-mail address in form of ants.e.palusaar@eesti.ee). In case if character replacement results with a dot in the beginning of the email address or straight before @ character, these dots will be removed (for example, for a person named as MARK GIREE' shall have an e-mail address in form mark.giree@eesti.ee).

Character codes are presented in hexadecimal form in the table above correspond to UTF-32 encoding

specified in the international standard ISO/IEC 10646 (Unicode).

The following substitutions shall be made for the characters in names:

No	Char	Char code	New char	New char code
1	A	0041		
2	a	0061		
3	B	0042		
4	b	0062		
5	C	0043		
6	c	0063		
7	D	0044		
8	d	0064		
9	E	0045		
10	e	0065		
11	F	0046		
12	f	0066		
13	G	0047		
14	g	0067		
15	H	0048		
16	h	0068		
17	I	0049		
18	i	0069		
19	J	004A		
20	j	006A		
21	K	004B		
22	k	006B		
23	L	004C		
24	l	006C		
25	M	004D		
26	m	006D		
27	N	004E		
28	n	006E		
29	O	004F		
30	o	006F		
31	P	0050		

32	p	0070		
33	Q	0051		
34	q	0071		
35	R	0052		
36	r	0072		
37	S	0053		
38	s	0073		
39	Š	0160	S	0053
40	š	0161	s	0073
41	Z	005A		
42	z	007A		
43	Ž	017D	Z	005A
44	ž	017E	z	007A
45	T	0054		
46	t	0074		
47	U	0055		
48	u	0075		
49	V	0056		
50	v	0076		
51	W	0057		
52	w	0077		
53	Õ	00D5	O	004F
54	õ	00F5	o	006F
55	Ä	00C4	A	0041
56	ä	00E4	a	0061
57	Ö	00D6	O	004F
58	ö	00F6	o	006F
59	Ü	00DC	U	0055
60	ü	00FC	u	0075
61	X	0058		
62	x	0078		
63	Y	0059		
64	y	0079		
65	À	00C0	A	0041
66	à	00E0	a	0061
67	Á	00C1	A	0041
68	á	00E1	a	0061
69	Â	00C2	A	0041
70	â	00E2	a	0061
71	Ã	00C3	A	0041
72	ã	00E3	a	0061
73		0100	A	0041
74		0101	a	0061
75		0102	A	0041
76		0103	a	0061
77	Å	00C5	A	0041
78	å	00E5	a	0061

79		0104	A	0041
80		0105	a	0061
81	Æ	00C6	A	0041
82	æ	00E6	a	0061
83		0106	C	0043
84		0107	c	0063
85		010C	C	0043
86		010D	c	0063
87	Ç	00C7	C	0043
88	ç	00E7	c	0063
89		010E	D	0044
90		010F	d	0064
91		0110	DJ	0044; 004A
92		0111	dj	0064; 006A
93	Đ	00D0	DH	0044; 0048
94	ð	00F0	dh	0064; 0068
95	È	00C8	E	0045
96	è	00E8	e	0065
97	É	00C9	E	0045
98	é	00E9	e	0065
99	Ê	00CA	E	0045
100	ê	00EA	e	0065
101		0112	E	0045
102		0113	e	0065
103		0116	E	0045
104		0117	e	0065
105	Ë	00CB	E	0045
106	ë	00EB	e	0065
107		011A	E	0045
108		011B	e	0065
109		0118	E	0045
110		0119	e	0065
111		011E	G	0047
112		011F	g	0067
113		0122	G	0047
114		0123	g	0067
115	Ì	00CC	I	0049
116	ì	00EC	i	0069
117	Í	00CD	I	0049
118	í	00ED	i	0069
119	Î	00CE	I	0049
120	î	00EE	i	0069
121		012A	I	0049
122		012B	I	0069
123		0130	I	0049
124		0131	i	0069
125	Ï	00CF	I	0049

126	ï	00EF	i	0069
127		012E	I	0049
128		012F	i	0069
129		0136	K	004B
130		0137	k	006B
131		0139	L	004C
132		013A	l	006C
133		013D	L	004C
134		013E	l	006C
135		013B	L	004C
136		013C	l	006C
137		0141	L	004C
138		0142	l	006C
139		0143	N	004E
140		0144	n	006E
141	Ñ	00D1	N	004E
142	ñ	00F1	n	006E
143		0147	N	004E
144		0148	n	006E
145		0145	N	004E
146		0146	n	006E
147	Ò	00D2	O	004F
148	ò	00F2	o	006F
149	Ó	00D3	O	004F
150	ó	00F3	o	006F
151	Ô	00D4	O	004F
152	ô	00F4	O	006F
153		014C	O	004F
154		014D	o	006F
155		0150	O	004F
156		0151	o	006F
157	Ø	00D8	O	004F
158	ø	00F8	o	006F
159	OE	0152	OE	004F; 0045
160	oe	0153	oe	006F; 0065
161		0154	R	0052
162		0155	r	0072
163		0158	R	0052
164		0159	r	0072
165		0156	R	0052
166		0157	r	0072
167		015A	S	0053
168		015B	s	0073
169		015E	S	0053
170		015F	s	0073
171	ß	00DF	ss	0073; 0073
172		0164	T	0054

173		0165	t	0074
174		0162	T	0054
175		0163	t	0074
176	Þ	00DE	TH	0054; 0048
177	þ	00FE	Th	0074; 0068
178	Ù	00D9	U	0055
179	ù	00F9	u	0075
180	Ú	00DA	U	0055
181	ú	00FA	u	0075
182	Û	00DB	U	0055
183	û	00FB	u	0075
184		016A	U	0055
185		016B	u	0075
186		016E	U	0055
187		016F	u	0075
188		0170	U	0055
189		0171	u	0075
190		0172	U	0055
191		0173	u	0075
192	Ý	00DD	Y	0059
193	ý	00FD	y	0079
194	Ÿ	0178	Y	0059
195	ÿ	00FF	y	0079
196		0179	Z	005A
197		017A	z	007A
198		017B	Z	005A
199		017C	z	007A