Certificates on identity card of Republic of Estonia

Valid from 1.January 2010

Version 3.3

TABLE OF CONTENT

SCOPE

This document describes profile of personal digital certificates stored on Estonian Republic Identity card (ID card). Annex A presents additional technical information and example of certificates.

This document does not describe other data collections stored in the Identity card.

This standard is based on the following documents:

A. Legal acts of Estonian Republic

1) Identity Documents Act (RT I 1999, 25, 365; 2006, 29, 221);
2) Digital Signature Act (RT I 2000, 26, 150; 92, 597; 2007, 24, 127);
3) Personal Data Protection Act (RT I 2007, 24, 127);
4) Decree of the Minister of Transport and Communications "Service provider's information systems' auditing procedure" (issued 03.10.2000, no 83, RTL 2000, 108, 1655)

B. IETF (Internet Engineering Task Force http://www.ietf.org) **documents**

1) RFC3280 - Internet X.509 Public Key Infrastructure - Certificate and CRL Profile (http://www.ietf.org/rfc/rfc3280.txt);
2) RFC3039 - Internet X.509 Public Key Infrastructure - Qualified Certificates Profile (http://www.ietf.org/rfc/rfc3039.txt).

1. TERMS AND DEFINITIONS

For the purposes of this document, the following terms and definitions apply.

Term	Explanation
Identity card, ID-card	Document identifying its holder and issued on the basis of a legal act
Identity card validity period	Period starting at issuing the Identity card and ending at the validity end time specified at the moment of issuing. Actual document validity period may be shorter due to the document possibly being revoked
SR	Register of Certification Service Providers (SR - *Sertifitseerimise Register*) according to Estonian Digital Signatures Act
CSP	Certification Service Provider according to Estonian Digital Signatures Act
OID	Object Identifier. Unique sequence of numbers to identify any digital data, defined in ITU-T recommendation X.208.
Distinguished name	Unique subject name in the infrastructure of certificates
Certificate	Digital document where a public key is associated with the owner of the key
Certificate issuer	Person who issues the certificate (CSP in the context of Digital Signatures Act)

Term	Explanation
Signing certificate	The certificate of CSP which CSP uses to sign the personal certificates that it issues
Certificate owner	Subject to whom the certificate has been issued
Certificate validity period	Period starting at creating the certificate and ending at certificate validity end time specified at the moment of issuing the certificate. Actual certificate validity period may be shorter due to the certificate possibly being revoked.

2. LIST AND PURPOSE OF CERTIFICATES

Two certificates are stored in the identification document:

1) authentication certificate for electronic identification, encryption and digital signing of e-mails;
2) digital signature certificate for creating electronic signatures according to the Estonian Digital Signature Act.

Certificates are issued by CSP:

1) who meets the requirements described in Digital Signatures Act;
2) who meets the requirements described in the decree of the Minister of Transport and Communications entitled "Service provider's information systems' auditing procedure";
3) who meets requirements of issuing qualified certificates as defined in “Directive 1999/93/EC of European Parliament and the Council on a Community framework for electronic signatures”.

3. DATA IN CERTIFICATES

Both personal certificates must contain the following data:

1) certificate issuer data;
2) certificate owner data;
3) technical certificate data.

The following chapters 4.1-4.3 describe content of the data. Technical details are covered in annex A.

3.1 Certificate Issuer Data

Certificates contain the following mandatory data about certificate issuer (CSP):

Attribute	OID of the attribute	ASN.1 type	Description	Example
C (countryName)	{id-at-countryName} { 2,5,4,6 }	DirectoryString: PrintableString	Country of origin	EE
O (organization)	{id-at-organization} { 2,5,4,10}	DirectoryString: PrintableString	Official name of STO as in business registry and SRR	AS Sertifitseerimis-keskus
OU (organizationUnit)	{id-at-organizationalUnit } { 2,5,4,11}	DirectoryString: PrintableString	Identity of certification service	ESTEID
CN (commonName)	{id-at-commonName} { 2,5,4,3 }	DirectoryString: PrintableString	Commin Name of the certification service	ESTEID-SK

Certificates may contain the following additional data about certificate issuer (CSP):

Attribute	OID of the attribute	ASN.1 type	Description	Example
SN (surName)	{id-at-surName} { 2,5,4,4}	DirectoryString: PrintableString	Serial number issued by SRR	1
E (e-mailAddress)	{1,2,840,113549,1 ,9,1}	DirectoryString: IA5String	e-mail address of the STO	pki@sk.ee

3.2 Certificate Owner Data

Certificates contain the following mandatory data about certificate owner:

Attribute	OID of the attribute	ASN.1 type	Descrition	Example
C (countryName)	{id-at-countryName} { 2,5,4,6 }	DirectoryString: PrintableString	Country of origin	EE
O (organization)	{id-at-organization} { 2,5,4,10}	DirectoryString: PrintableString	Type of the certificate	ESTEID
OU (organizationUnit)	{id-at-organizationalUnit} { 2,5,4,11}	DirectoryString: PrintableString	Usage type of the certificate	*authentication* or *digital signature*
SN (surName)	{id-at-surName} { 2,5,4,4}	DirectoryString: BMPString or UTF8* or PrintableString	Family name(s)	MÄNNIK
G (givenName)	{id-at-givenName} { 2,5,4,42 }	DirectoryString: BMPString or UTF8* or PrintableString	First name(s)	MARI-LIIS
S (serialNumber)	{id-at-serialNumber} { 2,5,4,5 }	DirectoryString: PrintableString	Personal Identification Code	47101010033

CN (commonName)	{id-at-commonName} { 2,5,4,3 }	DirectoryString: BMPString or UTF8* or PrintableString	Comma-separated first names, family names and personal identification code	MÄNNIK,MARI-LIIS,47101010033

3.3 Technical Certificate Data

Personal certificates contain the following technical certificate data:

1) certificate format version;
2) certificate serial number;
3) certificate signing algorithm;
4) validity period of the certificate;
5) public key in the certificate and its presentation algorithm;
6) CSP public key identifier;
7) person's public key identifier;
8) key usage;
9) certificate policy identifier and reference;
10) reference to CDP (CRL Distribution Point);
11) person's e-mail address (only in authentication certificates);
12) CSP additional data;
13) extended key usage (only in authentication certificates);
14) identification of qualified certificate.

* BMPString or UTF8 coding is used in case the name contains characters not present in ASCII7 character encoding table.

Appendix A
ADDITIONAL CERTIFICATE-SPECIFIC TECHNICAL INFORMATION

A.1 General

Following is the detailed contents of certificate data fields with standard terms (in cursive).

A.2 Main certificate fields

A.2.1 Certificate format version (“*version” by RFC*)

The field contains certificate format version number.

Identity card use X.509 v3 certificates, the value of this field is thus 2.

A.2.2 Certificate serial number (*serialNumber*)

The field contains certificate sequence number. It must be unique across all certificates issued by one CSP.

A.2.3 Certificate signing algorithm (*signatureAlgorithm*)

The field contains encryption algorithm which CSP uses to sign the issued certificates.

Identity card certificates use the SHA-1 algorithm and the value of this field is thus:

- **sha1WithRSAEncryption** { 1, 2, 840, 113549, 1, 1, 5 }.

A.2.4 Certificate validity period (*validity*)

Certificate validity period indicates the period during which CSP guarantees provision of validation service for the certificate. Certificates are valid generally **1825 days** (5 years) counting from certificate issuance, but no longer than identification document expiration date.

Dates in certificates are stored according to RFC3280.

A.2.5 Public key in certificate and its presentation algorithm (*subjectPublicKeyInfo*)

The field contains certificate owner's public key with its presentation algorithm.

The following encryption algorithm is used (on the **AlgorithmIdentifier** field) in identification document certificates:

- **rsaEncryption** { 1, 2, 840, 113549, 1, 1, 1 }.

A.3 Certificate extensions

Certificate extensions in use are presented in the following table:

Name of the Extension	ASN.1 name and OID	Present?	Critical?
AuthorityKeyIdentifier	{id-ce-authorityKeyIdentifier} {2,5,29,35}	**YES**	NO
SubjectKeyIdentifier	{id-ce-subjectKeyIdentifier} {2,5,29,14}	**YES**	NO
KeyUsage	{id-ce-keyUsage} {2,5,29,15}	**YES**	**YES**
CertificatePolicies	{ id-ce-certificatePolicies} {2,5,29,32}	**YES**	NO
SubjectAltName (in certificate for authentication)	**{** id-ce-subjectAltName} {2,5,29,17}	**YES**	NO
IssuerAltName	**{** id-ce-issuerAltName} {2,5,29,18}	**YES**	NO
CRLDistributionPoints	**{**id-ce-CRLDistributionPoints} {2,5,29,18}	**YES**	NO
ExtKeyUsage (in certificate for authentication)	{id-ce-extKeyUsage} {2,5,29,37}	**YES**	**YES**
ExtKeyUsage (in certificate for digital signature)	{id-ce-extKeyUsage} {2,5,29,37}	**NO**	NO
BasicConstraints	{id-ce-basicConstraints} {2,5,29,18}	**YES**	NO
qcStatements	id-pe-qcStatements {1,3,6,1,5,5,7,1,3}	**YES**	NO

The "Present?" column specifies whether the extension is present in the certificate. If the extension is present, the "Critical?" notice means that software applications using the certificate must always check its contents.

A.3.1 CSP public key identifier (*authorityKeyIdentifier*)

The field contains identifier of CSP's public key whose matching private key was used to sign the personal certificate. This is necessary for constructing CSP certificate chain.

Only the **keyIdentifier** field is used.

This is a noncritical extension.

A.3.2 Person's public key identifier (*subjectKeyIdentifier*)

The field contains identifier of public key contained in the certificate. This is necessary for quickly identifying the public key (if the certificate owner has got several certificates from the same CSP).

Method 1 is used according to RFC3280.

This is a noncritical extension.

A.3.3 Key usage (*keyUsage*)

The following values are used in personal certificates:

1) **digitalSignature,**
2) **nonRepudiation,**
3) **keyEncipherment,**
4) **dataEncipherment,**

They are used as follows:

In authentication certificate:

- digitalSignature,
- keyEncipherment,
- dataEncipherment,

In digital signature certificate:

- nonRepudiation.

This is a **critical** extension.

A.3.4 Certificate policies *(certificatePolicies)*

The field contains reference to certificate practice statement which has been used to issue the certificate. The field contains *URL* and *OID* identifier.

This is a noncritical extension.

A.3.5 CRL Distribution Points *(cRLDistributionPoints)*

The field contains reference to CRL (Certificate Revocation List) associated with the certificates issued by CSP. It is presented as URL. Both LDAP and HTTP may be used as access protocol.

This is a noncritical extension.

A.3.6 Person's e-mail address (*SubjAltName*)

The field contains certificate owner's e-mail address. The e-mail address is only present in the authentication certificate.

The basic form of e-mail address is created from the person's first and last name(s) (firstnames.lastnames@eesti.ee) according to G and SN values in certificate with necessary character substitutions made in advance according to this chapter. In case repeated names, if the basic form is already issued, a incremental decimal number is added to the name in form of firstnames.lastnames.N@eesti.ee. Addresses are issued from eesti.ee subdomain.

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. Other characters besides dash are replaced with the dot character.

The following alphabetic character substitutions are made:

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	Ā	0100	A	0041
74	ā	0101	a	0061
75	Ă	0102	A	0041
76	ă	0103	a	0061
77	Å	00C5	A	0041
78	å	00E5	a	0061
79	Ą	0104	A	0041
80	ą	0105	a	0061
81	Æ	00C6	A	0041
82	æ	00E6	a	0061
83	Ć	0106	C	0043
84	ć	0107	c	0063
85	Č	010C	C	0043
86	č	010D	c	0063
87	Ç	00C7	C	0043
88	ç	00E7	c	0063
89	Ď	010E	D	0044
90	ď	010F	d	0064
91	Đ	0110	DJ	0044; 004A
92	đ	0111	dj	0064; 006A
93	Ð	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	Ē	0112	E	0045
102	ē	0113	e	0065
103	Ė	0116	E	0045

104	ė	0117	e	0065
105	Ë	00CB	E	0045
106	ë	00EB	e	0065
107	Ě	011A	E	0045
108	ě	011B	e	0065
109	Ę	0118	E	0045
110	ę	0119	e	0065
111	Ğ	011E	G	0047
112	ğ	011F	g	0067
113	Ģ	0122	G	0047
114	ģ	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	Ī	012A	I	0049
122	ī	012B	i	0069
123	İ	0130	I	0049
124	ı	0131	i	0069
125	Ï	00CF	I	0049
126	ï	00EF	i	0069
127	Į	012E	I	0049
128	į	012F	i	0069
129	Ķ	0136	K	004B
130	ķ	0137	k	006B
131	Ĺ	0139	L	004C
132	Í	013A	l	006C
133	Ľ	013D	L	004C
134	ľ	013E	l	006C
135	Ļ	013B	L	004C
136	ļ	013C	l	006C
137	Ł	0141	L	004C
138	ł	0142	l	006C
139	Ń	0143	N	004E
140	ń	0144	n	006E
141	Ñ	00D1	N	004E
142	ñ	00F1	n	006E
143	Ň	0147	N	004E
144	ň	0148	n	006E
145	Ņ	0145	N	004E
146	ņ	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	Ō	014C	O	004F
154	ō	014D	o	006F
155	Ő	0150	O	004F
156	ő	0151	o	006F
157	Ø	00D8	O	004F
158	ø	00F8	o	006F
159	Œ	0152	OE	004F; 0045
160	œ	0153	oe	006F; 0065
161	Ŕ	0154	R	0052
162	ŕ	0155	r	0072
163	Ř	0158	R	0052
164	ř	0159	r	0072
165	Ŗ	0156	R	0052
166	ŗ	0157	r	0072
167	Ś	015A	S	0053
168	ś	015B	s	0073
169	Ş	015E	S	0053
170	ş	015F	s	0073
171	ß	00DF	ss	0073; 0073
172	Ť	0164	T	0054
173	ť	0165	t	0074
174	Ţ	0162	T	0054
175	ţ	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	Ū	016A	U	0055
185	ū	016B	u	0075
186	Ů	016E	U	0055
187	ů	016F	u	0075
188	Ű	0170	U	0055
189	ű	0171	u	0075
190	Ų	0172	U	0055
191	ų	0173	u	0075
192	Ý	00DD	Y	0059
193	ý	00FD	y	0079

194	Ÿ	0178	Y	0059
195	ÿ	00FF	y	0079
196	Ź	0179	Z	005A
197	ź	017A	z	007A
198	Ż	017B	Z	005A
199	ż	017C	z	007A

Character codes in hexadecimal form in the table above correspond to UTF-32 encoding specified in the standard ISO/IEC 10646 (Unicode).

Example e-mail addresses:

- Mari-Liis Männik: mari-liis.mannik@eesti.ee
- Jaan Tamm: jaan.tamm.2@eesti.ee

This is a noncritical extension.

A.3.7 STO additional data *(IssuerAltName)*

The value of this field is obtained from CSP signing certificate field *SubjAltName* and it contains additional information about the CSP.

This is a noncritical extension.

A.3.8 Extended key usage *(ExtendedKeyUsage)*

Personal certificates contain the value

- **ClientAuthentication**
- **SecureEmail**

only in authentication certificate.

This is a **critical** extension in authentication certificate. It is not present in digital signature certificate.

A.3.9 Basic Constraints

The basic constraints extension identifies the subject of the certificate is an end-endity.

This is a noncritical extension.

A.3.10 Identification of Qualified Certificate

This extension indicates that the certificate is issued by CSP complying to requirements for CA issuing qualified certificates. The extension is formed according to ETSI TS 101 862 v 1.3.2.

Digital signature certificate contains at least following statement:

- **Statement claiming that the certificates is a Qualified Certificate according to Annex I and II of the EU Directive 1999/93/EC** {id-etsi-qcs-QcCompliance }, {0.4.0.1862.1.1}

This is a noncritical extension.

A.4 Certificate Revocation List Profile

CRL format is x.509v2 (defined in RFC3280).

CSP follows suggestions in this document when creating the revocation list.

A.4.1 CRL extension

All CRL-s issued by CSP must contain the following fields:

- **Authority Key Identifier** {id-ce-authorityKeyIdentifier}, {2,5,29,35};
- **CRL number** {id-ce-cRLNumber}, {2,5,29,20}.

The **authorityKeyIdentifier** field contains CSP public key identifier whose corresponding private key was used to sign the CRL. This is necessary for creating CSP certificate chain.

The **CRLnumber** field grows sequentially and is the sequence number of CRL issed by CSP.

CSP may also issue *deltaCRL*-s according to requirements specified in RFC3280. The same RFC also discusses the nature of *DeltaCRL*.

CSP may also use *CRL Entry* extensions if possible, following requirements and recommendations presented in RFC3280.

A.5 Example Certificates

Following are two example certificates created based on this profile.

A.5.1 Authentication certificate

CERTIFICATE FIELD	EXAMPLE
VERSION	V3
SERIAL NUMBER	3BD9 1AEB
ISSUER	CN = ESTEID-SK SN = 1 OU = ESTEID O = AS Sertifitseerimiskeskus C = EE E = pki@sk.ee
SIGNATURE ALGORITHM	sha1RSA
VALID FROM	28. January 2007 0:00:00
VALID TO	31. January 2012 23:59:59
SUBJECT	Serial Number=60110260002 G = MARI-LIIS SN = MÄNNIK CN = MÄNNIK,MARI-LIIS,60110260002 OU = authentication O = ESTEID C = EE
PUBLIC KEY	RSA(1024 bits) 3081 8902 8181 00C2 AFE1 0488 4987 6C2D 4382 78FF D4E6 9F2C AEE7 2676 F3E7 33C1 8A38 706C 0F95 DF89 596A 95B8 B808 5A09 9FC7 4390 B642 AE78 AB46 00AF 647A 283B 7A44 7E25 1827 C0F5 06A0 30C1 75C1 8159 FAC5 455F 6BDB 844A 8665 1A36 2126 1370 A480 E9D5 719C 6F7D E8F5 04BF 87BF 25C3 3F20 9635 A273 05EE EB64 20BE A39E 42C6 B1D2 58A6 5425 B302 0301 0001
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)
CRL DISTRIBUTION POINTS	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.sk.ee/crls/esteid/esteid.crl
SUBJECT ALTERNATIVE NAME	RFC822 Name=mari-liis.mannik@eesti.ee
CERTIFICATE POLICIES	[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.10015.1.1.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=none [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.sk.ee/cps/
IDENTIFICATION OF QUALIFIED CERTIFICATE	id-etsi-qcs-QcCompliance
KEY USAGE	Digital Signature , Key Encipherment , Data Encipherment(B0)
BASIC CONSTRAINTS	Subject Type=End Entity Path Length Constraint=None
THUMBPRINT ALGORITHM	sha1
THUMBPRINT	973B 877E 12BB 5302 2EB6 88CC 9D04 6D9C D374 35E1

A.5.2 Digital signature certificate

CERTIFICATE FIELD	EXAMPLE
VERSION	V3
SERIAL NUMBER	3BD9 1AEB
ISSUER	CN = ESTEID-SK SN = 1 OU = ESTEID O = AS Sertifitseerimiskeskus C = EE E = pki@sk.ee
SIGNATURE ALGORITHM	sha1RSA
VALID FROM	28 January 2007 0:00:00
VALID TO	31 January 2012 23:59:59
SUBJECT	Serial Number=60110260002 G = MARI-LIIS SN = MÄNNIK CN = MÄNNIK,MARI-LIIS,60110260002 OU = digital signature O = ESTEID C = EE
PUBLIC KEY	RSA(1024 bits) 3081 8902 8181 00CD 8EAE 9276 61D2 FAB8 BC78 7F56 62F2 C43E 55E2 5E8A 1C75 B373 EEAB 5BAC A563 BF55 4CEE 1EA5 1F54 933F 1969 D50D 2595 52EC A878 4DD8 B121 9A1D B872 9B76 22AB A299 A982 1AA5 0DBB 501F 2B5A 3387 DB2A A75B 56D3 DFD3 E486 2565 5E6A E390 355E 6327 7EF4 5806 6854 F2F2 1FA1 F744 5457 9C62 6F47 3BA4 12F4 5548 2696 4827 3990 0302 0301 0001
CRL DISTRIBUTION POINTS	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.sk.ee/crls/esteid/esteid.crl
CERTIFICATE POLICIES	[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.10015.1.1.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=none [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.sk.ee/cps/
IDENTIFICATION OF QUALIFIED CERTIFICATE	id-etsi-qcs-QcCompliance
KEY USAGE	Non-Repudiation(40)
BASIC CONSTRAINTS	Subject Type=End Entity Path Length Constraint=None
THUMBPRINT ALGORITHM	sha1
THUMBPRINT	973B 877E 12BB 5302 2EB6 88CC 9D04 6D9C D374 35E1