Certificates on the personal identification documents of the Republic of Estonia

Version 6.0
Valid from January 1st 2016

Version information		
Date	**Version**	**Changes/Amendments**
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, E-resident 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 Mobile-ID 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

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). Appendix A describes the technical details and delivers the examples of the certificates.

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

1.1. Table of Contents

1.2. Terms and Abbreviations

The following terms and abbreviations are being used in this document.

1.2.1. Terms

Refer to CPS p.10

Term	Description
ID-card	ID-card is the mandatory identification document for a citizen of the Republic of Estonia and for a citizen of European Union residing in Estonia.
RP-card	RP-card, issued since 2011, is the mandatory identification document for a foreigner residing in Estonia on terms of residence permit or on right of residence.
Digi-ID	Digital identity document is a smart card similar to ID-card which provides the functionality of digital authentication and digital signature in electronic environments.

Term	Description
Resident digi-ID	Digital identity document issued to Estonian citizen or alien who have previously been issued ID card or RP-card or who is applying ID card or RP-card with Digi-ID at the same time.
E-resident digi-ID	Digital identification document issued to a person who has no right and need to apply for ID card or RP card.
Mobile-ID	Digital identity document in the form of Mobile-ID issued by the Republic of Estonia.
E-resident mobile-ID	Digital identity document in the form of Mobile-ID issued by the Republic of Estonia to a person who has no right and need to apply for ID card or RP card.
Document	ID-card, RP-card, Digi-ID and Mobile-ID.
Distinguished name	Unique subject name in the infrastructure of certificates.
Certificate	Digital document where the public key is associated with the owner of the key.
Certificate issuer	Certificate issuing entity - CSP.
Signing certificate	The certificate of CSP which CSP uses to sign the certificates that it issues.
Certificate owner	Subject to whom the certificate has been issued.
Certificate validity period	Period starting at creation of the certificate and ending at certificate validity end time specified at the moment of creation of the certificate. Actual certificate validity period may be shorter due to the certificate possibly being revoked.

1.2.2. Abbreviations

Refer to CPS p.11

Abbreviation	Description
SR	Register of Certification Service Providers (SR - *Sertifitseerimise Register*) according to Estonian Digital Signatures Act.
CSP	Certification Service Provider in correspondence to Estonian Digital Signatures Act.
OID	Object Identifier assigned to a certificate data object in accordance to the standard.

2. List and Purpose of Certificates

There are two types of certificates loaded to the Documents:

1) A certificate for digital authentication, digital signing of e-mails and encryption;
2) A certificate for creation of digital signatures in accordance to the Digital Signatures Act of Estonia.

The certificates are being issued by CSP.

3. Data in Certificates

Certificates must contain the following data:

1) Certificate issuer data;
2) Certificate owner data;
3) Technical certificate data.

The following chapters 3.1 - 3.3 shall provide the description of the data sets. Technical details are covered in annex A.

3.1. Certificate Issuer Details

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

Attribute	OID	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 CSP as in business registry and in SR.	AS Sertifitseerimiskeskus
CN (commonName)	{id-at-commonName} { 2,5,4,3}	DirectoryString: PrintableString	Common name of the certification service.	ESTEID-SK 2011

The certificates may also contain the following issuer (CSP) data:

Attribute	OID	ASN.1 type	Description	Example
E (e-mailAddress)	{1,2,840,113549,1 ,9,1}	DirectoryString: IA5String	E-mail address of the CSP	pki@sk.ee

3.2. Certificate Owner Details

The following mandatory attributes of the certificate owner's distinguished name are presented in the certificates:

Attribute	OID	ASN.1 type	Description	Example
C (countryName)	{id-atcountryName} { 2,5,4,6 }	DirectoryString: PrintableString	Country of origin	EE
O	{id-	DirectoryString:	Type of the certificate	ESTEID[1]

1 O attribute value is different from the example depending on the type of document.

ID-card and RP-card O = ESTEID

Attribute	OID	ASN.1 type	Description	Example
(organization)	atorganization} { 2,5,4,10}	UTF8		
OU (organizationUnit)	{id-atorganizationalUnit } { 2,5,4,11}	DirectoryString: UTF8	Area of use of the certificate	*authentication* or *digital signature*
SN (surName)	{id-at-surName} { 2,5,4,4}	DirectoryString: UTF8	Surnames	MÄNNIK
G (givenName)	{id-at-givenName} { 2,5,4,42 }	DirectoryString: UTF8	Given names	MARI-LIIS
S (serialNumber)	{id-atserialNumber} { 2,5,4,5 }	DirectoryString: PrintableString	Personal identity code	47101010033
CN (commonName)	{id-atcommonName } { 2,5,4,3 }	DirectoryString: UTF8	Comma-separated surnames, first names and personal identity code.	MÄNNIK,MARILIIS, 47101010033

3.3. Certificate Technical Details

The following technical data is stored in the certificates:

1) Format version of the certificate;
2) Certificate serial number assigned by CSP;
3) Signing algorithm of the certificate;
4) Validity period of the certificate;
5) Public key included in the certificate and its presentation algorithm.
6) CSP public key identifier;
7) Person's public key identifier;
8) Key usage of the certificate;
9) Identifier and reference to certificate practice statement;
10) Reference to CRL distribution point;
11) Person's e-mail address (only in certificates facilitating digital authentication);
12) Additional data of CSP;
13) Extended key usage (only in certificates facilitating digital authentication);

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)

14) Identifier of a qualified certificate.

4. Referred and Related Documents

The following documents were used and based on for compiling the certificate profiles in hand:

4.1. Legal Acts of Republic of Estonia

[1] Identity Documents Act, published: https://www.riigiteataja.ee/akt/123032015016&leiaKehtiv;
[2] Digital Signatures Act, published: https://www.riigiteataja.ee/akt/114032014012&leiaKehtiv.

4.2. IETFi Documents

(Internet Engineering Task Force http://www.ietf.org)

[3] RFC5280 - Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, http://www.ietf.org/rfc/rfc5280.txt;
[4] RFC3739 - Internet X.509 Public Key Infrastructure - Qualified Certificates Profile, http://www.ietf.org/rfc/rfc3739.txt.

Appendix A
Additional Certificate-specific Technical Information

A.1 General

Following is presenting detailed description of the contents of the certificate data fields.

A.2 Main Fields of a Certificate

A.2.1 Certificate Format Version (*version*)

The field contains the format version of the certificate.

Documents are using X.509 v3 certificates; the value of this field is thus 2.

A.2.2 Certificate Serial Number Originated from CSP (*serialNumber*)

The field contains the certificate serial number which must be unique across all certificates issued by this CSP.

A.2.3 Certificate Signing Algorithm (*signatureAlgorithm*)

The field contains descriptor of the encryption algorithm which is being used by CSP to sign the issued certificates.

For signing the certificates of the Documents use the RSA and SHA-256 algorithms and the value of this field is thus:

- **sha256WithRSAEncryption** { 1.2.840.113549.1.1.11 }.

A.2.4 Certificate Validity Period (*validity*)

Not valid before and not valid after dates of the certificate are stored in the certificate.

Not valid after date of the certificate matches the end of validity of the Document.

The dates in the certificates are presented in accordance to RFC 5280.

A.2.5 Public Key in the Certificate and its Presentation Algorithm (*subjectPublicKeyInfo*)

The field contains the public key of the certificate owner along with its presentation algorithm.

The following encryption algorithm identifiers (**AlgorithmIdentifier**) are used in certificates of the Documents:

- **rsaEncryption** { 1.2.840.113549.1.1.1 }, 2048 bit keys;

- **ecPublicKey** { 1.2.840.10045.2.1 }, prime256v1 { 1.2.840.10045.3.1.7 }.

In case of ID-card, RP-card and Digi-ID one pair of certificates is issued with encryption algorithm rsaEncryption with key length 2048 bits. In case of Mobile-ID two pairs of certificates are issued with encryption algorithm rsaEncryption with key length 2048 bits and encryption algorithm ecPublicKey with key length 256 bits.

A.3 Certificate Extensions

The following table describes the extensions used in the certificates:

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 facilitating digital authentication)	{id-ce-subjectAltName} {2,5,29,17}	YES	NO
IssuerAltName	{id-ce-issuerAltName} {2,5,29,18}	YES	NO
CRLDistributionPoints	{id-ce-CRLDistributionPoints} {2,5,29,31}	YES	NO
ExtKeyUsage (in certificate facilitating digital authentication)	{id-ce-extKeyUsage} {2,5,29,37}	YES	YES
ExtKeyUsage (in certificate facilitating digital signature)	{id-ce-extKeyUsage} {2,5,29,37}	EI	NO
BasicConstraints	{id-ce-basicConstraints} {2,5,29,19}	YES	NO
qcStatements (in certificate facilitating digital signature)	{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 or not.

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*)

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

Only the **keyIdentifier** field is used.

This is a non-critical 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 RFC5280.

This is a non-critical extension.

A.3.3 Key Usage of the Certificate (*keyUsage*)

The following values are used in the certificates:

- DigitalSignature,
- NonRepudiation,
- KeyEncipherment,
- DataEncipherment.

These values are used as follows:

In certificates facilitating digital authentication:

- DigitalSignature,
- KeyEncipherment,
- dataEncipherment,

In certificates facilitating digital signature only the following value is used:

- nonRepudiation.

This is a **critical** extension.

A.3.4 Certificate Policies (*certificatePolicies*)

The field contains reference to the certification practice statement, certification policy or contract under which the certificate has been issued. The reference also includes the URL and OID identifier.

This is a non-critical 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 non-critical extension.

A.3.6 Person's E-mail Address (*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 e-mail 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).

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		

No	Char	Char code	New char	New char code
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

No	Char	Char code	New char	New char code
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

No	Char	Char code	New char	New char code
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

No	Char	Char code	New char	New char code
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 are presented in hexadecimal form in the table above correspond to UTF-32 encoding specified in the international 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 non-critical extension.

A.3.7 CSP Additional Data (*Issuer Alternative Name*)

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

This extension occurs in the certificate only if issuer certificate contains Subject Alternative Name.

This is a non-critical extension.

A.3.8 Extended Key Usage

The certificate facilitating person's digital authentication, the following values are being used:

- *ClientAuthentication*,
- *SecureEmail*.

This is a **critical** extension in authentication certificate.

This extension is not present in the certificate facilitating digital signature.

A.3.9 Basic Constraints

This extension declares the certificate owner to be an end-entity.

This is a non-critical extension.

A.3.10 Identification of Qualified Certificate (*qcStatements*)

This extension indicates that the certificate has been issued by a CSP complying with requirements set to the CSP's issuing qualifying certificates. This extension is compiled in accordance to ETSI TS 101 862 v 1.3.2.

The digital signature certificate includes at least the following statements:

- Statement claiming that the certificate 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}
- Statement claiming that the private key associated with the certificate is stored on the secure signature creation device in accordance to Annex III of the EU Directive 1999/93/EC {id-etsi-qcs-QcSSCD}, {0.4.0.1862.1.4}

This is a non-critical extension.

A.4 Certificate Revocation List Profile

Certification revocation list (CRL) format is X.509 v2 (defined in RFC 5280).

CSP follows also the recommendations of this document during the creation of certification revocation lists.

A.4.1 CRL Extensions

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

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

On the field **authorityKeyIdentifier**, the identifier of the public key (corresponding to witch the private key was used to sign the CRL) of the CSP is presented. This is necessary for creating CSP certificate chain.

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

CSP may also issue *deltaCRL*s according to the requirements specified in RFC 5280. The same RFC also discusses the nature of *deltaCRL*.

CSP may also use the CRL Entry extensions, following the requirements and recommendations presented in RFC 5280.

A.5 Sample Certificates

The following are example certificates based on this profile:

A.5.1 Digital Authentication Certificate

Certificate Field	Content Example
Version	V3
Serial Number	32 3b b3 3a 2a a6 af 23 4f fe de f2 3b 73 4a ed
Issuer	CN = ESTEID-SK 2011 O = AS Sertifitseerimiskeskus C = EE E = pki@sk.ee
Signature Algorithm	sha256RSA
Valid From	28. jaanuar 2015 09:15:24
Valid To	31. jaanuar 2020 23:59:59
Subject	Serial Number=47101010033 G = MARI-LIIS SN = MÄNNIK CN = MÄNNIK,MARI-LIIS,47101010033 OU = authentication O = ESTEID

Certificate Field	Content Example
	C = EE
Public Key	RSA(2048 bits) 30 82 01 0a 02 82 01 01 00 a9 cd 81 7e fd 38 ed 57 58 e5 90 dd a0 d1 38 a8 99 8a c0 98 69 df d2 fc 63 62 22 d4 b2 b2 34 5f 76 5b 3a 8d 38 8a 64 0b 74 b8 c1 de 12 f9 0e 88 b4 bb 50 f4 9a 4d 84 a9 a3 44 ef e6 55 e0 b9 70 7f 6b 7c 0c 24 6a 60 62 66 5f 12 44 c1 6c 6c 34 a4 ea 8b 21 0b db 5f be 49 66 62 5f 8b 07 63 47 ba 29 5d cd f1 8c 89 54 07 71 09 3d c0 7c ba e1 44 11 c6 69 50 99 79 4f 7a e0 14 69 b1 af 8d fc 91 4a e0 ff dd 31 39 b5 8b 37 b0 05 af c7 ce aa 9e 54 e6 82 f9 25 7a 6a db f3 60 b2 66 f9 62 58 97 77 8f e1 d2 1f 8f 8a be e7 4f cc e3 40 40 f1 f0 4b 41 08 f5 e8 ae a7 0e 55 19 6f 9e 21 5c 1b 19 86 db 1f 7f 93 d1 b9 08 66 15 65 fe b1 c0 fb c3 53 bd 22 24 66 c7 55 f5 db 83 f2 ca 04 cb 5f 8c 7e b9 da 14 f8 78 57 b0 12 ee 82 7e 66 5c 03 6c 4b 2a 4f 2e ad 3f 6a f4 4c 9f 9c 9d e8 e0 59 02 03 01 00 01
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/repository/crls/esteid2011.crl
Subject Alternative Name	RFC822 Name=mari-liis.mannik@eesti.ee
Certificate Policies	[1]Certificate Policy[2]: PolicyIdentifier=1.3.6.1.4.1.10015.1.1.4 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Contract 1.11-9 http://www.sk.ee/cp [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.sk.ee/cps/
Key Usage	Digital Signature , Key Encipherment , Data Encipherment(B0)
Basic Constraints	Subject Type=End Entity Path Length Constraint=None

A.5.2 Digital Signature Certificate

[2] See clause A.3.4 Certificate Policies.

Certificate Field	Content Example
Version	V3
Serial Number	39 9a be 9a ad 4b 67 56 4f fe de ef 6a 48 c0 90
Issuer	CN = ESTEID-SK 2011 O = AS Sertifitseerimiskeskus C = EE E = pki@sk.ee
Signature Algorithm	sha256RSA
Valid From	28. jaanuar 2015 09:15:24
Valid To	31. jaanuar 2020 23:59:59
Subject	Serial Number=47101010033 G = MARI-LIIS SN = MÄNNIK CN = MÄNNIK,MARI-LIIS, 47101010033 OU = digital signature O = ESTEID C = EE
Public Key	RSA(2048 bits) 30 82 01 0a 02 82 01 01 00 ba ea e3 d1 c4 c2 75 71 74 2b 68 14 1f be c3 a1 03 f1 e7 a6 bd 50 8a 98 ab e8 64 08 69 c3 92 52 9e f3 f2 4a 4f ee b6 f8 47 6a 65 d9 62 df b3 a2 9c a6 5c 36 4d 95 22 b4 cd 97 e8 49 0d 6d 63 2d 60 4c fb 31 57 f5 74 33 1c f5 25 ce 76 f4 39 bd 9e f0 34 34 58 7d bf 86 65 c4 a5 52 04 28 ac 25 59 4a 15 58 39 79 82 34 f8 87 24 69 1a 52 33 84 08 90 ab 8a d9 f7 d7 c6 92 60 c4 d4 03 bb 3e 32 91 de 8b b6 37 2e f4 b7 9a c7 fb 7d 28 34 84 11 83 1e b0 71 2d 6d c2 d1 b6 6b 40 34 15 dd 76 99 c2 69 57 c0 96 37 54 e5 76 e7 36 59 0b e7 77 98 26 23 ad 07 a9 8c bc 9c d8 1a 8c ac 4f 04 8b 9a 74 7d 90 6b 1e 68 59 53 e3 66 83 3b 6c 0b 09 ef 09 7d ae 6e 7b 8b 53 ac 51 ad 83 f8 cc bd be b2 b3 80 b9 2b 52 e9 a5 57 a8 29 b3 a6 63 ac 49 5a 88 c8 c6 9d 55 e7 5b 03 b7 3b c7 34 42 61 e2 99 02 03 01 00 01
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://www.sk.ee/repository/crls/esteid2011.crl
Certificate Policies	[1]Certificate Policy[2]: PolicyIdentifier=1.3.6.1.4.1.10015.1.1.4 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Contract 1.11-9 http://www.sk.ee/cp

Certificate Field	Content Example
	[1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.sk.ee/cps/
Identification of Qualified Certificate	id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD
Key Usage	Non-Repudiation(40)
Basic Constraints	Subject Type=End Entity Path Length Constraint=None