Personal Certificates in Estonian Republic identification document

CONTENTS

1. Overview

This document describes profile of personal digital certificates stored on Estonian Republic identification document (ID card) and also presents example certificates.

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

This document is based on the following documents:

A. Legal acts of Estonian Republic

1) Identity Documents Act (as of 12.06.2001)
2) Digital Signatures Act (as of 12.06.2001)
3) Personal Data Protection Act (as of 09.05.2001)
4) Decree of the Minister of Transport and Communications "Teenuse osutajate infosüsteemide auditeerimise kord" (issued 03.10.2000)

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

1) RFC2459 - Internet X.509 Public Key Infrastructure - Certificate and CRL Profile (http://www.ietf.org/rfc/rfc2459.txt)
2) RFC3039 - Internet X.509 Public Key Infrastructure - Qualified Certificates Profile (http://www.ietf.org/rfc/rfc3039.txt)
3) Internet Draft – Internet X.509 Public Key Infrastructure - Certificate and CRL Profile draft-ietf-pkix-new-part1-08.txt (http://www.ietf.org/internet-drafts/draft-ietf-pkix-new-part1-08.txt)

2. Concepts

Following are the short explanations of concepts used in the text.

Concept	Explanation
Identification document	Document identifying its holder and issued on the basis of a legal act
Identification document validity period	Period starting at issuing the identification document 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
SRR	National Register of Certification Service Providers (SRR - *Sertifitseerimise Riiklik Register*) according to Estonian Digital Signatures Act
STO	Certification Service Provider (STO - *Sertifitseerimisteenuse osutaja*) according to Estonian Digital Signatures Act
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 (STO in the context of Digital Signatures Act)
Signing certificate	The certificate of STO which STO 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.

3. List and Purpose of Certificates

Two certificates are stored in the identification document:

1) authentication certificate
2) digital signature certificate

Authentication certificate is issued by a service provider who meets the requirements described in the decree of the Minister of Transport and Communications entitled **"Teenuse osutajate infosüsteemide auditeerimise kord"**.

Digital signature certificate is issued by STO who meets the requirements described in Digital Signatures Act.

The purpose of authentication certificate is to autenthicate its owner in any form of electronic communication requiring personal identification.

The purpose of digital signature certificate is to enable its owner to sign data digitally according to Estonian Digital Signatures Act.

The personal certificates stored in the identification document are valid up to **1100 days** (3 years and 4 days), but no longer than the identification document itself is valid.

4. Data in Certificates

Both personal certificates must contain the following data:

1) certificate issuer data
2) certificate owner data
3) certificate validity data
4) technical certificate data

The following chapters 4.1-4.4 describe content of the data. Technical details are covered in chapters 5 and 6.

4.1. Certificate Issuer Data

Personal certificates contain the following data of certificate issuer (STO):

1) full name (name registered in SRR)
2) register code (in SRR register)

4.2. Certificate Owner Data

Personal certificates contain the following certificate owner data:

1) First name(s)
2) Last name
3) Personal code

4.3. Certificate Validity Data

Personal certificates must contain the following 2 dates and times:

1) date and time of creating the certificate
2) date and time of certificate validity end (certificate expiration)

See also references in chapters 4.4 and 6.2.4

4.4. Technical Certificate Data

Personal certificates contain the following technical certificate data:

1) certificate format version
2) certificate serial number
3) certificate signing algorithm
4) public key in the certificate and its presentation algorithm
5) STO public key identifier
6) person's public key identifier
7) key usage
8) certificate policy identifier and reference
9) reference to CDP (CRL Distribution Point)
10) person's e-mail address (only added if the person wishes to do so)
11) STO additional data
12) extended key usage (only in authentication certificates)
13) STO additional services identifier and reference

5. Names in Certificates

All certificates contain 2 distinguished names: issuer and owner (subject) name. In addition to these, additional name of STO is added in the certificate.
Requirements specified in RFC2459 are considered when encoding all distinguished names. According to this RFC, names of all certificates issued from January 1, 2004 must be encoded as data type UTF8String. This data type matches all name forms used in Estonia and is immediately taken into use for encoding names in certificates. Up to December 31, 2003, the data type PrintableString may be used for encoding names.

Personal certificates contain the distinguished name of signing certificate belonging to STO. The name is in the same form as it is in the register of SRR.

Certificate owner distinguished name (DN) in personal certificates contains the following attributes:

Attribute	Description	Example
CountryName	2-letter country code	‘EE’
O (Organisation)	Certificate type	‘ESTEID’
OU (Organisational Unit)	Certificate field of use	[‘*authentication*’,‘*digital signature’*]
SN (Surname)	Last names	‘Kask’
G (GivenName)	First names	‘Juhan’
Serialnumber	Personal code	‘37011126789’
CN (CommonName)	Last and first names and personal code (separated with commas)	‘Kask,Juhan,37011126789’

Notes.

1. Certificate type “ESTEID” in the *O* field is used to collect personal certificates in identification documents into one branch of certificate directory.

2. Certificate field of usage is defined in *DN* in the field *OU* (*Organisational Unit*) in English (for universal usage). It may be *authentication* (certificate is for authentication purposes) or *digital signature* (certificate is for giving signatures).
The *OU* field is used because of its suitability for this and to ensure compatibility.
According to X.509v3 standard, this information could also be placed elsewhere, e.g. in the field *Description* (OID 2.5.4.13).

3. The attribute *CommonName* uses "comma" as separator, because "space" may also be used in the names themselves (e.g. first name consisting of two or more parts).

6. Addendum

6.1. Additional certificate-specific technical information

Following is the detailed contents of certificate data fields with standard terms.

6.2. Main certificate fields

6.2.1. Certificate format version (“*version” by RFC*)

The field contains certificate format version number.
Identification documents use X.509 v3 certificates, the value of this field is thus 2.

6.2.2. Certificate serial number (*serialNumber*)

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

6.2.3. Certificate signing algorithm (*signatureAlgorithm*)

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

Identification document certificates use the SHA-1 algorithm and the value of this field is thus:

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

6.2.4. Certificate validity period (*validity*)

Certificate validity start time is the time and date of creating the certificate in STO information system. Validity end time of personal certificates is either **1100 days** counting from validity start time, or identification document expiration date and time, whichever is earlier.

Dates in certificates are stored according to RFC2459.

6.2.5. 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 }

6.3. Certificate extensions

Following are the used certificate extensions:

Extension name	Identification document	
	Present?	Critical?
AuthorityKeyIdentifier	**YES**	NO
SubjectKeyIdentifier	**YES**	NO
KeyUsage	**YES**	**YES**
CertificatePolicies	**YES**	NO
SubjectAltName	**YES**	NO
IssuerAltName	**YES**	NO
CRLDistributionPoints	**YES**	NO
ExtKeyUsage (in authentication certificate)	**YES**	**YES**
ExtKeyUsage (in digital signature certificate)	**NO**	NO
Authority Information Access	**YES**	NO
Basic Constraints	**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.

6.3.1. STO public key identifier (*authorityKeyIdentifier*)

The field contains identifier of STO-s public key whose matching private key was used to sign the personal certificate. This is necessry for constructing STO certificate chain.
Only the **keyIdentifier** field is used.

This is a noncritical extension.

6.3.2. 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 STO). Method 1 is used according to RFC2459.

This is a noncritical extension.

6.3.3. Key usage (*keyUsage*)

The following values are used in personal certificates:

- **digitalSignature**
- **nonRepudiation**
- **keyEncipherment**
- **dataEncipherment**

They are used as follows:

In authentication certificate
- digitalSignature
- keyEncipherment
- dataEncipherment

In digital signature certificate
- nonRepudiation

This is a **critical** extension.

6.3.4. 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.

6.3.5. CRL Distribution Points (*cRLDistributionPoints*)

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

This is a noncritical extension.

6.3.6. 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 address is created from the person's first and last name(s), underscore and four random digits. The address domain 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. Other characters besides dash are replaced with the dot character. The following character substitutions are made:

š – s	ž – z
õ – o	ä – a
ö – o	ü – y

Example e-mail address: mari.sert_0123@eesti.ee

This is a noncritical extension.

6.3.7. STO additional data (*IssuerAltName*)

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

This is a noncritical extension.

6.3.8. 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.

6.3.9. Additional STO services (*AuthorityInformationAccess*)

The field contains additional information about STO services and is completed by STO.
For example, if STO offers OCSP (*Online Certificate Status Protocol*) service, this field contains its location as URL.

This is a noncritical extension.

6.3.10. Basic Constraints

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

This is a noncritical extension.

6.4. Certificate Revocation List Profile

CRL format is x.509v2 (defined in RFC2459).
STO follows suggestions in this document when creating the revocation list.

6.4.1. CRL extension

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

- **Authority Key Identifier**
- **CRL number**

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

The **CRLnumber** field grows sequentially and is the sequence number of CRL issed by STO.
STO may also issue *deltaCRL*-s according to requirements specified in RFC2459. The same RFC also discusses the nature of *DeltaCRL*.
STO may also use *CRL Entry* extensions if possible, following requirements and recommendations presented in RFC2459.

6.5. Example Certificates

Following are two example certificates created based on this profile.

6.5.1. Authentication certificate

FIELD NAME IN ESTONIAN	CERTIFICATE FIELD	EXAMPLE
SERTIFIKAADI VORMINGU VERSIOON	VERSION	V3
STO-PÕHINE UNIKAALNE JÄRJEKORRANUMBER	SERIAL NUMBER	3BD9 1AEB
STO ERALDUSNIMI	ISSUER	CN = ESTEID-SK SN = 1 OU = ESTEID O = AS Sertifitseerimiskeskus C = EE E = pki@sk.ee
SERTIFIKAADI SIGNEERIMISALGORITM	SIGNATURE ALGORITHM	sha1RSA
SERTIFIKAADI KEHTIVUSE ALGUS	VALID FROM	28. jaanuar 2002. A. 0:00:00
SERTIFIKAADI KEHTIVUSE LÕPP	VALID TO	31. jaanuar 2005 23:59:59
SERTIFIKAADI ERALDUSNIMI	SUBJECT	Serial Number=60110260002 G = MARI SN = SERT CN = SERT,MARI,60110260002 OU = authentication O = ESTEID C = EE
AVALIK VÕTI (1024 bitti)	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
SERTFIKAADI LISAKASUTUSVALDKOND	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)
TÜHISTUSNIMEKIRJADE LEVITUSPUNKTID	CRL DISTRIBUTION POINTS	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.sk.ee/crls/esteid/esteid.crl
ISIKU E-POSTI AADRESS	SUBJECT ALTERNATIVE NAME	RFC822 Name=mari.sert_0123@eesti.ee
SERTIFITSEERIMISPÕHIMÕTTED	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/
SERTIFIKAADI PÕHISKASUTUS-VALDKOND	KEY USAGE	Digital Signature , Key Encipherment , Data Encipherment(B0)
BASIC CONSTRAINTS	BASIC CONSTRAINTS	Subject Type=End Entity Path Length Constraint=None
RÄSI ALGORITM	THUMBPRINT ALGORITHM	sha1
RÄSI	THUMBPRINT	973B 877E 12BB 5302 2EB6 88CC 9D04 6D9C D374 35E1

6.5.2. Digital signature certificate

FIELD NAME IN ESTONIAN	CERTIFICATE FIELD	EXAMPLE
SERTIFIKAADI VORMINGU VERSIOON	VERSION	V3
STO-PÕHINE UNIKAALNE JÄRJEKORRANUMBER	SERIAL NUMBER	3BD9 1AEB
STO ERALDUSNIMI	ISSUER	CN = ESTEID-SK SN = 1 OU = ESTEID O = AS Sertifitseerimiskeskus C = EE E = pki@sk.ee
SERTIFIKAADI SIGNEERIMISALGORITM	SIGNATURE ALGORITHM	sha1RSA
SERTIFIKAADI KEHTIVUSE ALGUS	VALID FROM	28.jaanuar 0:00:00
SERTIFIKAADI KEHTIVUSE LÕPP	VALID TO	31.jaanuar 23:59:59
SERTIFIKAADI ERALDUSNIMI	SUBJECT	Serial Number=60110260002 G = MARI SN = SERT CN = SERT,MARI,60110260002 OU = digital signature O = ESTEID C = EE
AVALIK VÕTI (1024 bitti)	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
TÜHISTUSNIMEKIRJADE LEVITUSPUNKTID	CRL DISTRIBUTION POINTS	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.sk.ee/crls/esteid/esteid.crl
SERTIFITSEERIMISPÕHIMÕTTED	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/
SERTIFIKAADI PÕHIKASUTUS-VALDKOND	KEY USAGE	Non-Repudiation(40)
BASIC CONSTRAINTS	BASIC CONSTRAINTS	Subject Type=End Entity Path Length Constraint=None
RÄSI ALGORITM	THUMBPRINT ALGORITHM	sha1
RÄSI	THUMBPRINT	973B 877E 12BB 5302 2EB6 88CC 9D04 6D9C D374 35E1