Organisation Certificates and CRL profiles of SK

Version 3.0
Valid from 22.06.2016

Version information		
Date	**Version**	**Changes/amendments**
22.06.2016	3.0	Approved version
24.03.2016	2.1	Draft of version 3.0. Chapter 2.1 - removed exeption for SHA-1 Signature Algorithm; Chapter 2.2.1 - added Qualified Certificate Identifier.
13.01.2015	2.0	Approved version
14.11.2014	1.5	Draft of version 2.0. - Chapter 2.1 - updated list of allowed key algorithms; - Chapter 3.1 - changed signature algorithm of CRL; - Chapter 4 - updated list of referred and related documents.
20.06.2014	1.4	- the term “web server certificate” replaced with “SSL server certificate”; - updated and amended the certificate technical profile; - added additional extension constraints to organisation certificate profile; - restructuring.
14.02.2011	1.3	- p 1 – Software signing certificate removed from certificates section; - p 3.2.2 – added „Data Encipherment“ value for authentication and encryption certificates; - p 3.3.2 – updated OID value and CPS reference.
10.05.2010	1.2	Updated list of certificate types in chapter 1. Specified certificate field descriptions and changed field value for „CRL Distribution Point”.
13.08.2009	1.1	Updated profiles to meet the requirements originated from Digital Signatures Act. Removed the term “device certificates”.
15.02.2005	1.0	Primary version.

1. Introduction

The document in hand determines the profiles of certificates issued by KLASS3-SK and the minimum requirements to these. The certificate profile may be customised during applying for the certificate.

With the term “organisation certificate”, we mean the certificates issued to legal bodies. The organisation certificates are divided into following types:

- Digital Stamp;
- SSL server;
- Client Autent server;
- VPN;
- Crypto; and
- B4B.

SSL server certificate is suitable for web server (https), ftp server (ftps) and other SSL/TLS servers.

1.1. Table of Contents

1.2. Terms and Abbreviations

1.2.1. Terms

Refer to CPS p.10

Term	Description
Object Identifier	Unique code assigned to an object (OID).

Term	Description
Certification Authority	Organizational unit issuing certificates.
Certification Policy	A set of rules that determine the field of use of issued certificates by certain user groups or how the certificate is applied for certain applications and common security requirements implemented.
Certification Practice Statement	The description of good practice of issuing, managing, revoking, renewing and re-keying of the certificates issued by the CA.
Shared Control	A security measure to limit the access to the security objects only in presence of two or more authorised key agents.

1.2.2. Abbreviations

Refer to CPS p.11

Abbreviation	Description
CP	Certification Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
FQDN	Fully Qualified Domain Name
OID	Object Identifier
SK	AS Sertifitseerimiskeskus, provider of the certification service
EECCRCA	EE Certification Centre Root CA

2. Technical Profile of the Certificate

Organisation certificate is compiled in accordance with the X.509 version 3 and guided by suggestive standard RFC 5280 [2].

2.1. Certificate Body

Field	OID	Compulsory	Value	Changeable	Description
Version		yes	Version 3	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		yes		no	Distinguished name of

Field	OID	Compulsory	Value	Changeable	Description
Distinguished name					the certificate issuer
Common Name (CN)	2.5.4.3	yes	KLASS3-SK 2010		Certificate authority
Organizational Unit (OU)	2.5.4.11	yes	Sertifitseerimisteenused		Identity of certification service
Organization (O)	2.5.4.10	yes	AS Sertifitseerimiskeskus		Organisation
Country (C)	2.5.4.6	yes	EE		Country code: EE – Estonia
Subject Distinguished Name		yes		yes	Unique subject (device) name in the infrastructure of certificates.
Serial Number	2.5.4.5	yes			Registry code of the certificate holder as described in certificate application. Not in use for SSL server certificates.
Common Name (CN)	2.5.4.3	yes			Common name of the certificate – client name and area of application on request. Not required for SSL server certificates, if used, also the Subject Alternative Name must be filled at least with the IP address or with the domain name.
Organizational Unit (OU)	2.5.4.11	no			The name of organisational unit as described in certificate application. If SK's security module is used, the English names of the products.
Organization (O)	2.5.4.10	yes			Subject (organisation)

Field	OID	Compulsory	Value	Changeable	Description
					name as stated in certificate application.
Locality (L)	2.5.4.7	yes			Name of the locality of the subject. Not required if State (S) is used.
State (S)	2.5.4.8	yes			State or province name of the subject as described in certificate application. Not required if Locality (L) is used.
Country (C)	2.5.4.6	yes			Country code of the subject in accordance with RFC 5280.
Valid from		yes		no	First date of certificate validity encoded in accordance with RFC 5280.
Valid to		yes		no	The last date of certificate validity encoded in accordance with RFC 5280.
Subject Public Key		yes	RSA 2048, RSA 4096 või ECC 256, ECC 320, ECC 384, ECC 512, ECC 521	no	Public key created in RSA algorithm in accordance with RFC 4055. Public key of ECC algorithm is created in accordance with RFC 5639 or FIPS Publication 186-4.
Signature		yes		no	Confirmation signature of the certificate issuer authority.

2.2. *Certificate Extensions*

2.2.1. Basic Constraints of Organisation Certificate

Extension	OID	Values and limitations	Criticality	Compulsory
Basic Constraints	2.5.29.19	SubjectType=End Entity Path Length Constraint=None	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/klass3/klass3-2010.crl	Non-critical	yes
Key Usage	2.5.29.15	Refer to p 2.2.2 "Additional Constraints"	Critical	yes
Extended Key Usage	2.5.29.37	Refer to p 2.2.2 "Additional Constraints"	Non-critical	yes
AuthorityKeyIdentifier	2.5.29.35		Non-critical	yes
SubjectKeyIdentifier	2.5.29.14		Non-critical	yes
id-pe-qcStatements[1]	1.3.6.1.5.5.7.1.3	Qualified Certificate Identifier. The certificate shall contain the following identifiers: • Qualified Certificate Identifier pursuant to Annex I and II of the EU directive on electronic signatures 1999/93/EC {id-etsi-qcs-QcCompliance }, {0.4.0.1862.1.1} • Identifier that private key associated with the certificate is stored on the secure signature creation device pursuant to Annex III of the EU Directive 1999/93/EC {id-etsi-qcs-QcSSCD}, {0.4.0.1862.1.4}	Non-critical	yes

[1] Only Digital Stamp certificate includes this extension. 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.

2.2.2. Additional Constraints

Extension	OID	Values and limitations	Criticality	Compulsory
Authority Information Access	1.3.6.1.5.5.7.1.1	caIssuers (OID 1.3.6.1.5.5.7.48.2) http://www.sk.ee/certs/KLASS3-SK_2010_ECCRCA.pem.crt ocsp (OID 1.3.6.1.5.5.7.48.1) http://ocsp.sk.ee/ssl	Non-critical	yes

2.2.3. Variable Extensions

Extension	Digital Stamp	SSL server	Client Autent server	VPN	Crypto	B4B
Key Usage						
Non-Repudiation	X					
Digital Signature		X	X	X	X	X
Data Encipherment			X		X	
Key Encipherment		X	X	X	X	X
Key Agreement						
Extended key usage						
Client Authentication			X	X		X
Server Authentication		X				
Code Signing						
Email Protection						
IPSEC End System				X		
IPSEC Tunnel						
IPSEC User						
Other extensions						
Subject Alternative Name[2]						
- rfc822Name			X			
- DNSName		X				
- IPAddress		X				

[2] In case of SSL server certificate, at least one of the Subject Alternative Name fields DNSName or IPAddress must be filled with at least one value. Both fields can be filled and with multiple values. In case of Client Autent server, the e-mail field rfc822Name as part of Subject Alternative Name is not required.

2.3. Certificate Policies

Certificate Policies - OID 2.5.29.32.

2.3.1. General Terms

There can be more than one record for certificate policy in an organisation certificate.

Intermediate CA certificate MUST include the reference to the certification policy of the certificate issuer.

2.3.2. Certificate Policy of Organisation Certificate

Element	Type	Value
PolicyIdentifier		1.3.6.4.1.10015.7.1.3
PolicyQualifier		
User Notice	UTF8 string	Asutuse sertifikaat. Corporate ID.
CPS		https://www.sk.ee/repository

The certificate policy extension is non-critical.

3. Profile of Certificate Revocation List

SK issues CRLs in accordance to the guides of RFC 5280.

3.1. Main Fields

Field	OID	Compulsory	Value	Description
Version		yes	Version 2	CRL format version pursuant to X.509.
Signature Algorithm			sha256WithRSAEncryption	CRL signing algorithm pursuant to RFC 5280
Issuer Distinguished Name		yes		Distinguished name of certificate issuer
Common Name (CN)	2.5.4.3	yes	KLASS3-SK 2010	Name of certification authority
Organizational Unit (OU)	2.5.4.11	yes	Sertifitseerimisteenused	Identity of certification service of SK
Organization (O)	2.5.4.10	yes	AS Sertifitseerimiskeskus	Organisation

Field	OID	Compulsory	Value	Description
Country (C)	2.5.4.6	yes	EE	Country code in accordance to RFC 5280.
Effective Date				Date and time of CRL issuance. Information is coded in accordance to RFC 5280.
Next Update				Date and time of issuance of the next CRL. The conditions are also described KLASS3-SK CP chapter 2.4.2.
Revoked Certificates				List of revoked certificates.
Serial Number				Serial number of the certificate revoked.
Revocation Date				Date and time of revocation of the certificate. Information is coded in accordance to RFC 5280.

Reason Code	2.5.29.21			Reason code for certificate revocation. The following codes are used:
				1 – Loss of key (keyCompromise);
				2 – CA loss of key (cACompromise);
				3 – Name change (affiliationChanged);
				4 – Replacement with new certificate (superseded);
				5 – Ceased operations of organization (cessationOfOperation)

Signature				Confirmation signature of the authority issued the CRL.

3.2. CRL Extensions

Field	OID	Values and limitations	Criticality
CRL Number	2.5.29.20	CRL sequence number	Non-critical

Field	OID	Values and limitations	Criticality
Issuing Distribution Point	2.5.29.28	CRL distribution point	Non-critical

4. Referred and Related Documents

[1] AS Sertifitseerimiskeskus, Certification Practice Statement;

[2] RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;

[3] RFC 2527 – Request For Comments 2527, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework;

[4] 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;

[5] RFC 3279 - Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;

[6] RFC 5639 - Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation;

[7] FIPS PUB 186-4.