Profile of institution certificates and Certificate Revocation List

Version 1.3

Table of contents

Document versions

Version number	***Date***	***Description***
1.3	14.02.2011	-p.1 – deleted from the certificates section: Software signing certificate -p3.2.2 – the Data Encipherment value was added to the authentication and encryption certificate P3.3.2 – changed were the OID value and the CPS address
1.2	10.05.2010	Point 1 was supplemented, with names of different certificates listed. Clarified were the certificate field descriptions and the value of the CRL Distribution Point field was changed.
1.1	13.08.2009	Ensured was compliance of the profile with the requirements of the Digital Signatures Act. The term "device certificates" was removed.
1.0	15.02.2005	First version

1. General information

The term "**institution certificate**" denotes a certificate issued to an organisation. These are the institution certificates:

- **Digital stamp certificate**
- **Web server certificate**
- **Client Autent server certificate**
- **VPN certificate**
- **Cryptocertificate**
- **B4B certificate**

This document describes profiles of institution certificates and their minimum requirements. You can agree on a precise certificate profile when applying for the certificate.

2. Terms and their acronyms

Term	***Description***
OID	*Object Identifier – the standards-regulated code for an object*
FQDN	*Fully Qualified domain name – the full name of a network device*

3. Certificate's technical profile

The institution certificate is created in compliance with the X.509 version 3 standard and the guidelines of the recommended RFC 3280 [1] standard.

3.1. Main fields

Field	***OID***	***Compulsory***	***Values***	***Amendable during application for certificate***	***Description***
Version		yes	Version 3	no	Certificate format's version number
Serial Number		yes		no	Certificate's unique sequence number
Signature Algorithm		yes		no	sha1withRSA
Issuer Distinguished Name		yes		no	Distinguished name of certificate issuer

Field	*OID*	*Compulsory*	*Values*	*Amendable during application for certificate*	*Description*
Common Name (CN)	2.5.4.3	yes	KLASS 3-SK 2010		Name of certifier
Organizational Unit (OU)	2.5.4.11	yes	Sertifitseerimisteenused (Certification services)		AS Sertifitseerimiskeskus: service type
Organization (O)	2.5.4.10	yes	AS Sertifitseerimiskeskus		Organisation
Country (C)	2.5.4.6	yes	EE		Country code: EE – Estonia
E-Mail (E)		yes	pki@sk.ee		AS Sertifitseerimiskeskus: contact e-mail address
Subject Distinguished Name		yes		yes	Distinguished name, name or pseudonym of certificate owner (device)
E-mail (E)					Contact e-mail address
Serial Number	2.5.4.5	yes			Registration code of the legal person indicated in the certificate application. This field is not used for the web server certificate
Common Name (CN)	2.5.4.3	yes			Certificate common name: client's name and, if desired, usage function. For web certificate: FQDN
Organizational Unit (OU)	2.5.4.11	no			Name of organisation's subunit, indicated in the certificate application. If a SK-issued security device is used, this contains the English-language product names

Field	*OID*	*Compulsory*	*Values*	*Amendable during application for certificate*	*Description*
Organization (O)	2.5.4.10	yes			Name of client (institution), indicated in the certificate application
Locality (L)	2.5.4.7	no			Name of client location's urban/rural settlement, indicated in the certificate application
State (S)	2.5.4.8	no			Name of client location's county, indicated in the certificate application
Country (C)	2.5.4.6	yes			Client location's country code, indicated in the certificate application, in compliance with the RFC 3280 guidelines
Valid From		yes		no	Certificate validity start time. Information coded in compliance with the RFC 3280 guidelines
Valid To		yes		no	Certificate validity expiry time. Information coded in compliance with the RFC 3280 guidelines
Subject Public Key		yes		no	Public key created based on RSA algorithm
Signature		yes		no	Confirmation signature of the certifier that issued the certificate

3.2. Certificate extensions

3.2.1. Institution certificate's unchangeable extensions

Extension	*OID*	*Values and restrictions*	*Critical*	*Compulsory*
Basic Constraints	2.5.29.19	Subject Type=End Entity Path Length Constraint=None	no	yes
CRL Distribution Points	2.5.29.31	http://www.sk.ee/crls/klass3/klass3-2010.crl	no	yes
Key Usage	2.5.29.15	See point 3.2.2. "Institution certificate's changeable extensions"	yes	yes
Enhanced Key Usage	2.5.29.37	See point 3.2.2. "Institution certificate's changeable extensions"	no	yes
AuthorityKeyIdentifier	2.5.29.17		no	yes
SubjectKeyIdentifier	2.5.29.35		no	yes

3.2.2. Institution certificate's changeable extensions

	Digital stamp	*WWW server*	*Authentication*	*VPN*	*Encryption*	*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						
	Enhanced 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					
- RFC822 Name			X			
- DNS name		X				
- IP		X				

	Digital stamp	*WWW server*	*Authentication*	*VPN*	*Encryption*	*B4B*

3.3. Certification policies, OID: 2.5.29.32

3.3.1. General information

The certificate CAN contain more than one certification policy entries.
The institution certificate MUST contain an entry describing the certification policy of the certificate issuer.

3.3.2. Institution certificate's certification policy

Element	*Type*	*Value*
Certifier's certification policy		
Policy Identifier		1.3.6.4.1.10015.7.1.2.2
Policy Qualifier		
User Notice	UTF8 string	Asutuse sertifikaat (Institution certificate). Corporate ID.
CPS		http://www.sk.ee/cps

The certification policy extension is not critical.

4. Certificate Revocation List profile

AS Sertifitseerimiskeskus issues Certificate Revocation Lists pursuant to the RFC 3280 guidelines.

4.1. Main fields

Field	*OID*	*Compulsory*	*Values*	*Description*
Version		yes	Version 2	CRL format version pursuant to X.509
Signature Algorithm			sha1withRSA	CRL signing algorithm pursuant to RFC 3280
Issuer Distinguished Name		yes		Distinguished name of certificate issuer
Common Name (CN)	2.5.4.3	yes	KLASS3-SK	Name of certifier
Organizational Unit (OU)	2.5.4.11	yes	Sertifitseerimisteenused (Certification	AS Sertifitseerimiskeskus: service type

Field	*OID*	*Compulsory*	*Values*	*Description*
			services)	
Organization (O)	2.5.4.10	yes	AS Sertifitseerimiskeskus	Organisation
Country (C)	2.5.4.6	yes	EE	Country code in compliance with the RFC 3280 guidelines
Effective Date				CRL issue date and time. Information coded in compliance with the RFC 3280 guidelines
Next Update				Next CRL issue date and time. The CRL issue conditions are also described in this CP point 2.4.2
Revoked Certificates				List of revoked certificates
Serial number				Revoked certificate number
Revocation date				Revocation date and time. Information coded in compliance with the RFC 3280 guidelines
Reason Code	2.5.29.21			Reason code for certificate revocation. The following reason codes can be used in this field: 1 – key loss *(keyCompromise)*; 2 – CA key loss *(cACompromise);* 3 – name change *(affiliationChanged);* 4 – replacement with new certificate *(superseded);* 5 – organisation ceases operations *(cessationOfOperation).*
Signature				Confirmation signature of the certifier that issued the CRL

4.2. CRL extensions

Field	*OID*	*Values and restrictions*	*Critical*
CRL Number	2.5.29.20	CRL sequence number	no

Field	*OID*	*Values and restrictions*	*Critical*
Issuing Distribution Point	2.5.29.28	CRL distribution point	no

5. Document references

[1] RFC 3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile