Certificate, OCSP and CRL Profile for Intermediate CA Issued by SK

Version 3.0
Valid from 01.01.2017

Version and Changes		
Version	**Date**	**Changes/amendments**
3.0	01.01.2017	Changed document structure; Added chapter 4, OCSP Profile; Improved certificate field descriptions; Chapter 3.2.1 – added Qualified Certificate Statement extension; Improved chapter 6, Referred and related Documents;
2.0	17.12.2015	Changed chapter 1. General Changed chapter 3. Technical certificate profile Changed chapter 3.1. Main fields Changed chapter 3.2. Certificate extensions Changed chapter 3.3. Certificate Policies, (OID: 2.5.29.32) Changed chapter 4. CRL Profile Changed chapter 4.1.CRL profile main fields Changed chapter 5. Referred and related documents
1.1	01.10.2010	Initial version

1. Introduction

The document describes minimal profile requirements for intermediate certificates issued by EE Certification Centre Root CA. Also for CRL-s and OCSP responder certificates.
The exact profile of the certificate may be further agreed upon a certificate application.

1.1 Abbreviations

Acronym	Definition
CA	Certificate Authority
CP	Certificate Policy
CPS	Certification Practice Statement. This document is a CPS.
CRL	Certificate Revocation List
OCSP	Online Certificate Status Protocol
OID	Object Identifier, a unique object identification code
SK	AS Sertifitseerimiskeskus, Certification Service provider
ETSI	European Telecommunications Standards Institute
EECCRCA	EE Certification Centre Root CA

2. Technical Profile of the Certificate

Intermediate CA and OCSP responder certificate is compiled in accordance with the X.509 version 3, IETF RFC 5280 [1] and clause 6.6 of ETSI EN 319 411-1 [6].

2.1 Certificate Body

Field	OID	Mandatory	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 or sha384WithRSAEncryption	no	Signature algorithm in accordance to RFC 5280 [1]
Issuer Distinguished name		yes		no	Distinguished name of the certificate issuer
Common Name (CN)	2.5.4.3	yes	EE Certification Centre Root CA		Root certificate authority name
Organisational Unit (OU)	2.5.4.11	yes	Certification services		Identity of certification service
Organisation (O)	2.5.4.10	yes	AS Sertifitseerimiskeskus		Organisation name
Country (C)	2.5.4.6	yes	EE		Country code: EE – Estonia (2 character ISO 3166 country code [7])
E-mail (E)		yes	pki@sk.ee		Contact address
Valid from		yes		no	First date of certificate validity.
Valid to		yes		no	The last date of certificate validity.
Subject Distinguished Name		yes		yes	Unique subject (device) name in the infrastructure of certificates.
Common Name (CN)	2.5.4.3	yes		yes	Intermediate CA name (e.g KLASS3-SK 2016 ; EID-SK 2016)
Organisational Unit (OU)	2.5.4.11	no		yes	Identity of certification service

Field	OID	Mandatory	Value	Changeable	Description
OrganisationName (O)	2.5.4.10	yes		yes	Subscriber (organisation) name as stated in certificate application.
Organisation Identifier	2.5.4.97	yes	NTREE-10747013	yes	Identification of the subject organisation different from the organisation name as specified in clause 5.1.4 of ETSI EN 319 412-1 [3]
LocalityName (L)	2.5.4.7	no		yes	Name of the locality of the subject.
State (ST)	2.5.4.8	no		yes	State or province name of the subject as described in certificate application.
Country (C)	2.5.4.6	yes		yes	Country code of the Subscriber in accordance with ISO 3166 [7]
Subject Public Key		yes	RSA 2048, RSA 4096	no	Public key created in RSA algorithm [8] in accordance with RFC 4055 [2]
Signature		yes		no	Confirmation signature of the certificate issuer authority.

2.2 Certificate Extensions

2.2.1 Common Extensions of Organisation Certificates

Extension	OID	Values and limitations	Criticality	Mandatory
Basic Constraints	2.5.29.19	Subject Type=CA Path Length Constraint=0 (For OCSP Responder: Subject Type=End Entity	Critical	yes

Extension	OID	Values and limitations	Criticality	Mandatory
		Path Length Constraint=None)		
Key Usage	2.5.29.15	Refer to p 3.2.2 "Variable Extensions "	Critical	yes
Certificate Policies	2.5.29.32	Refer to p 3.2.3"Certificate policy"	Non-critical	yes
Name Constraints	2.5.29.30	Permitted=None Excluded [1]Subtrees (0..Max): DNS Name="" [2]Subtrees (0..Max): IP Address=0.0.0.0 Mask=0.0.0.0 [3]Subtrees (0..Max): IP Address=0000:0000:0000:0000:0000:0000:0000:0000 Mask=0000:0000:0000:0000:0000:0000:0000:0000	Non-critical	no
CRL Distribution Points	2.5.29.31	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.sk.ee/repository/crls/eeccrca.crl	Non-critical	yes (Not included in OCSP responder certificates)
Extended Key Usage	2.5.29.37	Refer to p 3.2.2 "Variable Extensions "	Non-critical	yes
AuthorityKeyIdentifier	2.5.29.35	SHA-1 hash of the public key used to sign the ceritificate	Non-critical	yes
SubjectKeyIdentifier	2.5.29.14	SHA-1 hash of the public key used to sign the ceritificate	Non-critical	yes
Authority Information Access	1.3.6.1.5.5.7.1.1		Non-critical	yes
OCSP	1.3.6.1.5.5.7.48.1	http://ocsp.sk.ee/CA	Non-critical	yes
caIssuers	1.3.6.1.5.5.7.48.2	http://www.sk.ee/certs/EE_Certification_Centre_Root_CA.der.crt	Non-critical	yes
Qualified Certificate Statement	1.3.6.1.5.5.7.1.3	NULL	Non-critical	no

Extension	OID	Values and limitations	Criticality	Mandatory
id-etsi-qcs-semanticsId-Legal	0.4.0.194121.1.2	NULL	Non-critical	no
id-pkix-ocsp-nocheck	1.3.6.1.5.5.7.48.1.5	NULL	Non-critical	no (Used only in OCSP Responder certificates)

2.2.2 Variable Extensions

Extension	Intermediate CA certificate	OCSP Responder certificate
Key usages		
Certificate signing	x	x
CRL signing	x	x
Qualified Certificate Statement[4]		
id-etsi-qcs-semantics-identifiers	x	
Extended key usage		
OCSP Signing	x	x
Client Authentication	x	
Secure Email	x	

2.2.3 Certificate Policy

OID of the extension: 2.5.29.32. The extension is marked non-critical.

The certificate policies extension contains a sequence of one or more policy information terms, each of which consists of an object identifier (OID) and optional qualifiers.
Certificate policies must conform exactly to those certificate profiles, under which certificates are issued. [1]

3. OCSP Profile

OCSP v1 according to [RFC 6960] [5]

Field	Mandatory	Value	Description
ResponseStatus	yes	0 for successful or error code	Result of the query
ResponseBytes			
ResponseType	yes	id-pkix-ocsp-basic	Type of the response
BasicOCSPResponse	yes		
tbsResponseData	yes		
Version	yes	1	Version of the response format
responderID	yes	C=EE, ST=Harjumaa, L=Tallinn, O=AS Sertifitseerimiskeskus, CN= EECCRCA OCSP RESPONDER YYYY-MM	Distinguished name of the OCSP responder Note: the Common Name will vary each month and includes the month in YYYYMM format
producedAt	yes		Date when the OCSP response was signed
Responses	yes		
certID	yes		Serial number of the certificate
certStatus	yes		Status of the certificate
revocationTime	no		Date of revocation or expiration of certificate
revocationReason	no		Code for revocation Reason according to RFC 5280 [1]
thisUpdate	yes		Date when the status was queried from database
signatureAlgorithm	yes	sha256WithRSAEncryption	
signature	yes		
certificate	yes		Certificate corresponding to the

Field	Mandatory	Value	Description
			private key used to sign the response.

OCSP nonce and no extensions are supported.

4. Profile of Certificate Revocation List

SK issues CRL's in accordance to the guides of RFC 5280 [1]

4.1 CRL main fields

Field	OID	Mandatory	Value	Description
Version		yes	Version 2	CRL format version pursuant to X.509.
Signature Algorithm		yes	sha256WithRSAEncryption	CRL signing algorithm pursuant to RFC 5280 [1]
Issuer Distinguished Name		yes		Distinguished name of certificate issuer
Common Name (CN)	2.5.4.3	yes	EE Certification Centre Root CA	Name of certification authority
Organisation Identifier	2.5.4.97	yes	NTREE-10747013	Identification of the issuer organisation different from the organisation name. Certificates may include one or more semantics identifiers as specified in clause 5.1.4 of ETSI EN 319 412-1 [3]
Organisational Unit (OU)	2.5.4.11	yes	Sertifitseerimisteen used	Identity of certification service of SK

Field	OID	Mandatory	Value	Description
Organisation (O)	2.5.4.10	yes	AS Sertifitseerimiskeskus	Organisation
Country (C)	2.5.4.6	yes	EE	Country code: EE – Estonia (2 character ISO 3166 country code [7])
Effective Date				Date and time of CRL issuance.
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.
Reason Code	2.5.29.21			Reason code for certificate revocation. 1 – *(keyCompromise)*; 2 – *(cACompromise);* 3 – *(affiliationChanged);* 4 – *(superseded);* 5 – *(cessationOfOperation).*
Signature				Confirmation signature of the authority issued the CRL.

4.2 CRL Extensions

Field	OID	Values and limitations	Criticality
CRL Number	2.5.29.20	CRL sequence number	Non-critical
Authority Key Identifier[1]	2.5.29.35	Matching the subject key identifier of the certificate	Non-critical

[1] SHA-1 hash of the public key corresponding to the private key used to sign the CRL is presented.

Field	OID	Values and limitations	Criticality
Issuing Distribution Point	2.5.29.28	Distribution Point Name: Full Name: URL=http://www.sk.ee/repository/crls/eeccrca.crl Only Contains User Certs=No Only Contains CA Certs=No Indirect CRL=No	Critical

5. Referred and Related Documents

[1] RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
[2] 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;
[3] ETSI EN 319 412-1 v1.1.1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures;
[4] ETSI EN 319 412-5 v2.2.2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements;
[5] RFC 6960 – X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP;
[6] ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
[7] ISO 3166 Codes;
[8] RFC 3279 - Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.