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

Version 3.3
Valid from 17.02.2022

Version and Changes		
Version	**Date**	**Changes/amendments**
3.3	17.02.2022	• Added root CA SKID Solutions ROOT G1R (RSA) and SK ID Solutions ROOT G1E (ECC) definition and references; • Chapter 4.2 - improved CRL Extensions description; • Amended document overall wording and references; • Corrected references in point 2.2.1. • Chapter 2.1 - added random to certificate serial number description; added signature algorithm ecdsa-with-sha384; added subject public key length ECC P384; • Chapter 3 – changed responderID value and description.
3.2	30.06.2020	• Chapter 3 – improved OCSP *nonce* usage. Changed OCSP ResponderID value for EECCRCA and EE-GovCA2018; • Chapter 2.2.2 – added information about timestamping certificate; Harmonized key usage values according issued certificates; • Chapter 4 – added “invalidityDate” extension; • Added EE-GovCA2018 acronym definition
3.1	04.01.2019	• Added new root certificate EE-GovCA2018 information • Changed chapter 2.1 – added new key and signature ECDSA algorithms; added “organisation identifier” in issuer DN; • Changed chapter 2.2 – fixed OCSP responder certificate key usage values; added Qualified Certificate Statement value “qcs-QcCompliance” • Changed chapter 3 – added nextUpdate extension; improved responderID values regarding to the new root certificate EE-GovCA2018 • Changed chapter 4 – added ECDSA signature algorithm and EE-GovCA2018 root certificate name in issuer DN
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 various combinations of profile for intermediate certificates issued by EE Certification Centre Root CA, EE-GovCA2018, SK ID Solutions Root G1R and SK ID Solutions Root G1E. Also CRL-s, OCSP responder certificates and timestamping 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 or SK ID Solutions AS, Certification Service provider
ETSI	European Telecommunications Standards Institute
EECCRCA	EE Certification Centre Root CA
EE-GovCA2018	Estonian Government Root CA
SK ID Solutions Root G1R	SK ID Solutions root CA with RSA encryption
SK ID Solutions Root G1E	SK ID Solutions root CA with ECC encryption
DN	Distinguished name

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 and random serial number of the certificate

Signature Algorithm	1.2.840.113549.1.1.11	yes	sha256WithRSAEncryption;
			sha384WithRSAEncryption;
			ecdsa-with-sha384;
			ecdsa-with-sha512
				no	Signature algorithm in accordance to RFC 5280 [1] and RFC 5480 [9]

Field	OID	Mandatory	Value	Changeable	Description
Issuer Distinguished name		yes		no	Distinguished name of the certificate issuer

Common Name (CN)	2.5.4.3	yes	EE Certification Centre Root CA;
			EE-GovCA2018;
			SK ID Solutions Root G1R;
			SK ID Solutions Root G1E
					Root certificate authority name

Organisational Unit (OU)	2.5.4.11	no	Certification services		Identity of certification service. Used only in older CA certificates issued by EECCRCA.
Organisation (O)	2.5.4.10	yes	SK ID Solutions AS		Organisation name
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]
Country (C)	2.5.4.6	yes	EE		Country code: EE – Estonia (2 character ISO 3166 country code [7])
E-mail (E)		no	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
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]
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, ECC P384, ECC P521	no	Public key created in RSA algorithm [8] in accordance with RFC 4055 [2]. ECC keys according to RFC 5480 [9]

Field	OID	Mandatory	Value	Changeable	Description
Signature		yes		no	Confirmation signature of the certificate issuer authority.

2.2 Certificate Extensions

2.2.1 Common Extensions of Organisation Certificates

The table describes different extensions that MAY be used.

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 Path Length Constraint=None)	Critical	yes[1]
Key Usage	2.5.29.15	Refer to p 2.2.2 "Variable Extensions "	Critical	yes
Certificate Policies	2.5.29.32	Refer to p 2.2.3 "Certificate policy"	Non-critical	yes

Name Constraints[2]	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[3]	2.5.29.31	[1]CRL Distribution Point Distribution Point Name: Full Name:	Non-critical	yes

[1] Not mandatory in timestamping certificate

[2] Used only in intermediate CA ESTEID-SK 2015 issued by EECCRCA

[3] Not included in OCSP responder and timestamping certificates

Extension	OID	Values and limitations	Criticality	Mandatory
		URL= http://www.sk.ee/repository/crls/eeccrca.crl **or** URL= http://c.sk.ee/EE-GovCA2018.crl **or** http://c.sk.ee/%20SK_ROOT_G1R.crl **or** http://c.sk.ee/%20SK_ROOT_G1E.crl		
Extended Key Usage	2.5.29.37	Refer to p 2.2.2 "Variable Extensions "	Critical	yes
AuthorityKeyIdentifier	2.5.29.35	SHA-1 hash of the public key	Non-critical	yes
SubjectKeyIdentifier	2.5.29.14	SHA-1 hash of the public key	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; **or** http://aia.sk.ee/ee-govca2018	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 **or** http://c.sk.ee/EE-GovCA2018.der.crt **or** http://c.sk.ee/SK_ID_Solutions_ROOT_G1R.der.crt **or** http://c.sk.ee/SK_ID_Solutions_ROOT_G1E.der.crt	Non-critical	yes
Qualified Certificate Statement	1.3.6.1.5.5.7.1.3	Refer to p 2.2.2 "Variable Extensions "	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	Timestamping certificate
Key usages			
Certificate signing	x		
CRL signing	x		
Digital Signature	x	x	x
Non-Repudiation	x		x

Extension	Intermediate CA certificate	OCSP Responder certificate	Timestamping certificate
Key usages			
Qualified Certificate Statement[4]			
qcs-QcCompliance	x		
id-etsi-qcs-semanticsId-Natural	x		
Extended key usage			
OCSP Signing	x	x	
Client Authentication	x		
Secure Email	x		
Time Stamping			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. Profile of OCSP response

Profile describes issuing CA OCSP response. 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	CN = <ca name> AIA OCSP RESPONDER YYYYMM
		2.5.4.97 = NTREE-10747013
		O = SK ID Solutions AS
		C = EE
			Distinguished name of the OCSP responder
			Note: the Common Name will vary each month and includes the month in YYYYMM format.
			For example:
			CN = EECCRCA AIA OCSP RESPONDER YYYYMM
			2.5.4.97 = NTREE-10747013
			O = SK ID Solutions AS
			C = EE

producedAt	yes		Date when the OCSP response was signed
Responses	yes		
certID	yes		CertID fields accordance with RFC 6960 [5] clause 4.1.1
certStatus	yes		Status of the certificate as follows: *good* - certificate is issued and has not been revoked or suspended *revoked* - certificate is revoked, suspended or not issued by this CA *unknown* - the issuer of certificate is unrecognized by this OCSP responder
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
Archive Cutoff	no	CA’s certificate "valid from" date.	ArchiveCutOff date - the CA's certificate "valid from" date.

Field	Mandatory	Value	Description
			Pursuant to RFC 6960 [6] clause 4.4.4
Extended Revoked Definition	no	NULL	Identification that the semantics of certificate status in OCSP response conforms to extended definition in RFC 6960 [6] clause 2.2
nextUpdate	Yes	ThisUpdate + 7 days	The time at or before which newer information will be available about the status of the certificate.
Nonce	No		Value is copied from request if it is included. Pursuant to RFC 6960 [5] clause 4.4.1
signatureAlgorithm	yes	sha256WithRSAEncryption; sha512WithRSAEncryption	Signing algorithm pursuant to RFC 5280 [1].
signature	yes		
certificate	yes		Certificate corresponding to the private key used to sign the response.

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, ecdsa-with-sha512	CRL signing algorithm pursuant to RFC 5280 [1] and and RFC 5480 [9]
Issuer Distinguished Name		yes		Distinguished name of certificate issuer
Common Name (CN)	2.5.4.3	yes		Name of the issuing 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

Field	OID	Mandatory	Value	Description
				EN 319 412-1 [3]
Organisational Unit (OU)	2.5.4.11	no	Sertifitseerimisteenused	Identity of certification service of SK. Used only in older CA certificates issued by EECCRCA.
Organisation (O)	2.5.4.10	yes	SK ID Solutions AS **or** AS Sertifitseerimiskeskus	Organisation name. "Sertifitseerimiskeskus" used only in older CA certificates issued by EECCRCA and Juur-SK.
Country (C)	2.5.4.6	yes	EE	Country code: EE – Estonia (2 character ISO 3166 country code [7])
Effective Date		yes		Date and time of CRL issuance.
Next Update		yes		Date and time of issuance of the next CRL.
Revoked Certificates		yes		List of revoked certificates.
Serial Number		yes		Serial number of the certificate revoked.
Revocation Date		yes		Date and time of revocation of the certificate.

Reason Code	2.5.29.21	yes		Reason code for certificate revocation.
				1 – *(keyCompromise)*;
				2 – *(cACompromise);*
				3 – *(affiliationChanged);*
				4 – *(superseded);*
				5 – *(cessationOfOperation).*

invalidityDate	2.5.29.24	no	InvalidityDate::= GeneralizedTime (i.e., times are YYYYMMDDHHMMSSZ)	The invalidity date is a non-critical CRL entry extension that provides the date on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid.
Signature				Confirmation signature of the authority issued the CRL.

4.2 CRL Extensions

Field	OID	Values and limitations	Criticality	Description
CRL Number	2.5.29.20	CRL sequence number	Non-critical	See clause 5.2.3 of RFC 5280 [1]
Authority Key Identifier[4]	2.5.29.35	Matching the subject key identifier of the certificate	Non-critical	See clause 5.2.1 of RFC 5280 [1]
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	See clause 5.2.5 of RFC 5280 [1]. Issuing Distribution Point extension is used only CRL's issued by EECCRCA.

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 v1.4.4 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures;

[4] ETSI EN 319 412-5 v2.3.1 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 v1.3.1 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.

[9] RFC 5480 - Elliptic Curve Cryptography Subject Public Key Information;

[4] SHA-1 hash of the public key corresponding to the private key.