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

Version 3.4
Valid from 08.11.2023

Version and Changes		
Version	**Date**	**Changes/amendments**
3.4	08.11.2023	• Regular review and update of references performed; • Document renamed “Certificate, OCSP and CRL Profile for Root, Intermediate CA and timestamping service” • Document restructuring: root certificate, intermediate certificate and timestamping certificate profiles described separately under different chapters • Chapter 3 – OCSP Profile: Archive Cutoff changed to mandatory.
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 root, intermediate and timestamping certificates issued by SK ID Solutions. Also relevant CRL-s and OCSP responder profiles.

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.
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
TSU	Timestamping unit certificate
DN	Distinguished name

2. Technical Profile of root certificate

Root CA certificate profile is compiled in accordance with the X.509 version 3, RFC 5280 [1] and ETSI EN 319 411-1 [6].

2.1. Certificate Body

Field	Mandatory	Value	Description
Version	yes	Version 3	Certificate format version
Serial Number	yes		Unique and random serial number of the certificate
Signature Algorithm	yes	sha1RSA sha384RSA sha512ECDSA	Signature algorithm in accordance to RFC 5280 [1] and RFC 5480 [9]. Signature sha1RSA used only for root EECCRCA.
Issuer Distinguished name	yes		Distinguished name of the root certificate.

Field	Mandatory	Value	Description

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

Organisation (O)	yes	SK ID Solutions AS	Organisation name
Organisation Identifier	yes	NTREE-10747013	Identification of the subject organisation different from the organisation name as specified in clause 5.1.4 of ETSI EN 319 412-1 [3]. Not used in EECCRCA root certificate.
Country (C)	yes	EE	Country code: EE – Estonia (2 character ISO 3166 country code [7])
E-mail (E)	no	pki@sk.ee	Contact e-mail
Valid from	yes		First date of certificate validity.
Valid to	yes		The last date of certificate validity.
Subject Distinguished Name	yes		The subject DN identifies the entity associated with the public key stored in the certificate.

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

OrganisationName (O)	yes		Organisation name
Organisation Identifier	yes	NTREE-10747013	Identification of the subject organisation different from the organisation name as specified in clause 5.1.4 of ETSI EN 319 412-1 [3]. Not used in EECCRCA root certificate.
Country (C)	yes		Country code: EE – Estonia (2 character ISO 3166 country code [7])
E-mail (E)[1]	no	pki@sk.ee	Contact e-mail
Subject Public Key	yes	RSA 2048, RSA 4096, ECC P384, ECC P521	Public key created in RSA algorithm [8] in accordance with RFC 4055 [2]. ECC keys according to RFC 5480 [9]
Signature	yes		Confirmation signature of the certificate issuer authority.

[1] Used in EECCRCA root certificate.

2.2. Certificate extensions

The table describes different certificate extensions that MAY be used in certificate profile.

Extension	Mandatory	Criticality	Value/example	Descrition/note
Basic Constraints	yes	Critical	Subject Type=CA Path Length Constraint=0	For root certificate EE-GovCA2018 Path Length Constraint=1
Key Usage	yes	Critical	keyCertSign, CRLSign	Defines the purpose of the key contained in the certificate.
Certificate Policies[2]	no	Non-critical	Certificate Policy: Policy Identifier=*<OID>* CPS URI: *<CPS URL>*	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.
Extended Key Usage[3]	no	Non-critical	Client Authentication (1.3.6.1.5.5.7.3.2) Server Authentication (1.3.6.1.5.5.7.3.1) Code Signing (1.3.6.1.5.5.7.3.3) Secure Email (1.3.6.1.5.5.7.3.4) Time Stamping (1.3.6.1.5.5.7.3.8) OCSP Signing (1.3.6.1.5.5.7.3.9)	Extension used only in EE-GovCA2018 and EE Certification Centre Root CA root certificate.
AuthorityKeyIdentifier	no	Non-critical	*<SHA-1 hash of the public key>*	The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a CRL. Not present in EE Certification Centre Root CA root certificate.
SubjectKeyIdentifier	yes	Non-critical	*<SHA-1 hash of the public key>*	Provides a means of identifying certificates that contain a particular public key.
Qualified Certificate Statement[4]	no	Non-critical	qcStatement – QcCompliance (0.4.0.1862.1.1)	Attribute of qualified certificate. Extension used only in EE-GovCA2018 root certificate.

[2] Extension used only in EE-GovCA2018 root certificate

[3] Extension used only in EE-GovCA2018 and EE Certification Centre Root CA root certificate.

[4] Extension used only in EE-GovCA2018 root certificate.

2.3. Technical Profile of intermediate certificate

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

2.3.1. Certificate Body

Field	Mandatory	Value	Description
Version	yes	Version 3	Certificate format version
Serial Number	yes		Unique and random serial number of the certificate
Signature Algorithm	yes	sha256RSA sha384RSA sha384ECDSA sha512ECDSA	Signature algorithm in accordance to RFC 5280 [1] and RFC 5480 [9].
Issuer Distinguished name	yes		Distinguished name of the certificate issuer

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

Organisation (O)	yes	SK ID Solutions AS	Organisation name. Certificates issued before 2017 hold name O = AS Sertifitseerimiskeskus
Organisation Identifier	yes	NTREE-10747013	Identification of the subject organisation different from the organisation name as specified in clause 5.1.4 of ETSI EN 319 412-1 [3]. Not used in EECCRCA root certificate.
Country (C)	yes	EE	Country code: EE – Estonia (2 character ISO 3166 country code [7])
E-mail (E)[5]	no	pki@sk.ee	If present, e-mail address.
Valid from	yes		The first date of certificate validity.
Valid to	yes		The last date of certificate validity.
Subject Distinguished Name	yes		The subject DN identifies the entity associated with the public key stored in the certificate.
Common Name (CN)	yes		Intermediate certificate authority name
OrganisationName (O)	yes	SK ID Solutions AS	Organisation name. Certificates issued before 2017 hold name O = AS Sertifitseerimiskeskus
Organisation Identifier	yes	NTREE-10747013	Identification of the subject organisation different from the organisation name as specified in clause 5.1.4 of ETSI EN 319 412-1 [3]

[5] Used in EECCRCA root certificate.

Field	Mandatory	Value	Description
Country (C)	yes		Country code: EE – Estonia (2 character ISO 3166 country code [7])
Subject Public Key	yes	RSA 2048, RSA 4096, ECC 256, ECC 384, ECC P521	Public key created in RSA algorithm [8] in accordance with RFC 4055 [2]. ECC keys according to RFC 5480 [9]
Signature	yes		Confirmation signature of the certificate issuer authority.

2.4. Certificate extensions

The table describes different certificate extensions that MAY be used in certificate profile.

Extension	Mandatory	Criticality	Value/example	Description/note
Basic Constraints	yes	Critical	Subject Type=CA Path Length Constraint=0 OR none	The value of Basic Constraints is set according to PKI hierarchy need
Key Usage	yes	Critical	keyCertSign, CRLSign	Defines the purpose of the key contained in the certificate.
Certificate Policies	no	Non-critical	Certificate Policy: Policy Identifier=*<OID>* CPS URI: *<CPS URL>*	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. The corresponding certificate policy is determined according to the scope of the certificate. Not documented here in detail.
Extended Key Usage[6]	no	Non-critical	OCSP Signing (1.3.6.1.5.5.7.3.9) Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)	If present, this extension indicates one or more purposes for which the certified public key may be used.
AuthorityKeyIdentifier	yes	Non-critical	*<SHA-1 hash of the public key>*	The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a CRL.

[6] Extension used only in intermediate certificates issued under EECCRCA

Extension	Mandatory	Criticality	Value/example	Description/note
SubjectKeyIdentifier	yes	Non-critical	*<SHA-1 hash of the public key>*	Provides a means of identifying certificates that contain a particular public key.
Qualified Certificate Statement[7]	no	Non-critical	qcStatement – QcCompliance (0.4.0.1862.1.1)	Attribute of qualified certificate. Extension used only in ESTEID2018, EID-SK 2016 and NQ-SK 2016 certificate.

Name Constraints[8]	no	Non-critical	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
				For description refer to IETF RFC 5280 [1] chapter 4.2.1.10

Authority Information Access	yes	Non-critical	Authority Info Access Access Method=On-line Certificate Status Protocol URL=*<ocsp_url_address>* Authority Info Access Access Method=Certification Authority Issuer URL=*<issuer_certificate_url_address>*	For description refer to IETF RFC 5280 [1] chapter 4.2.2.1. For example, most of SK issued intermediate CA's use URL http://ocsp.sk.ee/CA
CRL Distribution Points	yes	Non-critcal	CRL Distribution Point Distribution Point Name: Full Name: URL=*<issuer_CA_CRL_url>*	For description refer to IETF RFC 5280 [1] chapter 4.2.1.13.

[7] Extension used only in ESTEID2018, EID-SK 2016 and NQ-SK 2016 certificate.

[8] Used only in intermediate CA ESTEID-SK 2015, EID_SK 2016 and NQ-SK 2016 issued by EECCRCA

3. Technical Profile of OCSP responder certificate

CA OCSP responder certificate and response profile is compiled in accordance with the X.509 version 3, IETF RFC 5280 [1] and RFC6960 [1]. Each CA certificate issues OCSP responder certificate, what is used in corresponding OCSP service.

3.1. Certificate Body

Field	Mandatory	Value	Description
Version	yes	Version 3	Certificate format version
Serial Number	yes		Unique and random serial number of the certificate
Signature Algorithm	yes	sha256RSA sha384RSA sha384ECDSA sha512ECDSA	Signature algorithm in accordance to RFC 5280 [1] and RFC 5480 [9].
Issuer Distinguished name	yes		Distinguished name of the certificate issuer
Common Name (CN)	yes	CN=*<issuer_CA_name>*	Issuer certificate authority name. E.g CN = ESTEID2018
Organisation (O)	yes	SK ID Solutions AS	Organisation name. Certificates issued before 2017 hold name O = AS Sertifitseerimiskeskus
Organisation Identifier	yes	NTREE-10747013	Identification of the subject organisation different from the organisation name as specified in clause 5.1.4 of ETSI EN 319 412-1 [3]. Not used in EECCRCA root certificate.
Country (C)	yes	EE	Country code: EE – Estonia (2 character ISO 3166 country code [7])
E-mail (E)[9]	no	pki@sk.ee	If present, e-mail address.
Valid from	yes		The first date of certificate validity.
Valid to	yes		The last date of certificate validity.
Subject Distinguished Name	yes		The subject DN identifies the entity associated with the public key stored in the certificate.
Common Name (CN)	yes	CN = *<ca_name>* AIA OCSP RESPONDER YYYYMM	OCSP responder certificate common name. OCSP responder certificate name, e.g CN = EID-SK 2016 AIA OCSP RESPONDER 202310
OrganisationName (O)	yes	SK ID Solutions AS	Organisation name. Certificates issued before 2017 hold name O = AS Sertifitseerimiskeskus

[9] Used in EECCRCA root certificate.

Field	Mandatory	Value	Description
Organisation Identifier	yes	NTREE-10747013	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)	yes		Country code: EE – Estonia (2 character ISO 3166 country code [7])
Subject Public Key	yes	RSA 2048, RSA 4096, ECC 256, ECC 384, ECC P521	Public key created in RSA algorithm [8] in accordance with RFC 4055 [2]. ECC keys according to RFC 5480 [9]
Signature	yes		Confirmation signature of the certificate issuer authority.

3.2. Certificate extensions

The table describes different certificate extensions that MAY be used in certificate profile.

Extension	Mandatory	Criticality	Value/example	Description/note
Key Usage	yes	Critical	digitalSignature	Defines the purpose of the key contained in the certificate.
Certificate Policies[10]	no	Non-critical	Certificate Policy: Policy Identifier=*<OID>* CPS URI: *<CPS URL>*	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. The corresponding certificate policy is determined according to the scope of the certificate. Not documented here in detail.
OCSP No Revocation Checking (id-pkix-ocsp-nocheck)	no	Non-critical	NULL	For description refer to RFC 6960 [5], chapter 4.2.2.2.1.
Extended Key Usage	no	Non-critical	OCSP Signing (1.3.6.1.5.5.7.3.9)	If present, this extension indicates one or more purposes for which the certified public key may be used.

[10] Extension added only in EECCRCA and EE-GovCA2018 AIA OCSP certificates.

Extension	Mandatory	Criticality	Value/example	Description/note
AuthorityKeyIdentifier	yes	Non-critical	*<SHA-1 hash of the public key>*	The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a CRL.
SubjectKeyIdentifier	yes	Non-critical	*<SHA-1 hash of the public key>*	Provides a means of identifying certificates that contain a particular public key.
Authority Information Access	yes	Non-critical	Authority Info Access Access Method=Certification Authority Issuer URL=*<issuer_certificate_url>*	For description refer to IETF RFC 5280 [1] chapter 4.2.2.1.

3.3. Profile of OCSP response

Profile describes 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		

Field	Mandatory	Value	Description
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	yes	CA’s certificate "valid from" date.	ArchiveCutOff date - the CA's certificate "valid from" date. 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. Technical Profile of timestamping certificate

Timestamping service (TSU) certificate is compiled in accordance with the X.509 version 3, RFC 5280 [1], RFC 3161 [1] and ETSI EN 319 421 [6].

4.1. Certificate Body

Field	Mandatory	Value	Description
Version	yes	Version 3	Certificate format version
Serial Number	yes		Unique and random serial number of the certificate
Signature Algorithm	yes	sha256RSA sha384RSA sha256ECDSA sha384ECDSA sha512ECDSA	Signature algorithm in accordance to RFC 5280 [1] and RFC 5480 [9].
Issuer Distinguished name	yes		Distinguished name of the certificate issuer

Common Name (CN)	yes	EE Certification Centre Root CA;
		SK TSA CA 2023E;
		SK TSA CA 2023R
			Issuer certificate authority name.

Organisation (O)	yes	SK ID Solutions AS	Organisation name. All TSU certificates issued directly under root EECCRCA include name O = AS Sertifitseerimiskeskus
Organisation Identifier	yes	NTREE-10747013	Identification of the subject organisation different from the organisation name as specified in clause 5.1.4 of ETSI EN 319 412-1 [3]. Not used in EECCRCA root certificate.
Country (C)	yes	EE	Country code: EE – Estonia (2 character ISO 3166 country code [7])
E-mail (E)[11]	no	pki@sk.ee	If present, e-mail address.
Valid from	yes		The first date of certificate validity.
Valid to	yes		The last date of certificate validity.
Subject Distinguished Name	yes		The subject DN identifies the entity associated with the public key stored in the certificate.
Common Name (CN)	yes		Intermediate certificate authority name
OrganisationName (O)	yes	SK ID Solutions AS	Organisation name. TSU certificates issued before 2019 hold name O = AS Sertifitseerimiskeskus
Organisation Identifier	yes	NTREE-10747013	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)	yes		Country code: EE – Estonia (2 character ISO 3166 country code [7])

[11] Used only in EECCRCA root certificate DN.

Field	Mandatory	Value	Description
Subject Public Key	yes	RSA 2048, RSA 4096, ECC 256, ECC 384, ECC P521	Public key created in RSA algorithm [8] in accordance with RFC 4055 [2]. ECC keys according to RFC 5480 [9]
Signature	yes		Confirmation signature of the certificate issuer authority.

4.2. Certificate extensions

The table describes different certificate extensions that MAY be used in certificate profile.

Extension	Mandatory	Criticality	Value/example	Descrition/note
Key Usage	yes	Critical	Digital Signature, Non-Repudiation	Defines the purpose of the key contained in the certificate.
Extended Key Usage	yes	Critical	Time Stamping (1.3.6.1.5.5.7.3.8)	If present, this extension indicates one or more purposes for which the certified public key may be used.
Certificate Policies	yes	Non-critical	Policy Identifier=0.4.0.2042.1.2	Certificate has been issued according to NCP+ policy as stated in ETSI EN 319 411-1 [6].
AuthorityKeyIdentifier	yes	Non-critical	*<SHA-1 hash of the public key>*	The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a CRL.
SubjectKeyIdentifier	yes	Non-critical	*<SHA-1 hash of the public key>*	Provides a means of identifying certificates that contain a particular public key.
Authority Information Access	yes	Non-critical	Authority Info Access Access Method=On-line Certificate Status Protocol URL=*<ocsp_url_address>* Authority Info Access Access Method=Certification Authority Issuer URL=*<issuer_certificate_url>*	For description refer to IETF RFC 5280 [1] chapter 4.2.2.1.
CRL Distribution Points	yes	Non-critcal	CRL Distribution Point Distribution Point Name:	For description refer to IETF RFC 5280 [1] chapter 4.2.1.13.

Extension	Mandatory	Criticality	Value/example	Descrition/note
			Full Name: URL=<*issuer_CA_CRL_url*>	

5. Profile of Certificate Revocation List

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

5.1. CRL main fields

Field	Mandatory	Value	Description
Version	yes	Version 2	CRL format version pursuant to X.509.
Signature Algorithm	yes	sha256RSA sha384RSA sha256ECDSA sha384ECDSA sha512ECDSA	CRL signing algorithm pursuant to RFC 5280 [1] and RFC 5480 [9]
Issuer Distinguished Name	yes		Distinguished name of certificate issuer
Common Name (CN)	yes		Name of the issuing certification authority
Organisation Identifier	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]
Organisation (O)	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)	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	yes		Reason code for certificate revocation.

Field	Mandatory	Value	Description

			1 – *(keyCompromise)*;
			2 – *(cACompromise);*
			3 – *(affiliationChanged);*
			4 – *(superseded);*
			5 – *(cessationOfOperation).*

Signature			Confirmation signature of the authority issued the CRL.

5.2. CRL Extensions

Field	Criticality	Values and limitations	Description
CRL Number	Non-critical	CRL sequence number	See clause 5.2.3 of RFC 5280 [1]
Authority Key Identifier[12]	Non-critical	Matching the subject key identifier of the certificate	See clause 5.2.1 of RFC 5280 [1]
Issuing Distribution Point[13]	Critical	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	See clause 5.2.5 of RFC 5280 [1].

6. 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 v1.5.1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures;
[4] ETSI EN 319 412-5 v2.4.1 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;
[10] RFC 3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
[11] ETSI EN 319 421 V1.2.1 - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

[12] SHA-1 hash of the public key corresponding to the private key.
[13] Issuing Distribution Point extension is used only in EECCRCA CRL and itermediate CA CRLs by EECCRCA.