Certificate, CRL and OCSP Profile for Organisation Certificates Issued by SK

Version 6.0
1 June 2017

Version information		
Date	**Version**	**Changes/amendments**
01.06.2017	6.0	Approved version - Chapter 2 – changed the name of the issuer CA from KLASS3-SK 2010 to KLASS3-SK 2016; - Chapters 3.1 and 5.1 – due to adding new CA KLASS3-SK 2016 to this document, updated the Common Name value; - Chapter 3.2.2 – replaced SK's former business name AS Sertifitiseerimiskeskus with its new name SK ID Solutions AS; - Chapters 3.2.1 and 4 - due to adding new CA KLASS3-SK 2016 to this document, changed AIA OCSP name; - Chapter 3.2.1 – changed calssuers certificate URL.
01.03.2017	5.1	Draft of version 6.0
03.02.2017	5.0	Approved version - Chapter 3.1 - added corrections in certification body (Issuer) and CPS reference; - Chapter 3.2.2 - specified Authentication Certificate key usage values; - Chapter 3.2.2 - added semantics identifier „id-etsi-qcs-semanticsId-Legal“ extension.
01.11.2016	4.1	Draft of version 5.0
01.07.2016	4.0	- Chapter 2 – added/renamed certificate profiles - Chapter 3.2 - improved certificate extensions table; - Chapter 3.2.3 - new OID's added in certificate policies.
01.04.2016	3.1	Draft of version 4.0. - Document name renamed; - Chapter 2 - renamed certificate profile types; - Chapter 2.1 - added terms and abbreviations; - Chapter 3.1 - improved "Technical Profile of the Certificate"; - Chapter 3.2 - improved certificate extensions table; - Chapter 3.3 - new OID's added in certificate policies; - Chapter 4 - added OCSP profile.
24.03.2016	2.1	Draft of version 3.0. Chapter 2.1 - removed exception 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.

1.1. Table of Contents

2. Introduction

The document describes the profiles of certificates, CRL-s and OCSP responses issued by KLASS3-SK 2016.

This document complements Certificate Policies [2][3] and Certification Practice Statement [1].

The organisation certificates are divided into following types:

- **e-Seal Certificate** - used for proof of integrity of a digital document and the relation with the owner of such document (e-Seal certificate can be issued also without extension “id-etsi-qcs-QcSSCD“ see [3.2.2]);
- **TLS Server Certificate** - Certificate issued to TLS server (HTTPS, IMAPS, FTPS, etc.) for proof of authenticity of TLS server owner;
- **Certificate for Authentication** - certificate used for authentication of the subscriber in WWW, S/MIME or other data processing systems;
- **Certificate for Encryption** – certificate used for data encryption.

Various areas of application can be combined into a single certificate. The area of application of e-Seal Certificate cannot be combined with other areas of application.

2.1. Terms and Abbreviations

Refer to Certification Practice Statement [1].

3. Technical Profile of the Certificate

Organisation certificate is compiled in accordance with the X.509 version 3, IETF RFC 5280 [4] and clause 6.6 of ETSI EN 319 411-1 [12].

3.1. 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	no	Signature algorithm in accordance to RFC 5280
Issuer Distinguished name		yes		no	Distinguished name of the certificate issuer
Common Name (CN)	2.5.4.3	yes	KLASS3-SK 2016		Certificate authority name
Organisation Identifier	2.5.4.97	yes	NTREE-10747013	no	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.
Organisational Unit (OU)	2.5.4.11	yes	Sertifitseerimisteenused		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

Field	OID	Mandatory	Value	Changeable	Description
					code [13])
Subject Distinguished Name		yes		yes	Unique subject (device) name in the infrastructure of certificates.
Serial Number	2.5.4.5	yes		yes	Registry code of the subscriber as described in certificate application. Not in use for TLS Server Certificates.
Common Name (CN)	2.5.4.3	yes		yes	Informal value can be used, according to subscriber requirements (also abbreviations can be used). Not required for TLS Server Certificates, if used, also the Subject Alternative Name must be filled at least with the IP address or with the domain name. Specified in clause 3.1 [1]
Organisational Unit (OU)	2.5.4.11	no		yes	The name of organisational unit as described in certificate application. If the information about area of application is missing from the application the following values are used depending on certificate type: „Key Encipherment“-Certificate for

Field	OID	Mandatory	Value	Changeable	Description
					Encryption; „e-Seal“ - e-Seal Certificate; „Corporate Authentication“ - Certificate for Authentication.
OrganisationName (O)	2.5.4.10	yes		yes	Subject (organisation) name as stated in certificate application.
Organisation Identifier[1]	2.5.4.97	yes	NP:EE-<registerCode> GO:EE-<registerCode> NTREE-<registerCode>	yes	Identification of the subject organisation different from the organisation name as specified in clause 5.1.4 of ETSI EN 319 412-1. Used only in e-Seal certificates.
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.
Valid from		yes		no	First date of certificate.
Valid to		yes		no	The last date of certificate validity.
Subject Public Key		yes	RSA 2048, RSA 4096 or ECC 256, ECC 320,	no	Public key created in RSA algorithm in

[1] NP:EE - Estonian Non-Profit Associations and Foundations Register
GO:EE - Estonian Register of State and Local Government Organisations
NTREE -Estonian National Business Register

Field	OID	Mandatory	Value	Changeable	Description
			ECC 384, ECC 512, ECC 521		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.

3.2. Certificate Extensions

3.2.1. Common Extensions of Organisation Certificates

Extension	OID	Values and limitations	Criticality	Mandatory
Basic Constraints	2.5.29.19	SubjectType=End Entity Path Length Constraint=None	Non-critical	yes
Key Usage	2.5.29.15	Refer to p 3.2.2 "Variable Extensions "	Critical	yes
Extended Key Usage	2.5.29.37	Refer to p 3.2.2 "Variable Extensions "	Non-critical	yes
AuthorityKeyIdentifier	2.5.29.35		Non-critical	yes
SubjectKeyIdentifier	2.5.29.14		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://aia.sk.ee/klass3-2016	Non-critical	yes
calssuers	1.3.6.1.5.5.7.48.2	https://c.sk.ee/KLASS3-SK_2016_EECCRCA_SHA384.der.crt	Non-critical	yes

3.2.2. Variable Extensions

Extension	e-Seal Certificate on QSCD	e-Seal Certificate	TLS server certificate	Certificate for Authentication[2]	Certificate for Encryption
	Key Usage				
Non-Repudiation	X	X			
Digital Signature			X	X	X
Data Encipherment				X	X
Key Encipherment			X	X	X
Key Agreement					
	Qualified Certificate Statement				
id-etsi-qcs-QcCompliance	X	X			
id-etsi-qcs-QcSSCD	X				
id-etsi-qcs-QcType[3]	2	2			
id-etsi-qcs-QcPDS	https://sk.ee/en/repository/conditions-for-use-of-certificates/	https://sk.ee/en/repository/conditions-for-use-of-certificates			
id-qcs-pkixQCSyntax-v2[4]	X	X			
	Extended key usage				
Client Authentication				X	
Server Authentication			X		
	Subject Alternative Name[5]				

[2] SK ID Solutions AS takes the right to change Key Usages according to subscriber requirements. Extented Key Usage must contain “Client Authentication”.
[3] Types according to clause 4.2.3 specified in ETSI EN 319 412-5.
[4] Semantics identifier „id-etsi-qcs-semanticsId-Legal“ is used as specified in clause 5.1.4 of ETSI EN 319 412-1

Extension	e-Seal Certificate on QSCD	e-Seal Certificate	TLS server certificate	Certificate for Authentication[2]	Certificate for Encryption
- DNSName			X		
- IPAddress			X		

NOTE: Depending on the service description in the Estonian Trust List, the id-etsi-qcs-QcCompliance fields can be automatically interpreted as set even without being contained in the certificate if the Key Usage has nonRepudiation bit asserted.

3.2.3. Certificate Policy

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

Profile	PolicyIdentifier	PolicyQualifier
e-Seal Certificate on QSCD	1.3.6.1.4.1.10015.7.3; 0.4.0.194112.1.3	https://www.sk.ee/cps
e-Seal Certificate	1.3.6.1.4.1.10015.7.3; 0.4.0.194112.1.1	https://www.sk.ee/cps
TLS Server Certificate	1.3.6.1.4.1.10015.7.2; 0.4.0.2042.1.7; 2.23.140.1.2.2	https://www.sk.ee/cps
Certificate for Encryption	1.3.6.1.4.1.10015.7.3; 0.4.0.2042.1.1	https://www.sk.ee/cps
Certificate for Authentication	1.3.6.1.4.1.10015.7.3; 0.4.0.2042.1.1	https://www.sk.ee/cps

[5] In case of TLS 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.

4. OCSP profile

OCSP v1 according to [RFC 6960] [11]

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=KLASS3-SK 2016 AIA OCSP RESPONDER YYYYMM	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[6]
revocationTime	no		Date of revocation or expiration of certificate
revocationReason	no		Code for revocation Reason according to RFC5280
thisUpdate	yes		Date when the status was queried from

[6] Exceptions: In case of expired certificate „revoked“ status is used and Revocation Time is set to notAfter value of the certificate if the responder has access to the full certificate.

Field	Mandatory	Value	Description
			database
signatureAlgorithm	yes	sha256WithRSAEncryption	
signature	yes		
certificate	yes		Certificate corresponding to the private key used to sign the response.

No extensions are supported.

5. Profile of Certificate Revocation List

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

5.1. 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
Issuer Distinguished Name		yes		Distinguished name of certificate issuer
Common Name (CN)	2.5.4.3	yes	KLASS3-SK 2016	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

Field	OID	Mandatory	Value	Description
				EN 319 412-1.
Organisational Unit (OU)	2.5.4.11	yes	Sertifitseerimisteen used	Identity of certification service of SK
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 [13])
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.
Signature				Confirmation signature of the authority issued the CRL.

5.2. CRL Extensions

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

On the field “authorityKeyIdentifier”, SHA-1 hash of the public key corresponding to the private key used to sign the CRL is presented.

6. Referred and related Documents

[1] SK ID Solutions AS - Certification Practice Statement for KLASS3-SK, published: https://sk.ee/en/repository/CPS/;
[2] SK ID Solutions AS - Certificate Policy for TLS Server Certificates, published: https://sk.ee/en/repository/CP/;
[3] SK ID Solutions AS - Certificate Policy for Organisation Certificates, published: https://sk.ee/en/repository/CP/;
[4] RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
[5] RFC 3647 – Request For Comments 2527, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework;
[6] 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;
[7] RFC 5639 - Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation;
[8] FIPS PUB 186-4;
[9] ETSI EN 319 412-1 v1.1.1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures;
[10] ETSI EN 319 412-5 v2.2.2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements;
[11] RFC 6960 – X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP;
[12] ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
[13] ISO 3166 Codes;
[14] RFC 3279 - Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.