Certificate and OCSP Profile for Organisation Certificates Issued by SK

Document Information	
Name	Certificate and OCSP Profile for Organisation Certificates Issued by SK
Version number	11.0
Version No. and date	Changes
11.03.2024 11.0	• Regular review and update of references performed; • Removed 'nextUpdate' from KLASS3-SK 2016 OCSP response; • Removed CRL reference from document as 'KLASS3-SK 2016' does not issue CRL; • Chapters 1., 3. – Removed references to Intermediate CA 'KLASS3-SK 2010' due to termination of CA (end of life cycle); • Chapter 2.1 – Changed certificate validity options.
01.02.2023 10.5	• Added Organisation Identifier values for eSeal EPREL (European Product Registry for Energy Labelling) • Added 3072-bit RSA Public Key value • Chapter 3 – OCSP Profile: Archive Cutoff extension mandatory • Chapter 3 – OCSP Profile: Clarification for different revocation times added.
17.02.2022 10.4	• Chapter 2.1 - added random to certificate serial number description • Chapter 2.2.1 - changed key usage and extended key usage references from 3.2.2 to 2.2.2 • Added ETSI EN 319 412-3 reference.
12.07.2021 10.3	• Approved version; • change of document name to SK-CPR-ORG (Certificate, CRL and OCSP Profile for Organisation Certificates Issued by SK); • chapter 3.2 - changed sk.ee domain to skidsolutions.eu in certificate extensions; • chapter 3 – Added new legal person semantics identifier (VAT); • amended document overall wording and references.
19.08.2020 10.2	• Approved version; • chapter 4 – changed OCSP Responder ID value; • changed sk.ee domain to skidsolutions.eu; • chapter 3.2.2 - „id-etsi-qcs-semanticsId-Legal“ usage specified. Element “nameRegistrationAuthorities“ used only for locally defined identity types; • chapter 3.2.3 – specified certificate policy for all authentication certificates.
18.02.2020 10.1	• Approved version; • chapter 4 - added nonce extension support for OCSP; corrected responder ID value by adding CN of KLASS3-SK 2010.
15.08.2019 10.0	• Approved version; • chapter 3.1 – usage of OU field in certificate subject is changed. No pre-defined values are added;

	• chapter 3.2.3 – new OID's are added under certificate policies what are used to define the certificate type; • chapter 6 – ETSI documentation versions updated.
04.01.2019 9.0	• Chapter 3.1 - Added certificate validity periods; • chapter 5.2 - corrections and improvements of AuthorityKeyIdentifier description; • chapter 4 - new extensions added: Archive Cutoff; - Extended Revoked Definition and nextUpdate; CertStatus description is renewed.
30.11.2017 8.0	• Approved version; • removed TLS Server Certificate profile; • chapter 3.2.1 – CRL distribution point URL removed as it is not used in KLASS3-SK 2016; • amended document wording and format.
01.09.2017 7.1	• Draft of version 8.0.
03.07.2017 7.0	• Approved version; • chapter 3.1- specified subject "Organisation Identifier" usage values.
04.04.2017 6.1	• Draft of version 7.0.
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 caIssuers 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.
Effective from date	11.03.2024

1 Introduction

The document describes profiles of organisation certificates issued by CA's KLASS3-SK 2016 and OCSP responses of KLASS3-SK 2016.

SK's PKI hierarchy description can be found from chapter 1.1 from Organisation Certification Practice Statement [1]

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

The organisation certificates are divided into following types:

- **e-Seal Certificate** - used for certifying digital documents and ensuring that the respective institution is associated with the specific document. e-Seal certificate can be issued under policy 'QCP-l' or 'QCP-I-qscd', see 2.2.2);
- **Certificate for Authentication** - used for identifying legal persons or for ensuring the authenticity and integrity of electronic data;
- **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.

1.1 Terms and Abbreviations

Refer to Certification Practice Statement [1].

2 Technical Profile of the Certificate

Organisation certificate is compiled in accordance with the X.509 version 3, IETF RFC 5280 [3] , clause 6.6 of ETSI EN 319 411-1 [11] and ETSI EN 319 412-3 [14]

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	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 [8].
Organisational Unit (OU)	2.5.4.11	yes	Sertifitseerimisteenused		Identity of certification service. OU field is used only in issuing CA's certified by EE Certification Centre Root CA.
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 [12])
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.

Common Name (CN)	2.5.4.3	yes		yes	Informal value can be used, according to subscriber requirements (also abbreviations can be used).
Organisational Unit (OU)	2.5.4.11	no		yes	The name of organisational unit as described in subscriber application. If the information about area is missing then OU is not added.
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:{ISO3166 country code}-{registerCode} GO:{ISO3166 country code}-{registerCode} NTR{ISO3166 country code}-{registerCode} VAT{ISO3166 country code}-{registerCode} NTR{ISO3166 country code}-{EPREL_EUID}	yes	Identification of the subject organisation different from the organisation name as specified in clause 5.1.4 of ETSI EN 319 412-1 [8]. Used only in e-Seal certificates. If eSeal for European Product Registry for Energy Labelling (EPREL) is issued, Organisation Identifier value is presented by following EPREL guideline [1] ANNEX 3 format.
LocalityName (L)	2.5.4.7	no		yes	Name of the locality.
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 [12].
Valid from		yes		no	First date of certificate validity.
Valid to		yes		no	The last date of certificate validity. Certificate validity can be up to 3 years.
Subject Public Key		yes	RSA 2048, RSA 3072, RSA 4096 or ECC 256, ECC 320, ECC 384, ECC 512, ECC 521	no	Public key created in RSA algorithm in accordance with RFC 4055. Public key of ECC algorithm is created in accordance with RFC 5480 or FIPS Publication 186-4 [7].

[1] NP:{ISO3166 country code} - Non-Profit Associations and Foundations Register;
GO:{ISO3166 country code} - Register of State and Local Government Organisations;
NTR{ISO3166 country code} - National Business RegisterVAT{ISO3166 country code} -Tax identification number
NTR{ISO3166 country code}-{EPREL_EUID} - Business Registers Interconnection System (BRIS)

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	SubjectType=End Entity Path Length Constraint=None	Non-critical	yes
Key Usage	2.5.29.15	Refer to p 2.2.2 "Variable Extensions"	Critical	yes
Extended Key Usage	2.5.29.37	Refer to p 2.2.2 "Variable Extensions"	Non-critical	yes
Authority Key Identifier	2.5.29.35	SHA-1 hash of the public key	Non-critical	yes
Subject Key Identifier	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://aia.sk.ee/klass3-2016	Non-critical	yes
caIssuers	1.3.6.1.5.5.7.48.2	https://c.sk.ee/KLASS3-SK_2016_EECCRCA_SHA384.der.crt	Non-critical	yes

2.2.2 Variable Extensions

Extension	e-Seal Certificate on QSCD	e-Seal Certificate	Certificate for Authentication[2]	Certificate for Encryption
Key usage				
Non-Repudiation	X	X		
Digital Signature			X	X
Data Encipherment			X	X
Key Encipherment			X	X
Key Agreement				
Qualified Certificate Statement				
id-etsi-qcs-QcCompliance	X	X		
id-etsi-qcs-QcSSCD	X			

[2] SK ID Solutions AS takes the right to combine Key Usage values for authentication certificate according to subscriber requirements. Extented Key Usage must contain “Client Authentication”.

id-etsi-qcs-QcType[3]	2	2		
id-etsi-qcs-QcPDS	https://www.skidsolutions.eu/en/repository/conditions-for-use-of-certificates/	https://www.skidsolutions.eu/en/repository/conditions-for-use-of-certificates/		
id-qcs-pkixQCSyntax-v2[4]	X	X		
Extended key usage				
Client Authentication			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.

2.2.3 Certificate Policy

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

Profile [5]	PolicyIdentifier	PolicyQualifier
e-Seal Certificate on QSCD	1.3.6.1.4.1.10015.7.3; 0.4.0.194112.1.3; 1.3.6.1.4.1.10015.9.2	https://www.skidsolutions.eu/en/repository/CPS/
e-Seal Certificate	1.3.6.1.4.1.10015.7.3; 0.4.0.194112.1.1; 1.3.6.1.4.1.10015.9.1	https://www.skidsolutions.eu/en/repository/CPS/
Certificate for Encryption	1.3.6.1.4.1.10015.7.3; 0.4.0.2042.1.1; 1.3.6.1.4.1.10015.9.4	https://www.skidsolutions.eu/en/repository/CPS/
Certificate for Authentication[6]	1.3.6.1.4.1.10015.7.3; 0.4.0.2042.1.1; 1.3.6.1.4.1.10015.9.3	https://www.skidsolutions.eu/en/repository/CPS/

[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 only when a locally defined identity type reference is provided (GO or NP). Then „nameRegistrationAuthorities“ element of Semantics Information shall be present. Used only for C=EE. Detailed specification in clause 5.1.4 of ETSI EN 319 412-1 [8].
[5] Certificate profile can be distinguished by policy identifier value. Object identifier 1.3.6.1.4.1. 10015 represents SK ID Solutions, which is private enterprises OID registered under Internet Assigned Numbers Authority (IANA).
Certificate profile can be distinguished as follows:
- e-Seal Certificate: 1.3.6.1.4.1.10015.9.1;
- e-Seal Certificate on QSCD: 1.3.6.1.4.1.10015.9.2;
- Certificate for Authentication: 1.3.6.1.4.1.10015.9.3;
- Certificate for Encryption: 1.3.6.1.4.1.10015.9.4
[6] OID 1.3.6.1.4.1.10015.9.3 is used for all types of authentication certificates.

3 OCSP profile

OCSP v1 according to [RFC 6960] [10]

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 O=SK ID Solutions AS 2.5.4.97=NTREE-10747013 CN=KLASS3-SK 2016 AIA OCSP RESPONDER YYYYMM or C=EE O=SK ID Solutions AS 2.5.4.97=NTREE-10747013 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 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 for a revoked or suspended certificate is the timestamp for revocation/suspension time; Date of revocation for a non-issued certificate is January 1, 1970.
revocationReason	no		Code for revocation Reason according to RFC5280
thisUpdate	yes		Date when the status was queried from database

Archive Cutoff	yes	CA's certificate "valid from" date.	Archive CutOff date - the CA's certificate "valid from" date. Pursuant to RFC 6960 [10] clause 4.4.4
Nonce	no		Value is copied from request if it is included. Pursuant to RFC 6960 [10] clause 4.4.1.
Extended Revoked Definition	no	NULL	Identification that the semantics of certificate status in OCSP response conforms to extended definition in RFC 6960 [10] clause 2.2
signatureAlgorithm	yes	sha256WithRSAEncryption	
signature	yes		
certificate	yes		Certificate corresponding to the private key used to sign the response.

4 Referred and related Documents

[1] SK ID Solutions AS - Certification Practice Statement for Organisation Certificates, published: https://www.skidsolutions.eu/resources/certification-practice-statement/
[2] SK ID Solutions AS - Certificate Policy for Organisation Certificates, published: https://www.skidsolutions.eu/resources/certificate-policies/;
[3] RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
[4] RFC 3647 – Request For Comments 2527, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework;
[5] 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;
[6] RFC 5480 - Elliptic Curve Cryptography Subject Public Key Information;
[7] FIPS PUB 186-4 Federal Information Processing Standards Publication; Digital Signature Standard (DSS);
[8] ETSI EN 319 412-1 v1.5.1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures;
[9] ETSI EN 319 412-5 v2.4.1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements;
[10] RFC 6960 – X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP;
[11] ETSI EN 319 411-1 v1.4.1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
[12] ISO 3166 Country Codes;
[13] RFC 3279 - Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
[14] ETSI EN 319 412-3 v1.3.1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
[15] European Product Registry for Energy Labelling (EPREL) GUIDELINE published: https://commission.europa.eu/system/files/2022-11/suppliers_verification_guide.pdf