DIGITALISERINGSSTYRELSEN

Den Danske Stat

Certificate Profiles

Contents

Changelog

Date	Version	Change description
29-10-2020	0.36	OCSP Profiles changed to include nextUpdate
10-11-2020	0.37	Sections on Subject Serial Number added
12-11-2020	1.0	Version updated for release
23-11-2020	1.0.1	Updated based on review from Digst
21-1-2021	1.0.2	Added note on attributes in distinguished name shall only appear once.
29-03-2021	1.0.3	Developer branding removed
06-05-2021	1.0.4	Moved to Documentation, all changes accepted. Reformatting
09-09-2021	1.0.5	Removed project branding and crlDistributionsPoints from OCSP Responder certificates.
03-03-2022	1.0.6	Updated description of OCSP nonce
31-08-2022	1.0.7	Added clarification to section Note on Subject SerialNumber

References

Term	Reference
[Qualified Person]	Public Certificate for qualified person certificates, Version 1.0, October 2019. https://certifikat.gov.dk/politikker-for-tillidstjenester/
[Qualified Employee]	Certificate Policy for qualified employee certificates, Version 1.0, October 2019. https://certifikat.gov.dk/politikker-for-tillidstjenester/
[Qualified Organization]	Public Certificate Policy for qualified organizational certificates. Version 1.0, October 2019. https://certifikat.gov.dk/politikker-for-tillidstjenester/
[OCES Employee]	Certificate Policy for OCES employee certificates (Public Certificates for Electronic Service), Version 7.0, October 2019. https://certifikat.gov.dk/politikker-for-tillidstjenester/
[OCES Organization]	Certificate Policy for OCES organizational certificates (Public Certificates for Electronic Services), Version 7.0, October 2019. https://certifikat.gov.dk/politikker-for-tillidstjenester/
[ETSI EN 319 412-2]	ETSI EN 319 412-2, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons, ETSI ESI, Version 2.2.1, July 2020. https://www.etsi.org/standards

[RFC5280]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, IETF Network Working Group, Request for Comments : 5280, May 2008, https://tools.ietf.org/html/rfc5280

1 Introduction

This document specifies the profile of certificates provided by the Den Danske Stat's infrastructure. The profiles are based on the requirements specified in the [Qualified Person, Qualified Employee, Qualified Organization, OCES Employee, OCES Organization].

The infrastructure supports the following key hierarchy with root CAs being self-signed entities and with indention indicating place in hierarchy.

- OCES root CA
    - OCES intermediate CA
        - MOCES (OCES certificate issued to a natural person associated with a legal person),
        - VOCES and FOCES (OCES certificate issued to a legal person)
        - OCES OCSP Responder for subject certificates
    - OCES OCSP Responder for CA certificates
- Qualified root CA
    - Qualified intermediate CA
        - QPerson (Qualified certificate issued to a natural person)
        - QEmployee (Qualified certificate issued to a natural person associated with a legal person)
        - QOrg (Qualified certificate issued to a legal person)
        - Qualified OCSP Responder for subject certificates
    - Qualified OCSP Responder for certificates
    - Qualified Timestamping Unit

All certificates are of type X.509v3 conformant to [RFC5280] and [ETSI EN 319 412-2].

The content of all certificates can be divided into

- Formalia covering version, serialNumber and Validity Period
- Issuer Distinguished Name (Issuer DN)
- Subject Distinguished Name (Subject DN)
- Public Key
- Extensions
- Signature

All content will be described in detail for the certificate types.

1.1 Notes regarding use of X.509 extensions

Note that for the keyUsage extension the attribute bit 1 is denoted *contentCommitment* as in recent editions of X.509 instead of the old term *nonrepudiation*.

Note than the following extension MUST NOT be present in the certificate profiles:

- policyMapping
- subjectDirectoryAttributes
- nameConstraints
- policyConstraints
- inhibitAnyPolicy

1.2 Note on certificate validity

The certificate periods described in this document assumes a Year is 365 days.

1.3 Note on key sizes and certificate validity

The certificate hierarchies described in this profile consist of a root certificate followed by an intermediate certificate which issues subject certificates.

The root certificate shall have the longest validity period and we aim for the maximum period recognized by industry standards. The intermediate certificates shall have a validity which is longer than subject certificates.

The certificate signature algorithms are always based on the RSA PSS scheme. It is parametrized by a digest hash algorithm and mask generation function (mgf). The mask generation functions, currently being available, are again based on a hash algorithm. While the digest hash algorithm and the mask generation function hash algorithm in principle can be distinct, it is good practice to aid consuming software and use the same algorithm.

In this scheme, in general for certificates with a validity of less than or equal to 3 Years, the hash algorithm is SHA-256 and for certificates with a longer validity, the hash algorithm is SHA-512. However, for a specific certificate signing key, the hash algorithm will always be the same.

Based on the above the following key sizes, algorithms and validity have been chosen for the profiles:

- Root CA: RSA 4096 bits and 25 Years and self-signed using RSA PSS with SHA-512.
- Intermedia CA: RSA 3072 bits and 10 Years and signed using RSA PSS with SHA-512
- Subject certificates signed using RSA PSS with SHA-256:
    - Long term RSA 3072 bits and 3 Years.
    - Short term EC 256 and 10 Days.
- Timestamp: RSA 4096 bits and 20 Years and signed using RSA PSS with SHA-512
- OCSP: RSA 3072 and or
    - root and intermediate validity are 3 months and signed using RSA PSS with SHA-512[1].
    - subject certificates validity is 72 hours and signed using RSA PSS with SHA-256.

1.4 Note on certificate attribute sizes

The profiles specified in the next sections are conformant to RFC 5280, PKIX Certificate and CRL Profile. The certificates contain subject attributes, which has the following restrictions in size.

Attribute	Size	Rationale
Subject Attributes		
organizationName	64	RFC 5280 indicates (ub-organization-name).
commonName	64	RFC 5280 indicates (ub-common-name).
givenName	128	RFC 5280 indicates 32768 (ub-name) for Surname and givenName. 128 is sufficient for this implementation.
Surname	128	RFC 5280 indicates 32768 (ub-name) for Surname and Givenname. 128 is sufficient for this implementation.
Pseudonym	128	RFC 5280 indicates (ub-pseudonym).

[1] Here SHA-512 is chosen as the root CA key will always use this algorithm

Attribute	Size	Rationale
organizationIdentifier	64	
serialNumber	64	RFC 5280 indicates (ub-serial-number).
SubjectAlternativeName Attributes		
Email	255	RFC 5280 indicates (ub-emailaddress)

Please note that:

- the size restriction on Pseudonum is artificial as only the value 'Pseudonym' is supported.
- the size of organizationIdentifer is not verified by ITU X.590. However, the 64 characters should be sufficient to encode Danish CVR numbers including NTRDK.

A certification request with an attribute containing a value larger than the restricted size will have its value truncated to the size by removing value data exceeding the allowed size.

1.5 Note on Subject SerialNumber

For the end entity certificates specified in this profile, the Subject DN serialNumber (SSN) must adhere to the following format:

UI:DK-<identity type acronym>:<persistence level acronym>:<uuid>

Three types of identities are supported:

Identity Type	Acronym	Description
Person	P	Physical person – usually Danish citizens.
Employee	E	Employee identity – a person associated to an organization, and acting in this context.
Organization	O	Organization identity – the identity representing the organization itself.

The following persistence levels are used:

Persistence Level	Acronym	Description
Global	G	The identifiers described in the section "Global identifiers" below are used, i.e. Persistent Identifier in employee certificates and CPR UUID in person certificates. All actors receive the same global identifiers. The - now deprecated - PID and RID identifiers are also global.

Persistence Level	Acronym	Description
Certificate	C	For long-term certificates, the user organization may choose to issue a new identifier for each user certificate. In this case, when the employee renews his/her certificate, a new identifier will be used.
Session	S	Identifiers specific to a given session. Every session (authentication or signing) will produce a new identifier, even if the same identity performs the authentication/signing.

For brevity the format will be listed as “UI:DK-X:X:XXXXXXX..XX” in the profile.

1.5.1 Duplicate information

Please note that qualified certificates issued until 5-9-2022 with global persistence level, the subject serial number included the identity type in the uuid, e.g:

UI:DK-O:G:organization:12345678-abcd-dcba-abcd-123456781234

Relying parties shall pay attention to use the correct form when the subject SerialNumber is used.

1.6 Note on name attributes

In the certificate profiles described in the following sections, the name attributes can only appear once.

2 OCES Root CA Profile

2.1 Formalia

Field	Value / Description	Encoding
X.509 version	3 Note that ASN.1-wise this value is encoded as the value 2 while X.509 enumerates from 0.	Integer
serialNumber	Serial number of the issued certificate. Note that this number should not be mistaken for the subject serialNumber.	Integer
Validity Period	The notBefore and notAfter fields specifying the validity of the certificate. 25 Years	UTCTime

2.2 Issuer DN

Field	Value / Description	Encoding
Country	DK	PrintableString (of size 2)
organizationName	Den Danske Stat	UTF8String
commonName	Den Danske Stat OCES rod-CA Note from CP that OCES must be in the name.	UTF8String
organizationalUnitName	For test certificates orginizationalUnitName is included and always on the form: Test - <environment>, where <environment> specifies the test environment that has issued the certificate.	UTF8String

2.3 Subject DN

Field	Value / Description	Encoding
Country	DK	PrintableString
organizationName	Den Danske Stat	UTF8String
commonName	Den Danske Stat OCES rod-CA	UTF8String

organizationalUnitName	For test certificates orginizationalUnitName is included and always on the form: Test - <environment>, where <environment> specifies the test environment that has issued the certificate.	UTF8String

2.4 SubjectPublicKeyInfo

Field	Value / Description	Encoding
Algorithm	RSA Encryption with ASN.1 NULL as algorithm parameter	AlgorithmIdentifier
Public Key	4096 bits RSA key	BitString

2.5 Extensions

Extension	Value / Description	Criticality
subjectKeyIdentifier	Key identifier of the issuers public key corresponding to the private key used to sign a certificate. The optional element keyIdentifier shall be used.	non-critical
keyUsage	bit 5 (keyCertSign) bit 6 (cRLSign)	critical
cRLDistributionPoints	A HTTP or HTTPS URL to a DER-encoded file containing a valid CRL. http://ca1.gov.dk/oces/root/crl/root.crl	non-critical
basicConstraints	cA: TRUE	critical
authorityInformationAccess	The AuthorityInformationAccessSyntax shall include two AccessDescription for this CA certificate location and for OCSP responder location. For the CA certificate: accessMethod shall be id-adcaIssuers accessLocation shall be a HTTP or HTTPS URL to a DER-encoded file containing the CA certificate used to sign the certificate. This can be used for building a trusted certificate path. This is useful for relying parties, which only has the end user certificate (or a fraction of a certificate chain). http://ca1.gov.dk/oces/root/cacert/root.cer	non-critical

Extension	Value / Description	Criticality
	For the OCSP responder: accessMethod shall be id-ad-ocsp. accessLocation shall be HTTP or HTTPS URL (Online Certificate Status Protocol) to the OCSP responder. http://ca1.gov.dk/ocsp	

2.6 Signature

Field	Value / Description

signatureAlgorithm	`RSASSA-PSS-params ::= SEQUENCE {`
	`hashAlgorithm [0] HashAlgorithm DEFAULT`
	`sha1Identifier,`
	`maskGenAlgorithm [1] MaskGenAlgorithm DEFAULT`
	`mgf1SHA1Identifier,`
	`saltLength [2] INTEGER DEFAULT 20,`
	`trailerField [3] INTEGER DEFAULT 1 }`
	hashAlgorithm shall be SHA-512
	maskGenAlgorithm shall be mgf1SHA-512Identifier
	saltLength shall have value 64 and trailerField shall be default value.

Signature	N/A

3 OCES Intermediate CA Profile

3.1 Formalia

Field	Value / Description	Encoding
X.509 version	3 Note that ASN.1-wise this value is encoded as the value 2 while X.509 enumerates from 0.	Integer
serialNumber	Serial number of the issued certificate. Note that this number should not be mistaken for the subject serialNumber.	Integer
Validity Period	The notBefore and notAfter fields specifying the validity of the certificate. 10 Years.	UTCTime

3.2 Issuer DN

Field	Value / Description	Encoding
Country	DK	PrintableString
organizationName	Den Danske Stat	UTF8String
commonName	Den Danske Stat OCES rod-CA	UTF8String
organizationalUnitName	For test certificates orginizationalUnitName is included and always on the form: Test - <environment>, where <environment> specifies the test environment that has issued the certificate.	UTF8String

3.3 Subject DN

Field	Value / Description	Encoding
Country	DK	PrintableString
organizationName	Den Danske Stat	UTF8String
commonName	Den Danske Stat OCES udstedende-CA N N is index for current active intermediate CA, starting from 1.	UTF8String
organizationalUnitName	For test certificates orginizationalUnitName is included and always on the form:	UTF8String

Field	Value / Description	Encoding
	Test - <environment>, where <environment> specifies the test environment that has issued the certificate.	

3.4 SubjectPublicKeyInfo

Field	Value / Description	Encoding
Algorithm	RSA Encryption with ASN.1 NULL as algorithm parameter	AlgorithmIdentifier
Public Key	3072 bits RSA key	BitString

3.5 Extensions

Extension	Value / Description	Criticality
subjectKeyIdentifier	Key identifier of the subjects public key included in the certificate	non-critical
authorityKeyIdentifier	Key identifier of the issuers public key corresponding to the private key used to sign a certificate. The optional element keyIdentifier shall be used.	non-critical
keyUsage	bit 5 (keyCertSign) bit 6 (cRLSign)	critical
cRLDistributionPoints	A HTTP or HTTPS URL to a DER-encoded file containing a valid CRL. http://ca1.gov.dk/oces/root/crl/root.crl	non-critical
authorityInformationAccess	The AuthorityInformationAccessSyntax shall include two AccessDescription for (root) CA certificate location and for OCSP responder location. For the CA certificate: accessMethod shall be id-adcaIssuers accessLocation shall be a HTTP or HTTPS URL to a DER-encoded file containing the CA certificate used to sign the certificate. This can be used for building a trusted certificate path. This is useful for relying parties, which only has the end user certificate (or a fraction of a certificate chain). http://ca1.gov.dk/oces/root/cacert/root.cer	non-critical

Extension	Value / Description	Criticality
	For the OCSP responder: accessMethod shall be id-ad-ocsp. accessLocation shall be HTTP or HTTPS URL (Online Certificate Status Protocol) to the OCSP responder. http://ca1.gov.dk/ocsp	
basicConstraints	cA: TRUE pathLenConstraint: 0	critical

3.6 Signature

Field	Value / Description

signatureAlgorithm	`RSASSA-PSS-params ::= SEQUENCE {`
	`hashAlgorithm [0] HashAlgorithm DEFAULT`
	`sha1Identifier,`
	`maskGenAlgorithm [1] MaskGenAlgorithm DEFAULT`
	`mgf1SHA1Identifier,`
	`saltLength [2] INTEGER DEFAULT 20,`
	`trailerField [3] INTEGER DEFAULT 1 }`
	hashAlgorithm shall be SHA-512
	maskGenAlgorithm shall be mgf1SHA-512Identifier
	saltLength shall be 64 and trailerField shall be default value.

Signature	N/A

4 MOCES Certificate Profile

OCES certificate issued to a natural person associated with a legal person.

4.1 Formalia

Field	Value / Description	Encoding
X.509 version	3 Note that ASN.1-wise this value is encoded as the value 2 while X.509 enumerates from 0.	Integer
serialNumber	Serial number of the issued certificate. This serialNumber SHALL be non-sequential across certificates and at least 64-bit to protect against collision attacks of weak hash functions. Note that this number should not be mistaken for the subject serialNumber.	Integer
Validity Period	The notBefore and notAfter fields specifying the validity of the certificate. 3 Years.	UTCTime

4.2 Issuer DN

Field	Value / Description	Encoding
Country	DK	PrintableString
organizationName	Den Danske Stat	UTF8String
commonName	Den Danske Stat OCES udstedende-CA N N is index for current active intermediate CA, starting from 1.	UTF8String
organizationalUnitName	For test certificates orginizationalUnitName is included and always on the form: Test - <environment>, where <environment> specifies the test environment that has issued the certificate.	UTF8String

4.3 Subject DN

Field	Value / Description	Encoding
Country	DK	PrintableString

Field	Value / Description	Encoding
organizationName	Certificate subscribers organizational name	UTF8String
commonName	Certificate subjects common name	UTF8String
givenName	Certificate subjects given name SHALL be present if surname is present. MUST not be present if pseudonym is present.	UTF8String
Surname	Certificate subjects surname SHALL be present if givenName is present. MUST not be present if pseudonym is present.	UTF8String
Pseudonym	Certificate subjects pseudonym MUST not be present if givenName and surname is present.	UTF8String
organizationIdentifier	Certificate subscribers CVR-number in the form NTRDK-XXXXXXXX	UTF8String
serialNumber	Unique identifier for the certificate subject in the form UI:DK-X:X:XXXXXXX..XX Note that this number should not be mistaken for the certificate serialNumber.	PrintableString

4.4 SubjectPublicKeyInfo

Field	Value / Description	Encoding
algorithm	RSA Encryption with ASN.1 NULL as algorithm parameter	AlgorithmIdentifier
Public Key	3072 bits RSA key	BitString

4.5 Extensions

Extension	Value / Description	Criticality
qcStatement-2	semanticsIdentifier: semanticsIdentifier: id-etsi-qcs-semanticsId-Natural nameRegistrationAuthorities: https://uid.gov.dk	non-critical

Extension	Value / Description	Criticality
subjectKeyIdentifier	Key identifier of the subjects public key included in the certificate	non-critical
authorityKeyIdentifier	Key identifier of the issuers public key corresponding to the private key used to sign a certificate.	non-critical
keyUsage	Profile F: bit 0 (digitalSignature) bit 1 (contentCommitment) bit 2 (keyEncipherment)	critical
subjectAlternativeName	If subjects e-mail address is included, it SHALL be inserted in this extension. The extension is optional. MUST be omitted if e-mail is not included.	non-critical
cRLDistributionPoint	A HTTP or HTTPS URL to a DER-encoded file containing a valid CRL. http://ca1.gov.dk/oces/issuing/N/crl/issuing.crl N is index for current active intermediate CA, starting from 1	non-critical
authorityInformationAccess	The AuthorityInformationAccessSyntax shall include two AccessDescription for CA certificate location and for OCSP responder location. For the CA certificate: accessMethod shall be id-adcaIssuers accessLocation shal be a HTTP or HTTPS URL to a DER-encoded file containing the CA certificate used to sign the certificate. This can be used for building a trusted certificate path. This is useful for relying parties, which only has the end user certificate (or a fraction of a certificate chain). http://ca1.gov.dk/oces/issuing/N/cacert/issuing.cer N is index for current active intermediate CA, starting from 1 For the OCSP responder: accessMethod shall be id-ad-ocsp	non-critical

Extension	Value / Description	Criticality
	accessLocation shall be a HTTP or HTTPS URL (Online Certificate Status Protocol) to the OCSP responder. http://ca1.gov.dk/ocsp	

certificatePolicies	Two policies are to be included.
	itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncp (1)
	and
	iso(1) iso-member-body(2) denmark(208) stat(169) pki(1) cp(1) nq(1) medarbejder(2) ver(7)
		non-critical

basicConstraints	cA: FALSE	critical

4.6 Signature

Field	Value / Description

signatureAlgorithm	`RSASSA-PSS-params  ::=  SEQUENCE  {`
	`  hashAlgorithm      [0] HashAlgorithm DEFAULT`
	`                                sha1Identifier,`
	`  maskGenAlgorithm   [1] MaskGenAlgorithm DEFAULT`
	`mgf1SHA1Identifier,`
	`  saltLength         [2] INTEGER DEFAULT 20,`
	`  trailerField       [3] INTEGER DEFAULT 1  }`
	hashAlgorithm shall be SHA-256
	maskGenAlgorithm shall be mgf1SHA-256Identifier
	saltLength shall be 32 and trailerField shall be default value.

signature	N/A

5 VOCES and FOCES Certificate Profiles

Certificates for companies shall be supported in two variants:

- VOCES
- FOCES

The VOCES certificate is aimed to be a general-purpose certificates expected to be used for signing documents and to be part of secure communication. This means it shall have keyUsage including digital signature, contentCommitment and keyAgreement. The FOCES certificate is aimed to be used to be part of secure communication. This means it shall have keyUsage including digital signature and keyAgreement. The exclusion of contentCommitment from FOCES certificates is to indicate the certificate is not aimed to be used for non-repudiation, i.e. document signing.

In the following sections, except for keyUsage everything is similar for VOCES and FOCES certificates. In the keyUsage section, it be clearly marked what is relevant for VOCES and FOCES certificates.

5.1 Formalia

Field	Value / Description	Encoding
X.509 version	3 Note that ASN.1-wise this value is encoded as the value 2 while X.509 enumerates from 0.	Integer
serialNumber	Serial number of the issued certificate. This serialNumber SHALL be non-sequential across certificates and at least 64-bit to protect against collision attacks of weak hash functions. Note that this number should not be mistaken for the subject serialNumber.	Integer
Validity Period	The notBefore and notAfter fields specifying the validity of the certificate. 3 Years.	UTCTime

5.2 Issuer DN

Field	Value / Description	Encoding
Country	DK	PrintableString
organizationName	Den Danske Stat	UTF8String
commonName	Den Danske Stat OCES udstedende-CA N N is index for current active intermediate CA, starting from 1.	UTF8String

Field	Value / Description	Encoding
organizationalUnitName	For test certificates orginizationalUnitName is included and always on the form: Test - <environment>, where <environment> specifies the test environment that has issued the certificate.	UTF8String

5.3 Subject DN

Field	Value / Description	Encoding
country	DK	PrintableString
organizationName	Certificate subscribers organizational name	UTF8String
commonName	Certificate subjects common name	UTF8String
organizationIdentifier	Certificate subscribers CVR-number in the form NTRDK-XXXXXXXX	UTF8String
serialNumber	Unique identifier for the certificate subject in the form UI:DK-X:X:XXXXXXX..XX Note that this number should not be mistaken for the certificate serialNumber.	PrintableString

5.4 SubjectPublicKeyInfo

Field	Value / Description	Encoding
algorithm	RSA Encryption with ASN.1 NULL as algorithm parameter	AlgorithmIdentifier
Public Key	3072 bits RSA key	BitString

5.5 Extensions

Extension	Value / Description	Criticality
qcStatement-2	semanticsIdentifier: id-etsi-qcs-semanticsId-Legal nameRegistrationAuthorities: https://uid.gov.dk	non-critical
subjectKeyIdentifier	Key identifier of the subjects public key included in the certificate	non-critical

Extension	Value / Description	Criticality
authorityKeyIdentifier	Key identifier of the issuers public key corresponding to the private key used to sign a certificate.	non-critical
keyUsage for VOCES	Profile F: bit 0 (digitalSignature) bit 1 (contentCommitment) bit 2 (keyEncipherment)	critical
keyUsage for FOCES	Profile D: bit 0 (digitalSignature) bit 2 (keyEncipherment)	critical
subjectAlternativeName	If subjects e-mail address is included, it SHALL be inserted in this extension. The extension is optional. MUST be omitted if e-mail is not included.	non-critical
cRLDistributionPoint	A HTTP or HTTPS URL to a DER-encoded file containing a valid CRL. http://ca1.gov.dk/oces/issuing/N/crl/issuing.crl N is index for current active intermediate CA, starting from 1	non-critical
authorityInformationAccess	The AuthorityInformationAccessSyntax shall include two AccessDescription for CA certificate location and for OCSP responder location. For the CA certificate: accessMethod shall be id-adcaIssuers accessLocation shal be a HTTP or HTTPS URL to a DER-encoded file containing the CA certificate used to sign the certificate. This can be used for building a trusted certificate path. This is useful for relying parties, which only has the end user certificate (or a fraction of a certificate chain). http://ca1.gov.dk/oces/issuing/N/cacert/issuing.cer N is index for current active intermediate CA, starting from 1 For the OCSP responder:	non-critical

Extension	Value / Description	Criticality
	accessMethod shall be id-ad-ocsp accessLocation shall be a HTTP or HTTPS URL (Online Certificate Status Protocol) to the OCSP responder. http://ca1.gov.dk/ocsp	
certificatePolicies	Two certificate policies are included. Sequence of itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncp (1) and iso(1) iso-member-body(2) denmark(208) stat(169) pki(1) cp(1) nq(1) virksomhed(3) ver(7)	non-critical
basicConstraints	cA: FALSE	critical

5.6 Signature

Field	Value / Description

signatureAlgorithm	`RSASSA-PSS-params ::= SEQUENCE {`
	`hashAlgorithm [0] HashAlgorithm DEFAULT`
	`sha1Identifier,`
	`maskGenAlgorithm [1] MaskGenAlgorithm DEFAULT`
	`mgf1SHA1Identifier,`
	`saltLength [2] INTEGER DEFAULT 20,`
	`trailerField [3] INTEGER DEFAULT 1 }`
	hashAlgorithm shall be SHA-256
	maskGenAlgorithm shall be mgf1SHA-256Identifier
	saltLength shall be 32 and trailerField shall be default value.

signature	N/A

6 OCES OCSP Responder Profiles

6.1 Formalia

Field	Value / Description	Encoding
X.509 version	3 Note that ASN.1-wise this value is encoded as the value 2 while X.509 enumerates from 0.	Integer
serialNumber	Serial number of the issued certificate. Note that this number should not be mistaken for the subject serialNumber.	Integer
Validity Period	The notBefore and notAfter fields specifying the validity of the certificate. OCSP responder providing status for root and intermediate certificates shall a have validity of 3 months. OCSP responder providing status for subject certificates shall a have validity of 72 hours.	UTCTime

6.2 Issuer DN

The OCES Root CA shall issue OCSP responder certificates which can provide status for OCES root and intermediate CA.

Field	Value / Description	Encoding
Country	DK	PrintableString
organizationName	Den Danske Stat	UTF8String
commonName	Den Danske Stat OCES rod-CA	UTF8String
organizationalUnitName	For test certificates orginizationalUnitName is included and always on the form: Test - <environment>, where <environment> specifies the test environment that has issued the certificate.	UTF8String

The OCES Intermediate certificate shall issue OCSP responder certificates which can provide status for OCES subject certificates.

Field	Value / Description	Encoding
Country	DK	PrintableString
organizationName	Den Danske Stat	UTF8String

Field	Value / Description	Encoding
commonName	Den Danske Stat OCES udstedende-CA N N is index for current active intermediate CA, starting from 1.	UTF8String

6.3 Subject DN

The OCES Root CA shall issue OCSP responder certificates which can provide status for OCES root and intermediate CA.

Field	Value / Description	Encoding
Country	DK	PrintableString
organizationName	Certificate subscribers organizational name shall be the same as issuer organizationName: Den Danske Stat	UTF8String
commonName	Den Danske Stat OCES rod-CA OCSP X X is indicating the OCSP node used for signing the response.	UTF8String

The OCES Intermediate certificate shall issue OCSP responder certificates which can provide status for OCES subject certificates.

Field	Value / Description	Encoding
Country	DK	PrintableString
organizationName	Certificate subscribers organizational name shall be the same as issuer organizationName: Den Danske Stat	UTF8String
commonName	Den Danske Stat OCES udstedende-CA OCSP N X N is index for corresponding intermediate CA. X is indicating the OCSP node used for signing the response.	UTF8String

6.4 SubjectPublicKeyInfo

Field	Value / Description	Encoding
Algorithm	RSA Encryption with ASN.1 NULL as algorithm parameter.	AlgorithmIdentifier
Public Key	3072 bits RSA key	BitString

6.5 Extensions

Extension	Value / Description	Criticality
authorityKeyIdentifier	Key identifier of the issuers public key corresponding to the private key used to sign a certificate.	non-critical
subjectKeyIdentifier	Key identifier of the subjects public key included in the certificate	non-critical
keyUsage	The following profile (ETSI EN 319 412-2): Profile C: bit 0 (digitalSignature)	critical
basicConstraints	cA: FALSE	critical
extKeyUsage	OCSPSigning (OID 1.3.6.1.5.5.7.3.9)	non-critical
OCSPNoCheck	(OID 1.3.6.1.5.5.7.48.1.5)	non-critical

6.6 Signature

Field	Value / Description

signatureAlgorithm	`RSASSA-PSS-params  ::=  SEQUENCE  {`
	`  hashAlgorithm      [0] HashAlgorithm DEFAULT`
	`                              sha1Identifier,`
	`  maskGenAlgorithm   [1] MaskGenAlgorithm DEFAULT`
	`mgf1SHA1Identifier,`
	`  saltLength         [2] INTEGER DEFAULT 20,`
	`  trailerField       [3] INTEGER DEFAULT 1  }`
	For OCSP Responder providing status for root and intermediate certificates:
	hashAlgorithm shall be SHA-512

Field	Value / Description
	maskGenAlgorithm shall be mgf1SHA-512Identifier saltLength shall be 64 and trailerField shall be default value. For OCSP Responder providing status subject certificates: hashAlgorithm shall be SHA-256 maskGenAlgorithm shall be mgf1SHA-256Identifier saltLength shall be 32 and trailerField shall be default value.
signature	N/A

7 Qualified Root CA Profile

7.1 Formalia

Field	Value / Description	Encoding
X.509 version	3 Note that ASN.1-wise this value is encoded as the value 2 while X.509 enumerates from 0.	Integer
serialNumber	Serial number of the issued certificate. Note that this number should not be mistaken for the subject serialNumber.	Integer
Validity Period	The notBefore and notAfter fields specifying the validity of the certificate.25 Years.	UTCTime

7.2 Issuer DN

Field	Value / Description	Encoding
Country	DK	PrintableString (of size 2)
organizationName	Den Danske Stat	UTF8String
commonName	Den Danske Stat kvalificeret rod-CA	UTF8String
organizationalUnitName	For test certificates orginizationalUnitName is included and always on the form: Test - <environment>, where <environment> specifies the test environment that has issued the certificate.	UTF8String

7.3 Subject DN

Field	Value / Description	Encoding
Country	DK	PrintableString (of size 2)
organizationName	Den Danske Stat	UTF8String
commonName	Den Danske Stat kvalificeret rod-CA	UTF8String
organizationalUnitName	For test certificates orginizationalUnitName is included and always on the form: Test - <environment>, where <environment> specifies the test environment that has issued the certificate.	UTF8String

7.4 SubjectPublicKeyInfo

Field	Value / Description	Encoding
algorithm	RSA Encryption with ASN.1 NULL as algorithm parameter	AlgorithmIdentifier
Public Key	4096 bits RSA key	BitString

7.5 Extensions

Extension	Value / Description	Criticality
subjectKeyIdentifier	Key identifier of the issuers public key corresponding to the private key used to sign a certificate.	non-critical
keyUsage	bit 5 (keyCertSign) bit 6 (cRLSign)	critical
cRLDistributionPoint	A HTTP or HTTPS URL to a DER-encoded file containing a valid CRL. http://ca1.gov.dk/qualified/root/crl/root.crl	non-critical
basicConstraints	cA: TRUE	critical
authorityInformationAccess	The AuthorityInformationAccessSyntax shall include two AccessDescription for (root) CA certificate location and for OCSP responder location. For the CA certificate: accessMethod shall be id-adcaIssuers accessLocation shall be a HTTP or HTTPS URL to a DER-encoded file containing the CA certificate used to sign the certificate. This can be used for building a trusted certificate path. This is useful for relying parties, which only has the end user certificate (or a fraction of a certificate chain). http://ca1.gov.dk/qualified/root/cacert/root.cer For the OCSP responder: accessMethod shall be id-ad-ocsp. accessLocation shall be HTTP or HTTPS URL (Online Certificate Status Protocol) to the OCSP responder. http://ca1.gov.dk/ocsp	non-critical

7.6 Signature

Field	Value / Description
signatureAlgorithm	RSASSA-PSS-params ::= SEQUENCE { hashAlgorithm [0] HashAlgorithm DEFAULT sha1Identifier, maskGenAlgorithm [1] MaskGenAlgorithm DEFAULT mgf1SHA1Identifier, saltLength [2] INTEGER DEFAULT 20, trailerField [3] INTEGER DEFAULT 1 } hashAlgorithm shall be SHA-512 maskGenAlgorithm shall be mgf1SHA-512Identifier saltLength shall be 64 and trailerField shall be default value.
signature	N/A

8 Qualified Intermediate CA Profile

8.1 Formalia

Field	Value / Description	Encoding
X.509 version	3 Note that ASN.1-wise this value is encoded as the value 2 while X.509 enumerates from 0.	Integer
serialNumber	Serial number of the issued certificate. Note that this number should not be mistaken for the subject serialNumber.	Integer
Validity Period	The notBefore and notAfter fields specifying the validity of the certificate. 10 Years.	UTCTime

8.2 Issuer DN

Field	Value / Description	Encoding
Country	DK	PrintableString (of size 2)
organizationName	Den Danske Stat	UTF8String
commonName	Den Danske Stat kvalificeret rod-CA	UTF8String
organizationalUnitName	For test certificates orginizationalUnitName is included and always on the form: Test - <environment>, where <environment> specifies the test environment that has issued the certificate.	UTF8String

8.3 Subject DN

Field	Value / Description	Encoding
Country	DK	PrintableString
organizationName	Den Danske Stat	UTF8String
commonName	Den Danske Stat kvalificeret udstedende-CA N N is index for current active intermediate CA, starting from 1.	UTF8String

Field	Value / Description	Encoding
organizationalUnitName	For test certificates orginizationalUnitName is included and always on the form: Test - <environment>, where <environment> specifies the test environment that has issued the certificate.	UTF8String

8.4 SubjectPublicKeyInfo

Field	Value / Description	Encoding
algorithm	RSA Encryption with ASN.1 NULL as algorithm parameter	AlgorithmIdentifier
Public Key	3072 bits RSA key	BitString

8.5 Extensions

Extension	Value / Description	Criticality
subjectKeyIdentifier	Key identifier of the subject's public key included in the certificate	non-critical
authorityKeyIdentifier	Key identifier of the issuers public key corresponding to the private key used to sign a certificate.	non-critical
keyUsage	bit 5 (keyCertSign) bit 6 (cRLSign)	critical
cRLDistributionPoint	A HTTP or HTTPS URL to a DER-encoded file containing a valid CRL. http://ca1.gov.dk/qualified/root/crl/root.crl	non-critical
authorityInformationAccess	The AuthorityInformationAccessSyntax shall include two AccessDescription for (root) CA certificate location and for OCSP responder location. For the CA certificate: accessMethod shall be id-adcaIssuers accessLocation shall be a HTTP or HTTPS URL to a DER-encoded file containing the CA certificate used to sign the certificate. This can be used for building a trusted certificate path. This is useful for relying parties, which only has the end user certificate (or a fraction of a certificate chain).	non-critical

Extension	Value / Description	Criticality
	http://ca1.gov.dk/qualified/root/cacert/root.cer For the OCSP responder: accessMethod shall be id-ad-ocsp. accessLocation shall be HTTP or HTTPS URL (Online Certificate Status Protocol) to the OCSP responder. http://ca1.gov.dk/ocsp	
basicConstraints	cA: TRUE pathLenConstraint: 0	critical

8.6 Signature

Field	Value / Description
signatureAlgorithm	RSASSA-PSS-params ::= SEQUENCE { hashAlgorithm [0] HashAlgorithm DEFAULT sha1Identifier, maskGenAlgorithm [1] MaskGenAlgorithm DEFAULT mgf1SHA1Identifier, saltLength [2] INTEGER DEFAULT 20, trailerField [3] INTEGER DEFAULT 1 } hashAlgorithm shall be SHA-512 maskGenAlgorithm shall be mgf1SHA-512Identifier saltLength shall be 64 and trailerField shall be default value.
signature	N/A

9 QPerson Certificate Profile

9.1 Formalia

Field	Value / Description	Encoding
X.509 version	3 Note that ASN.1-wise this value is encoded as the value 2 while X.509 enumerates from 0.	Integer
serialNumber	Serial number of the issued certificate. This serialNumber SHALL be non-sequential across certificates and at least 64-bit to protect against collision attacks of weak hash functions. Note that this number should not be mistaken for the subject serialNumber.	Integer
Validity Period	The notBefore and notAfter fields specifying the validity of the certificate. 10 Days	UTCTime

9.2 Issuer DN

Field	Value / Description	Encoding
Country	DK	PrintableString
organizationName	Den Danske Stat	UTF8String
commonName	Den Danske Stat kvalificeret udstedende-CA N N is index for current active intermediate CA, starting from 1.	UTF8String
organizationalUnitName	For test certificates orginizationalUnitName is included and always on the form: Test - <environment>, where <environment> specifies the test environment that has issued the certificate.	UTF8String

9.3 Subject DN

Field	Value / Description	Encoding
Country	DK	PrintableString
commonName	Certificate subjects common name	UTF8String

Field	Value / Description	Encoding
givenName	Certificate subjects given name SHALL be present if surname is present. MUST not be present if pseudonym is present.	UTF8String
surname	Certificate subjects surname SHALL be present if givenName is present. MUST not be present if pseudonym is present.	UTF8String
pseudonym	Certificate subjects pseudonym MUST not be present if givenName and surname is present.	UTF8String
serialNumber	Unique identifier for the certificate subject in the form UI:DK-X:X:XXXXXXX..XX Note that this number should not be mistaken for the certificate serialNumber.	PrintableString

9.4 SubjectPublicKeyInfo

Field	Value / Description	Encoding
algorithm	id-ecPublicKey with parameter namedCurve containing the elliptic curve identifier secp256r1.	AlgorithmIdentifier
Public Key	A public key on secp256r1	BitString

9.5 Extensions

Extension	Value / Description	Criticality
qcStatement-2	From CP covering QPerson krav 7.1.2-01 Since the certificate is qualified: esi4-qcStatement-1 must be present. Since the certificate is qualified according to eIDAS regulation (and not signature directive) esi4-qcStatement-6 must be present Since this is a QPerson certificate the QCType shall have the value for electronic signature: id-etsi-qct-esign	non-critical

Extension	Value / Description	Criticality
	Since the private key is manged by a QSCD esi4-qcStatement-4 From CP covering QPerson Krav 7.1.2-02 semanticsIdentifier: id-etsi-qcs-semanticsId-Natural nameRegistrationAuthorities: https://uid.gov.dk	
subjectKeyIdentifier	Key identifier of the subjects public key included in the certificate	non-critical
authorityKeyIdentifier	Key identifier of the issuers public key corresponding to the private key used to sign a certificate.	non-critical
keyUsage	Profile A: bit 1 (contentCommitment)	critical
cRLDistributionPoint	A HTTP or HTTPS URL to a DER-encoded file containing a valid CRL. http://ca1.gov.dk/qualified/issuing/N/crl/issuing.crl N is index for current active intermediate CA, starting from 1.	non-critical
authorityInformationAccess	The AuthorityInformationAccessSyntax shall include two AccessDescription for (root) CA certificate location and for OCSP responder location. For the CA certificate: accessMethod shall be id-adcaIssuers accessLocation shall be a HTTP or HTTPS URL to a DER-encoded file containing the CA certificate used to sign the certificate. This can be used for building a trusted certificate path. This is useful for relying parties, which only has the end user certificate (or a fraction of a certificate chain). http://ca1.gov.dk/qualified/issuing/N/cacert/issuing.cer N is index for current active intermediate CA, starting from 1. For the OCSP responder: accessMethod shall be id-ad-ocsp.	non-critical

Extension	Value / Description	Criticality
	accessLocation shall be HTTP or HTTPS URL (Online Certificate Status Protocol) to the OCSP responder. http://ca1.gov.dk/ocsp	

certificatePolicies	Sequence of
	itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112)
	policy-identifiers(1) qcp-natural-qscd (2)
	and
	iso(1) iso-member-body(2) denmark(208) stat(169) pki(1) cp(1) q(2) person(1) ver(1)
		non-critical

basicConstraints	cA: FALSE	Critical

9.6 Signature

Field	Value / Description

signatureAlgorithm	`RSASSA-PSS-params  ::=  SEQUENCE  {`
	`  hashAlgorithm      [0] HashAlgorithm DEFAULT`
	`                                    sha1Identifier,`
	`  maskGenAlgorithm   [1] MaskGenAlgorithm DEFAULT`
	`mgf1SHA1Identifier,`
	`  saltLength         [2] INTEGER DEFAULT 20,`
	`  trailerField       [3] INTEGER DEFAULT 1  }`
	hashAlgorithm shall be SHA-256
	maskGenAlgorithm shall be mgf1SHA-256Identifier
	saltLength shall be 32 and trailerField shall be default value.

signature	N/A

10 QEmployee Certificate Profile

10.1 Formalia

Field	Value / Description	Encoding
X.509 version	3 Note that ASN.1-wise this value is encoded as the value 2 while X.509 enumerates from 0.	Integer
serialNumber	Serial number of the issued certificate. This serialNumber SHALL be non-sequential across certificates and at least 64-bit to protect against collision attacks of weak hash functions. Note that this number should not be mistaken for the subject serialNumber.	Integer
Validity Period	The notBefore and notAfter fields specifying the validity of the certificate. For certificates issued through the signingservice, validity is 10 days. For certificates issued through Erhvervsidentitetsadministrationskomponenten validity is 3 Years.	UTCTime

10.2 Issuer DN

Field	Value / Description	Encoding
Country	DK	PrintableString
organizationName	Den Danske Stat	UTF8String
commonName	Den Danske Stat kvalificeret udstedende-CA N N is index for current active intermediate CA, starting from 1.	UTF8String
organizationalUnitName	For test certificates orginizationalUnitName is included and always on the form: Test - <environment>, where <environment> specifies the test environment that has issued the certificate.	UTF8String

10.3 Subject DN

Field	Value / Description	Encoding
Country	DK	PrintableString
organizationName	Certificate subscribers organizational name	UTF8String
commonName	Certificate subjects common name	UTF8String
givenName	Certificate subjects given name SHALL be present if surname is present. MUST not be present if pseudonym is present.	UTF8String
Surname	Certificate subjects surname SHALL be present if givenName is present. MUST not be present if pseudonym is present.	UTF8String
pseudonym	Certificate subjects pseudonym MUST not be present if givenName and surname is present.	UTF8String
organizationIdentifier	Certificate subscribers CVR-number in the form NTRDK-XXXXXXXX	UTF8String
serialNumber	Unique identifier for the certificate subject in the form UI:DK-X:X:XXXXXXX..XX Note that this number should not be mistaken for the certificate serialNumber.	PrintableString

10.4 SubjectPublicKeyInfo

Field	Value / Description	Encoding
algorithm	If the certificate is issued through the Signingservice: id-ecPublicKey with parameter namedCurve containing the elliptic curve identifier secp256r1. If the certificate is issued through Erhvervsidentitetsadministrationskomponenten: RSA Encryption with ASN.1 NULL as algorithm parameter.	AlgorithmIdentifier

Field	Value / Description	Encoding
Public Key	If the certificate is issued through the Signingservice: A public key on secp256r1 If the certificate is issued through Erhvervsidentitetsadministrationskomponenten: 3072 bits RSA key	BitString

10.5 Extensions

Extension	Value / Description	Criticality
qcStatement-2	From CP covering QEmployee krav 7.1.2-01 Since the certificate is qualified: esi4-qcStatement-1 must be present. Since the certificate is qualified according to eIDAS regulation (and not signature directive) esi4-qcStatement-6 must be present Since this is a QEmployee certificate the QCType shall have the value for electronic signature: id-etsi-qct-esign Since the private key is managed by a QSCD esi4-qcStatement-4 From CP covering QEmployee Krav 7.1.2-02 semanticsIdentifier: id-etsi-qcs-semanticsId-Natural nameRegistrationAuthorities: https://uid.gov.dk	non-critical
subjectKeyIdentifier	Key identifier of the subjects public key included in the certificate	
authorityKeyIdentifier	Key identifier of the issuers public key corresponding to the private key used to sign a certificate.	non-critical
keyUsage	Profile A: bit 1 (contentCommitment)	critical
subjectAlternativeName	If subjects e-mail address is included it SHALL be inserted in this extension. The extension is optional. MUST be omitted if e-mail is not included.	non-critical

Extension	Value / Description	Criticality
	For certificates issued through the signingservice this extension is not supported. For certificates issued through Erhvervsidentitetsadministrationskomponenten this extension is supported.	
cRLDistributionPoint	A HTTP or HTTPS URL to a DER-encoded file containing a valid CRL. http://ca1.gov.dk/qualified/issuing/N/crl/issuing.crl N is index for current active intermediate CA, starting from 1.	non-critical
authorityInformationAccess	The AuthorityInformationAccessSyntax shall include two AccessDescription for (root) CA certificate location and for OCSP responder location. For the CA certificate: accessMethod shall be id-adcaIssuers accessLocation shall be a HTTP or HTTPS URL to a DER-encoded file containing the CA certificate used to sign the certificate. This can be used for building a trusted certificate path. This is useful for relying parties, which only has the end user certificate (or a fraction of a certificate chain). http://ca1.gov.dk/qualified/issuing/N/cacert/issuing.cer N is index for current active intermediate CA, starting from 1. For the OCSP responder: accessMethod shall be id-ad-ocsp. accessLocation shall be HTTP or HTTPS URL (Online Certificate Status Protocol) to the OCSP responder. http://ca1.gov.dk/ocsp	non-critical

certificatePolicies	Sequence of
	itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112)
	policy-identifiers(1) qcp-natural-qscd (2)
	and
		non-critical

Extension	Value / Description	Criticality
	iso(1) iso-member-body(2) denmark(208) stat(169) pki(1) cp(1) q(2) medarbejder(2) ver(1)	
basicConstraints	cA: FALSE	critical

The keyUsage extension only includes contentCommitment in the initial delivery. Certificate profiles is manged by the CA software and changes to the extension can be provided as a configuration without any software change.

10.6 Signature

Field	Value / Description

signatureAlgorithm	`RSASSA-PSS-params ::= SEQUENCE {`
	`hashAlgorithm [0] HashAlgorithm DEFAULT`
	`sha1Identifier,`
	`maskGenAlgorithm [1] MaskGenAlgorithm DEFAULT`
	`mgf1SHA1Identifier,`
	`saltLength [2] INTEGER DEFAULT 20,`
	`trailerField [3] INTEGER DEFAULT 1 }`
	hashAlgorithm shall be SHA-256
	maskGenAlgorithm shall be mgf1SHA-256Identifier
	saltLength shall be 32 and trailerField shall be default value.

signature	N/A

11 QOrg Certificate Profile

11.1 Formalia

Field	Value / Description	Encoding
X.509 version	3 Note that ASN.1-wise this value is encoded as the value 2 while X.509 enumerates from 0.	Integer
serialNumber	Serial number of the issued certificate. This serialNumber SHALL be non-sequential across certificates and at least 64-bit to protect against collision attacks of weak hash functions. Note that this number should not be mistaken for the subject serialNumber.	Integer
Validity Period	The notBefore and notAfter fields specifying the validity of the certificate. For certificates issued through the signingservice, validity is 10 days. For certificates issued through Erhvervsidentitetsadministrationskomponenten validity is 3 Years.	UTCTime

11.2 Issuer DN

Field	Value / Description	Encoding
Country	DK	PrintableString
organizationName	Den Danske Stat	UTF8String
commonName	Den Danske Stat kvalificeret udstedende-CA N N is index for current active intermediate CA, starting from 1.	UTF8String
organizationalUnitName	For test certificates orginizationalUnitName is included and always on the form: Test - <environment>, where <environment> specifies the test environment that has issued the certificate.	UTF8String

11.3 Subject DN

Field	Value / Description	Encoding
country	DK	PrintableString
organizationName	Certificate subscribers organizational name	UTF8String
commonName	Certificate subjects common name	UTF8String
organizationIdentifier	Certificate subscribers CVR-number in the form NTRDK-XXXXXXXX	UTF8String
serialNumber	Unique identifier for the certificate subject in the form UI:DK-X:X:XXXXXXX..XX Note that this number should not be mistaken for the certificate serialNumber.	PrintableString

11.4 SubjectPublicKeyInfo

Field		Value / Description	Encoding
algorithm		If the certificate is issued through the Signingservice: id-ecPublicKey with parameter namedCurve containing the elliptic curve identifier secp256r1. If the certificate is issued through Erhvervsidentitetsadministrationskomponenten: RSA Encryption with ASN.1 NULL as algorithm parameter.	AlgorithmIdentifier
Public Key		If the certificate is issued through the Signingservice: A public key on secp256r1 If the certificate is issued through Erhvervsidentitetsadministrationskomponenten: 3072 bits RSA key	BitString

11.5 Extensions

Extension	Value / Description	Criticality
qcStatement-2	From CP covering QOrg krav 7.1.2-01 Since the certificate is qualified:	non-critical

Extension	Value / Description	Criticality
	esi4-qcStatement-1 must be present. Since the certificate is qualified according to eIDAS regulation (and not signature directive) esi4-qcStatement-6 must be present Since this is a QOrg certificate the QCType shall have the value for electronic signature: id-etsi-qct-eseal Since the private key is managed by a QSCD esi4-qcStatement-4 From CP covering QOrg Krav 7.1.2-02 semanticsIdentifier: id-etsi-qcs-semanticsId-Legal nameRegistrationAuthorities: https://uid.gov.dk	
subjectKeyIdentifier	Key identifier of the subjects public key included in the certificate	non-critical
authorityKeyIdentifier	Key identifier of the issuers public key corresponding to the private key used to sign a certificate.	non-critical
keyUsage	Profile A: bit 1 (contentCommitment)	critical
subjectAlternativeName	If subjects e-mail address is included it SHALL be inserted in this extension. The extension is optional. MUST be omitted if e-mail is notincluded. For certificates issued through the signingservice this extension is not supported. For certificates issued through Erhvervsidentitetsadministrationskomponenten this extension is supported.	non-critical
cRLDistributionPoint	A HTTP or HTTPS URL to a DER-encoded file containing a valid CRL. http://ca1.gov.dk/qualified/issuing/N/crl/issuing.crl N is index for current active intermediate CA, starting from 1.	non-critical

Extension	Value / Description	Criticality
authorityInformationAccess	The AuthorityInformationAccessSyntax shall include two AccessDescription for (root) CA certificate location and for OCSP responder location. For the CA certificate: accessMethod shall be id-adcaIssuers accessLocation shall be a HTTP or HTTPS URL to a DER-encoded file containing the CA certificate used to sign the certificate. This can be used for building a trusted certificate path. This is useful for relying parties, which only has the end user certificate (or a fraction of a certificate chain). http://ca1.gov.dk/qualified/issuing/N/cacert/issuing.cer N is index for current active intermediate CA, starting from 1. For the OCSP responder: accessMethod shall be id-ad-ocsp. accessLocation shall be HTTP or HTTPS URL (Online Certificate Status Protocol) to the OCSP responder. http://ca1.gov.dk/ocsp	non-critical

certificatePolicies	Sequence of
	Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112)
	policy-identifiers(1) qcp-legal-qscd (3)
	and
	iso(1) iso-member-body(2) denmark(208) stat(169) pki(1) cp(1) q(2) virksomhed(3) ver(1)
		non-critical

basicConstraints	cA: FALSE	critical

The keyUsage extension only includes contentCommitment in the initial delivery. Certificate profiles is manged by the CA software and changes to the extension can be provided as a configuration without any software change.

11.6 Signature

Field	Value / Description
signatureAlgorithm	RSASSA-PSS-params ::= SEQUENCE { hashAlgorithm [0] HashAlgorithm DEFAULT sha1Identifier, maskGenAlgorithm [1] MaskGenAlgorithm DEFAULT mgf1SHA1Identifier, saltLength [2] INTEGER DEFAULT 20, trailerField [3] INTEGER DEFAULT 1 } hashAlgorithm shall be SHA-256 maskGenAlgorithm shall be mgf1SHA-256Identifier saltLength shall be 32 and trailerField shall be default value.
signature	N/A

12 Qualified OCSP Responder

12.1 Formalia

Field	Value / Description	Encoding
X.509 version	3 Note that ASN.1-wise this value is encoded as the value 2 while X.509 enumerates from 0.	Integer
serialNumber	Serial number of the issued certificate. This serialNumber SHALL be long and at least 64-bit to protect against collision attacks of weak hash functions. Note that this number should not be mistaken for the subject serialNumber.	Integer
Validity Period	The notBefore and notAfter fields specifying the validity of the certificate. OCSP responder providing status for root and intermediate certificates shall a have validity of 3 months. OCSP responder providing status for subject certificates shall a have validity of 72 hours.	UTCTime

12.2 Issuer DN

The Qualified Root certification authority shall issue OCSP responder certificates which can provide status for Qualified Root and Qualified Intermediate certificates.

Field	Value / Description	Encoding
Country	DK	PrintableString
organizationName	Den Danske Stat	UTF8String
commonName	Den Danske Stat kvalificeret rod-CA	UTF8String
organizationalUnitName	For test certificates orginizationalUnitName is included and always on the form: Test - <environment>, where <environment> specifies the test environment that has issued the certificate.	UTF8String

The Qualified Intermediate certification authority shall issue OCSP responder certificates which can provide status for Qualified subject certificates.

Field	Value / Description	Encoding
Country	DK	PrintableString
organizationName	Den Danske Stat	UTF8String
commonName	Den Danske Stat kvalificeret udstedende-CA N N is index for current active intermediate CA, starting from 1.	UTF8String
organizationalUnitName	For test certificates orginizationalUnitName is included and always on the form: Test - <environment>, where <environment> specifies the test environment that has issued the certificate.	UTF8String

12.3 Subject DN

The Qualified Root certification authority shall issue OCSP responder certificates which can provide status for Qualified Root and Qualified Intermediate certificates.

Field	Value / Description	Encoding
country	DK	PrintableString
organizationName	Certificate subscribers organizational name: "Den Danske Stat"	UTF8String
commonName	Den Danske Stat kvalificeret rod-CA OCSP X X is indicating the OCSP node used for signing the response.	UTF8String

The Qualified Intermediate certification authority shall issue OCSP responder certificates which can provide status for Qualified subject certificates.

Field	Value / Description	Encoding
country	DK	PrintableString
organizationName	Certificate subscribers organizational name: "Den Danske Stat"	UTF8String
commonName	Den Danske Stat kvalificeret udstedende-CA OCSP N X	UTF8String

Field	Value / Description	Encoding
	Where ”N” is index for the corresponding intermediate CA. X is indicating the OCSP node used for signing the response.	

12.4 SubjectPublicKeyInfo

Field	Value / Description	Encoding
algorithm	RSA Encryption with ASN.1 NULL as algorithm parameter.	AlgorithmIdentifier
Public Key	3072 bits RSA key	BitString

12.5 Extensions

Extension	Value / Description	Criticality
authorityKeyIdentifier	Key identifier of the issuers public key corresponding to the private key used to sign a certificate.	non-critical
subjectKeyIdentifier	Key identifier of the subjects public key included in the certificate	non-critical
keyUsage	The following profile (ETSI EN 319 412-2): Profile C: bit 0 (digitalSignature)	critical
basicConstraints	cA: FALSE	critical
extKeyUsage	OCSPSigning (1.3.6.1.5.5.7.3.9)	non-critical
OCSPNoCheck	(OID 1.3.6.1.5.5.7.48.1.5)	non-critical

12.6 Signature

Field	Value / Description

signatureAlgorithm	`RSASSA-PSS-params ::= SEQUENCE {`
	`hashAlgorithm [0] HashAlgorithm DEFAULT`
	`sha1Identifier,`
	`maskGenAlgorithm [1] MaskGenAlgorithm DEFAULT`

	`mgf1SHA1Identifier,`
	`  saltLength         [2] INTEGER DEFAULT 20,`
	`  trailerField       [3] INTEGER DEFAULT 1  }`
	For OCSP Responder providing status for root and intermediate certificates:
	hashAlgorithm shall be SHA-512
	maskGenAlgorithm shall be mgf1SHA-512Identifier
	saltLength shall be 64 and trailerField shall be default value.
	For OCSP Responder providing status subject certificates:
	hashAlgorithm shall be SHA-256
	maskGenAlgorithm shall be mgf1SHA-256Identifier
	saltLength shall be 32 and trailerField shall be default value.

signature	N/A

13 Qualified Timestamp Unit

13.1 Formalia

Field	Value / Description	Encoding
X.509 version	3 Note that ASN.1-wise this value is encoded as the value 2 while X.509 enumerates from 0.	Integer
serialNumber	Serial number of the issued certificate. This serialNumber SHALL be long and at least 64-bit to protect against collision attacks of weak hash functions. Note that this number should not be mistaken for the subject serialNumber.	Integer
Validity Period	The notBefore and notAfter fields specifying the validity of the certificate. 20 Years.	UTCTime

13.2 Issuer DN

This certificate is issued by Qualified Root CA.

Field	Value / Description	Encoding
Country	DK	PrintableString (of size 2)
organizationName	Den Danske Stat	UTF8String
commonName	Den Danske Stat kvalificeret rod-CA	UTF8String
organizationalUnitName	For test certificates orginizationalUnitName is included and always on the form: Test - <environment>, where <environment> specifies the test environment that has issued the certificate.	UTF8String

13.3 Subject DN

Field	Value / Description	Encoding
country	DK	PrintableString
organizationName	Certificate subscribers organizational name: “Digitaliseringsstyrelsen”	UTF8String

Field	Value / Description	Encoding
commonName	Certificate subjects common name. "Kvalificeret tidsstemplingsenhed N" Where N is an index of the TSU starting with 1 The commonName[2] shall uniquely identify the TSU within the TSA.	UTF8String
organizationIdentifier	Certificate subscribers CVR-number in the form NTRDK-34051178	UTF8String
serialNumber	Unique identifier for the certificate subject in the form UI:DK-X:X:XXXXXXX..XX Note that this number should not be mistaken for the certificate serialNumber.	UTF8String

13.4 SubjectPublicKeyInfo

Field	Value / Description	Encoding
algorithm	RSA Encryption with ASN.1 NULL as algorithm parameter.	AlgorithmIdentifier
Public Key	4096 bits RSA key	BitString

13.5 Extensions

Extension	Value / Description	Criticality
authorityKeyIdentifier	Key identifier of the issuers public key corresponding to the private key used to sign a certificate.	non-critical
subjectKeyIdentifier	Key identifier of the subject's public key included in the certificate	non-critical
keyUsage	The following profile (ETSI EN 319 412-2): Profile C: bit 0 (digitalSignature)	critical
cRLDistributionPoint	A HTTP or HTTPS URL to a DER-encoded file containing a valid CRL.	non-critical

[2] The TimeStampAuthority software supports multiple units providing timestamps so the common name must be unique.

Extension	Value / Description	Criticality
	http://ca1.gov.dk/qualified/root/crl/root.crl	
authorityInformationAccess	The AuthorityInformationAccessSyntax shall include two AccessDescription for (root) CA certificate location and for OCSP responder location. For the CA certificate: accessMethod shall be id-adcaIssuers accessLocation shall be a HTTP or HTTPS URL to a DER-encoded file containing the CA certificate used to sign the certificate. This can be used for building a trusted certificate path. This is useful for relying parties, which only has the end user certificate (or a fraction of a certificate chain). http://ca1.gov.dk/qualified/root/cacert/root.cer For the OCSP responder: accessMethod shall be id-ad-ocsp. accessLocation shall be HTTP or HTTPS URL (Online Certificate Status Protocol) to the OCSP responder. http://ca1.gov.dk/ocsp	non-critical
basicConstraints	cA: FALSE	critical
extKeyUsage	timeStamping (1.3.6.1.5.5.7.3.8)	critical

13.6 Signature

Field	Value / Description

signatureAlgorithm	`RSASSA-PSS-params  ::=  SEQUENCE  {`
	`  hashAlgorithm      [0] HashAlgorithm DEFAULT`
	`                                        sha1Identifier,`
	`  maskGenAlgorithm   [1] MaskGenAlgorithm DEFAULT`
	`mgf1SHA1Identifier,`
	`  saltLength         [2] INTEGER DEFAULT 20,`
	`  trailerField       [3] INTEGER DEFAULT 1  }`

Field	Value / Description
	hashAlgorithm shall be SHA-512 maskGenAlgorithm shall be mgf1SHA-512Identifier saltLength shall be 64 and trailerField shall be default value.
signature	N/A

14 CRL

The CRL profile is compliant with IETF RFC 5280 [RFC5280].

14.1 Basic elements

Field	Value / Description	Encoding

CertificateList. signatureAlgorithmIdentifier	`RSASSA-PSS-params ::= SEQUENCE {`
	`hashAlgorithm [0] HashAlgorithm DEFAULT`
	`sha1Identifier,`
	`maskGenAlgorithm [1] MaskGenAlgorithm DEFAULT`
	`mgf1SHA1Identifier,`
	`saltLength [2] INTEGER DEFAULT 20,`
	`trailerField [3] INTEGER DEFAULT 1 }`
	For CRL providing status for root and intermediate certificates:
	hashAlgorithm shall be SHA-512
	maskGenAlgorithm shall be mgf1SHA-512Identifier
	saltLength shall be 64 and trailerField shall be default value.
	For CRL providing status for subject certificates:
	hashAlgorithm shall be SHA-256
	maskGenAlgorithm shall be mgf1SHA-256Identifier
	saltLength shall be 32 and trailerField shall be default value.
		AlgoritmIdentifier

TBSCertList.version	1 to indicate version 2.	Integer
TBSCertList.issuer	Subject Name of certificate used to issue CRL	Name
TBSCertList.thisUpdate	Time of issuance of CRL Datetime format is YYMMDDHHMMSSz	UTCTime
TBSCertList.nextUpdate	For CRL providing status of root and intermediate certificates 3 months after thisUpdate. For CRL providing status of subject certificates 24 hours after thisUpdate. Datetime format is YYMMDDHHMMSSz	UTCTime

14.2 CRL Extensions and CRL entry extensions

Extension	Value / Description	Criticality
CRL Extensions.Authority Key Identifier	Key identifier of the issuers public key corresponding to the private key used to sign a certificate. The optional element keyIdentifier shall be used.	non-critical
CRL Extensions.CRL Number	The CRL serial number.	non-critical
CRL Extensions.expiredCertificatesOnCRL	The inclusion of this extension indicates that the revocation information contains information about revoked certificates since the date described in the time.	non-critical
CRLEntryExtensions.Reason	Indicates the reason for revocation. The following are supported: unspecified (0), keyCompromise (1), cACompromise (2), affiliationChanged (3), superseded (4), cessationOfOperation (5), -- value 7 is not used privilegeWithdrawn (9), The following reasons are not supported by the CA service. cACompromise (2), cessationOfOperation (5), certificateHold (6), removeFromCRL (8), aACompromise (10) In addition it is not possible to change the revocation reason.	non-critical

Extension	Value / Description	Criticality
	CertificateHold and removeFromCRL are used in the context of suspending a certificate. This is not supported by the CA service. aACompromise is only used for attribute certificates, which are not issued by the CA service.	

15 OCSP

The profile is inspired by RFC 5019 with the major exception, that hash algorithm is SHA256 and not as indicated in RFC 5019 SHA-1.

15.1 Request elements

Field	Value / Description	Encoding
OCSPRequest.tbsRequest	Contains one TBSRequest	TBSRequest
OCSPRequest.optionalSignature	Omitted	Omitted
TBSRequest.version	Default v1	Omitted
TBSRequest.requestorName	Omitted	Omitted
TBSRequest.requestList	Contains a list with one entry of Request	Sequence of Request
TBSRequest.requestExtensions	Optional, but if included it shall contain a nonce	Extensions
Nonce	Object Identifier with value 1.3.6.1.5.5.7.48.1.2 Extension value is an Octet String with a nonce value.	This extension is optional and if included the response shall contain the same value.
Request.reqCert	CertID	CertID
Request.singleRequestExtension	Omitted	Omitted
CertID.hashAlgorithm	The hash algorithm used to identify the issuer. The Signing Service uses SHA 256 but other options are supported.	AlgorithmIdentifier
CertID.issuerNameHash	Hash of issuer name	Octet
CertID.issuerKeyHash	Hash of issuers public key	Octet
CertID.serialNumber	Certificate serial number for which status is requested	Integer

15.2 Response elements

Field	Value / Description	Encoding
OCSPResponse.responseStatus	Enum with status of handling the request.	Enumerated
OCSPResponse.responseBytes	If the response is successful, it contains ResponseBytes	ResponseBytes

Field	Value / Description	Encoding
ResponseBytes.responseType	Object Identifier with value PKIX OCSP Basic (1.3.6.1.5.5.7.48.1.1)	Object Identifier
ResponseBytes.response	The response is encoded as an Octet containing one BasicOCSPResponse	Octet
BasicOCSPResponse.tbsResponseData		ResponseData

BasicOCSPResponse.signatureAlgorithm	`RSASSA-PSS-params ::= SEQUENCE {`
	`hashAlgorithm [0] HashAlgorithm DEFAULT`
	`sha1Identifier,`
	`maskGenAlgorithm [1] MaskGenAlgorithm DEFAULT`
	`mgf1SHA1Identifier,`
	`saltLength [2] INTEGER DEFAULT 20,`
	`trailerField [3] INTEGER DEFAULT 1 }`
	hashAlgorithm shall be SHA-256
	maskGenAlgorithm shall be mgf1SHA-256Identifier
	saltLength shall be 32 and trailerField shall be default value.
		AlgorithmIdentifier

BasicOCSPResponse.signature	The signature	Bit String
BasicOCSPResponse.certs	Contains the certificate in the path containing the OCSP responder certificate	Sequence Of Certificate
ResponseData.version	Default 1	Omitted
ResponseData.responderID	The responderID shall be the KeyHash choice, i.e. a SHA-1 of the public key used to sign the response.	ResponderID
ResponseData.producedAt	Time of producing the OCSP response	GeneralizedTime
ResponseData.responses	Contains a SingleResponse	Sequence of SingleResponse
ResponseData.responseExtensions	Shall contain at least one extension Nonce (optional) ArchiveCutoff (mandatory)	Sequence of Extensions
Nonce	Object Identifier with value 1.3.6.1.5.5.7.48.1.2 Extension value is an Octet String with same value as request.	This extension is optional and shall only be included if

Field	Value / Description	Encoding
		the request contains one.
ArchiveCutoff	Object Identifier with value 1.3.6.1.5.5.7.48.1.6 Extension value is GeneralizedTime.	ObjectIdentifier
SingleResponse.certID	Contains the identifier of the certificate for which status is provided.	CertID
SingleResponse.certStatus	A choice with one of good, revoked, unknown	CertStatus
SingleResponse.thisUpdate	The time at which the status being indicated is known to be correct	GeneralizedTime
SingleResponse.nextUpdate	The time at or before which newer information will be available.	GeneralizedTime
SingleResponse.singleExtensions	Omitted	Extensions
CertID.hashAlgorithm	The same as used in the request.	AlgorithmIdentifier
CertID.issuerNameHash	Hash of issuer name	Octet
CertID.issuerKeyHash	Hash of issuers public key	Octet
CertID.serialNumber	Certificate serial number for which status is requested	Integer
CertStatus.good	If the certificate is not revoked: [0] Implicit NULL Either CertStatus.good, CertStatus.revoked or CertStatus.unknown is present.	0x80 0x00
CertStatus.revoked	RevokedInfo Either CertStatus.good, CertStatus.revoked or CertStatus.unknown is present.	RevokedInfo
CertStatus.unknown	If the status is not known: [2] Implicit NULL CertStatus.unknown must be returned if the certificate is unknown to the OCSP responder	0x82 0x00

Field	Value / Description	Encoding
	Either CertStatus.good, CertStatus.revoked or CertStatus.unknown is present.	
RevokedInfo.revocationTime	Time at which the certificate was revoked.	GeneralizedTime
RevokedInfo.revocationReason	Taken from CRL	Reason