CERTIFICATE PROFILES

IN Groupe DK A/S

Document information			
No. of pages : 15	Reference : N/A	Department : eID Development	Classification : Public
Creation date : 17/02/2025		Last saved update: 25/03/2025 17:46	Version: 1.0.1

Version history			
Version	**Date**	**Author**	**Description of update Updated paragraphs**
1.0	17/02/2025 00:00	KJAERSGAARD, Jan	Initial version
1.0.1	25/03/2025 00:00	KJAERSGAARD, Jan	Updated CRL signature algorithm, removed extension from time stamp token and removed OCSP Cutoff extension.
	Cliquez ou appuyez ici pour entrer une date.		
	Cliquez ou appuyez ici pour entrer une date.		
	Cliquez ou appuyez ici pour entrer une date.		
	Cliquez ou appuyez ici pour entrer une date.		

CONTENTS

1 INTRODUCTION

This document describes IN Groupe Denmark A/S QTSP formats for certificates, OCSP request and response, CRL and time-stamp tokens.

The CA hierarchy, CRL and OCSP is as follows:

- Root certificate
  - Qualified issuing CA
    - Qualified Subject certificates for natural person
    - Qualified OCSP Responder certificate
  - Timestamping Unit
  - CRL for certificates issued by the Root.

All references in AuthorityInformationAccess for CA certificates uses the extension .crt and points to ASN.1 DER encoded certificate.

2 PROFILES

2.1 Test certificates

The QTSP issues test certificates in production. For a description of these certificates, consult internal QTSP documentation.

In the external test environment the certificate issuer common name is prepended with “Test -“.

In this environment urls pointing to a certificate or CRL are extended with a pp, i.e.

- Production https://pki.ingroupe.dk/repository/ca/root.crl
- External test environment https://pki.ingroupe.dk/repository/ca/**pp/**root.crl

And url for the OCSP Responder is ocsp.pki.pp.ingroupe.dk

For other test environment, the certificate issuer common name is prepended with “Test (ENV) -“ where ENV is the name of the test environment.

2.2 Root certificate

Field	Value	Critical
Version	V3	
Serial number	Generated by CA software	
Issuer		
CommonName organizationName organizationIdentifier CountryName	IN Groupe Denmark Root CA IN Groupe Denmark A/S NTRDK-30808460 DK	
Validity		
notBefore	Certificate generation time	
notAfter	notBefore + 20 Years	
Subject	Same as Issuer.	
SubjectPublicKeyInfo		
Algorithm Public Key	id-ecPublicKey with parameter namedCurve containing the elliptic curve identifier secp521r1. A public key on secp521r1	
authorityKeyIdentifier	SHA-1 digest of value of the Public Key	False
BasicConstraints	CA: True	True
KeyUsage	bit 5 (keyCertSign) bit 6 (cRLSign)	True
subjectKeyIdentifier	SHA-1 digest of value of the Public Key	False
SignatureAlgorithm	ECDSA with SHA-512	

2.3 Qualified issuing CA

Field	Value	Critical
Version	V3	
Serial number	Generated by CA software	
Issuer	Root certificate Issuer	
Validity		
notBefore	Certificate generation time	
notAfter	notBefore + 10 Years	
Subject		
CommonName	IN Groupe Denmark Qualified issuing CA I	
organizationName	IN Groupe Denmark A/S	
organizationIdentifier	NTRDK-30808460	
CountryName	DK	
SubjectPublicKeyInfo		
Algorithm Public Key	id-ecPublicKey with parameter namedCurve containing the elliptic curve identifier secp384r1. A public key on secp384r1	
authorityInfoAccess	One AccessDescription for id-ad-caIssuers containing the value https://pki.ingroupe.dk/repository/ca/root.crt	False
authorityKeyIdentifier	SHA-1 digest of value of the Root certificate Public Key	False
BasicConstraints	CA: True	True
crlDistributionPoints	url with https://pki.ingroupe.dk/repository/ca/root.crl	False
KeyUsage	bit 5 (keyCertSign) bit 6 (cRLSign)	True
subjectKeyIdentifier	SHA-1 digest of value of the Public Key	False
SignatureAlgorithm	ECDSA with SHA-512	

2.4 Qualified short term subject certificates for natural person

Field	Value	Critical
Version	V3	
Serial number	Generated by CA software	
Issuer		
CommonName	IN Groupe Denmark Qualified issuing CA I	
organizationName	IN Groupe Denmark A/S	
organizationIdentifier	NTRDK-30808460	
CountryName	DK	
Validity		
notBefore	Certificate generation time	
notAfter	notBefore + 15 minutes	
Subject		
CountryName	As received by the identity provider. PrintableString.	
CommonName	If givenName and surname are present, this value is the concatenation of givenName and surname with a space as separator. If either givenName or surname (not both) are present, CommonName consist of the value present. If givenName and surname are not present, the value will be Pseudonym. UTF8String	
givenName	As received by the identity provider. Must only be present if surname is present. Must not be present if pseudonym is present. UTF8String	
surname	As received by the identity provider. Must only be present if givenName is present. Must not be present if pseudonym is present. UTF8String	
pseudonym	If the identity provider request pseudonym to be used, the value will be Pseudonym. In this case givenName and surname shall not be present. UTF8String	
serialNumber	As received by the identity provider.	
SubjectPublicKeyInfo		
Algorithm Public Key	id-ecPublicKey with parameter namedCurve containing the elliptic curve identifier secp256r1. A public key on secp256r1	

Field	Value	Critical
authorityInfoAccess	The authorityInfoAccess shall include two AccessDescriptions for CA certificate and OCSP responder. The AccessDescription for the CA certificate shall be id-ad-caIssuers containing the value https://pki.ingroupe.dk/repository/ca/qualified-ica-1.crt The AccessDescription for the OCSP Responder shall be id-ad-ocsp containing the value https://ocsp.pki.ingroupe.dk	False
authorityKeyIdentifier	SHA-1 digest of value of the Qualified CA certificate Public Key	False
BasicConstraints	CA: False	True
CertificatePolicies	QCP-n-qscd (Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2))	False
KeyUsage	bit 1 (nonRepudiation)	True
qc-statements	Qualified certificate: esi4-qcStatement-1 QSCD: esi4-qcStatement-4 eIDAS regulation: esi4-qcStatement-6 with QcType type id-etsi-qct-esign Semantics identifier: id-qcs-pkixQCSyntax-v2 with type id-etsi-qcs-semanticsId-Natural	False
subjectKeyIdentifier	SHA-1 digest of value of the Public Key	False
Validity Assured Certificate (id-etsi-ext-valassured-ST-certs)	NULL	False
SignatureAlgorithm	ECDSA with SHA-256	

2.5 Qualified CA OCSP Responder Certificate

Field	Value	Critical
Version	V3	
Serial number	Generated by CA software	
Issuer		
CommonName	IN Groupe Denmark Qualified issuing CA I	
organizationName	IN Groupe Denmark A/S	
organizationIdentifier	NTRDK-30808460	

CountryName	DK	
Validity		
notBefore	Certificate generation time	
notAfter	notBefore + 73 hours	
Subject		
CommonName	Qualified CA OCSP Responder	
organizationName	IN Groupe Denmark A/S	
organizationIdentifier	NTRDK-30808460	
CountryName	DK	
SubjectPublicKeyInfo		
Algorithm Public Key	id-ecPublicKey with parameter namedCurve containing the elliptic curve identifier secp256r1. A public key on secp256r1	
authorityInfoAccess	One AccessDescription for id-ad-caIssuers containing the value https://pki.ingroupe.dk/repository/ca/qualified-ica-1.crt	False
authorityKeyIdentifier	SHA-1 digest of value of the Qualified CA certificate Public Key	False
BasicConstraints	CA: False	True
extKeyUsage	OCSPSigning	False
KeyUsage	bit 0 (digitalSignature)	True
id-pkix-ocsp-nocheck	NULL	False
subjectKeyIdentifier	SHA-1 digest of value of the Public Key	False
SignatureAlgorithm	ECDSA with SHA-256	

2.6 CRL profile for Root certificate

Field	Value	Critical
CertificateList		
tbsCertList	TBSCertList	
signatureAlgorithm	SignatureAlgorithm	
signatureValue		
TBSCertList		
version	v2	
signature	SignatureAlgorithm	
issuer	Subject name for Root CA.	
thisUpdate	Production time generated by the root CA.	
nextUpdate	thisUpdate + 3 Months.	

revokedCertificates	Sequence of Sequence {
	userCertificate CertificateSerialNumber
	revocationDate Time
	crlEntryExtensions Extensions
	}
	The crlEntryEntensions include:
	• reasonCode	

crlExtensions	Extensions contains: • AuthorityKeyIdentifier for RootCA • crlNumber CRLReason	
AuthorityKeyIdentifier	SHA-1 digest of value of the Root CA's Public Key	False
CRLNumber	Unique number of the CRL.	False
CRLReason	The reason for revocation.	
SignatureAlgorithm	ECDSA with SHA-512	

2.7 OCSP request and response profile

2.7.1 OCSP request

Field	Value	Restrictions/Critical
OCSP Request		
tbsRequest	TBSRequest	
optionalSignature		Optional field not supported.
TBSRequest		
version	Version	
requestorName		Optional field not supported
requestList	Sequence of Request	Only one entry is supported.
requestExtensions	Extensions	
Version	V1, i.e. value is 0.	
Request		
reqCert	CertID	
singleRequestExtensions		Optional field not supported
CertID		
hashAlgorithm	The hash algorithm used to calculate the next two fields.	
issuerNameHash	The hash of the issuer name as found in the issuer certificate	
issuerKeyHash	The hash of the public key as found in the issuer certificate	
serialNumber	The serial number of the certificate to retrieve status for	
Extensions	Sequence of Extension	Optional field. If included it shall contain a Nonce
Nonce	Octet String with nonce value	False

2.7.2 OCSP response

Field	Value	Restrictions/Critical
OCSPResponse		
responseStatus	OCSPResponseStatus with one of the values as specified in RFC6960.	
responseBytes	ResponseBytes	
ResponseBytes		
responseType	Contains the value for 1.3.6.1.5.5.7.48.1.1	
response	BasicOCSPResponse	
BasicOCSPResponse		
tbsResponseData	ResponseData	
signatureAlgorithm	ECDSA with SHA256	
signature	The signature value.	
certs	Contains the OCSP responder certificate.	
ResponseData		
version	Default 1 and therefore not set.	
responderID	ResponderID	
producedAt	GenerallizedTime with the time the response was produced.	
responses	Sequence of SingleResponse	
responseExtensions	Extensions	
ResponderID		KeyHash is supported.
KeyHash	SHA-1 hash of the OCSP responders public key.	
SingleResponse		
certID	CertID	
certStatus	• Always the value good for certificates issued by a CA managed by the QTSP. • Unknown for certificates managed by other CAs • Revoked, if the status was requested for a non-issued certificate by one of the CAs managed by the QTSP.	
thisUpdate	Indicates the time at which the status being indicated is known to be correct.	
nextUpdate	If included, the time at which updated revocation information will be made available.	
singleExtensions	One extension may be included:	

	• Nonce - Optional	
Nonce	If the nonce was included in the request it is returned in the response.	
ArchiveCutoff	The value shall be the issuing CAs notBefore date.	

2.8 TimeStamping Unit

Field	Value	Critical
Version	V3	
Serial number	Generated by CA software	
Issuer	Root certificate Issuer	
Validity		
notBefore	Certificate generation time	
notAfter	notBefore + 10 Years	
Subject		
CommonName	IN Groupe Denmark TimeStamping Unit I	
organizationName	IN Groupe Denmark A/S	
organizationIdentifier	NTRDK-30808460	
CountryName	DK	
SubjectPublicKeyInfo		
Algorithm Public Key	id-ecPublicKey with parameter namedCurve containing the elliptic curve identifier secp256r1. A public key on secp256r1	
authorityInfoAccess	One AccessDescription for id-ad-caIssuers containing the value https://pki.ingroupe.dk/repository/ca/root.crt	False
authorityKeyIdentifier	SHA-1 digest of value of the Root certificate Public Key	False
BasicConstraints	CA: False	True
crlDistributionPoints	url with https://pki.ingroupe.dk/repository/ca/root.crl	False
extKeyUsage	Timestamping identified by iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) kp(3) timestamping (8)	True
KeyUsage	bit 0 (digitalSignature)	True
subjectKeyIdentifier	SHA-1 digest of value of the Public Key	False
SignatureAlgorithm	ECDSA with SHA-512	

2.9 Time stamp token

Field	Value	Restrictions/Critical
TimeStampToken		
contentType	The object identifier has the value 1.2.840.113549.1.7.2 for SignedData.	
Content	SignedData	
SignedData		
Version	Version is 3.	
digestAlgorithms	Contains one AlgorithmIdentifier with value 2.16.840.1.101.3.4.2.1 for SHA-256.	
encapContentInfo	EncapsulatedContentInfo	
certificates	Contains the TSA certificate	
crls	This field is not used.	
signerInfos	Contains one SignerInfo	
EncapsulatedContentInfo		
eContentInfo	ObjectIdentifier with value 1.2.840.113549.1.9.16.1.4 for TSTInfo.	
eContent	TSTInfo	
TSTInfo		
version	Version is 1.	
policy	Contains the value 0.4.0.2023.1.1 for best-practices-ts-policy	
messageImprint	MessageImprint	
serialNumber	Contains a unique integer for each time stamp.	
genTime	Contains the UTC time for the generation of time stamp.	
accuracy	Accuracy	
ordering	This field is not present.	
nonce	Contains the value from the request.	
tsa	Contains a GeneralName with the Name from the TSU certificate subject field.	
MessageImprint		
hashAlgorithm	Contains the AlgorithmIdentifier with value 2.16.840.1.101.3.4.2.1 for SHA-256.	
hashedMessage	Contains the digest value as received in the request. It shall have length of 256/8 bytes.	
Accuracy		

seconds	1	
millis	N/A	
micros	N/A	
SignerInfo		
version	Version is 1.	
sid	SignerIdentifier	
digestAlgorithm	Contains the AlgorithmIdentifier with value 2.16.840.1.101.3.4.2.1 for SHA-256.	
signedAttrs	Contains three attributes: • ContentType identified by 1.2.840.113549.1.9.3 and value 1.2.840. 113549.1.9.16.1.4 for TSTInfo • MessageDigest identified by 1.2.840.113549.1.9.4 and value being the hash value of TSTInfo • SigningCertificateV2 identified by 1.2.840.113549.1.9.16.2.47	
signatureAlgorithm	ECDSA with SHA-256	
signature	Contains signature value	
unsignedAttrs	None	
SigningCertificateV2		
certs	SEQUENCE OF ESSCertIDv2	
policies	N/A	
ESSCertIDv2		
hashAlgorithm	We use the default SHA-256 and it is therefore not included.	
certHash	Hash value of TSU certificate	
issuerSerial	As received from the TSU certificate.	