ADVANCED CERTIFICATE PROFILES

IN Groupe DK A/S

Document information			
No. of pages : 8	Reference : N/A	Department : eID Development	Classification : Public
Valid from: 31/08/2025			Version: 1.0.0

Version history			
Version	Date	Author	Description of update Updated paragraphs
1.0	15/07/2025 00:00	KJAERSGAARD, Jan	Initial version
	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 TSP formats for advanced certificates, OCSP request and response.

The CA hierarchy and OCSP certificate is as follows:

- Root certificate
    - Advanced issuing CA
        - Advanced Subject certificates for natural person
        - Advanced OCSP Responder certificate

The Root certificate and revocation status information on certificates issued by the Root certificate are described the document Certificate Profiles which is available at the same location as this document.

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 TSP issues test certificates in production. For a description of these certificates, consult internal TSP 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

In the external test environment, the 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 Advanced 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 Advanced 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	

2.3 Advanced short term subject certificates for natural person

Field	**Value**	**Critical**
Version	V3	
Serial number	Generated by CA software	
Issuer		
CommonName	IN Groupe Denmark Advanced 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 from 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 from the identity provider. Must only be present if surname is present. Must not be present if pseudonym is present. UTF8String	
surname	As received from 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/advanced-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 Advanced CA certificate Public Key	False
BasicConstraints	CA: False	True
CertificatePolicies	NCP+ (itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus (2))	False
KeyUsage	bit 1 (nonRepudiation)	True
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	

2.4 Advanced CA OCSP Responder Certificate

Field	Value	Critical
Version	V3	
Serial number	Generated by CA software	
Issuer		
CommonName	IN Groupe Denmark Advanced 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	Advanced CA OCSP Responder	
organizationName	IN Groupe Denmark A/S	
organizationIdentifier	NTRDK-30808460	
CountryName	DK	

SubjectPublicKeyInfo		
Algorithm	id-ecPublicKey with parameter namedCurve containing the elliptic curve identifier secp256r1.	
Public Key	A public key on secp256r1	
authorityInfoAccess	One AccessDescription for id-ad-caIssuers containing the value https://pki.ingroupe.dk/repository/ca/advanced-ica-1.crt	False
authorityKeyIdentifier	SHA-1 digest of value of the Advanced 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	