

Qualified Electronic Seal CA Certificate Profiles IDnow Trust Services AB

Version 1.3

Table of Contents

Document Information	3
Change Log	3
1. Introduction	4
2. Certificate Body	5
2.1 CA Certificate	5
2.2 Seal Certificate.....	8
2.3 OCSP Certificate.....	11
3. CRL	13

Document Information

Version	1.3
Version date	29.01.2025
Confidentiality level	Public
Approved by	Representative of IDnow Trust Services Management
Owner of the document	System Administrator
Document name	Qualified Electronic Seal CA Certificate Profiles
Relevant for	External
Document OID	1.3.6.1.4.1.61867.2.1.4.1.4

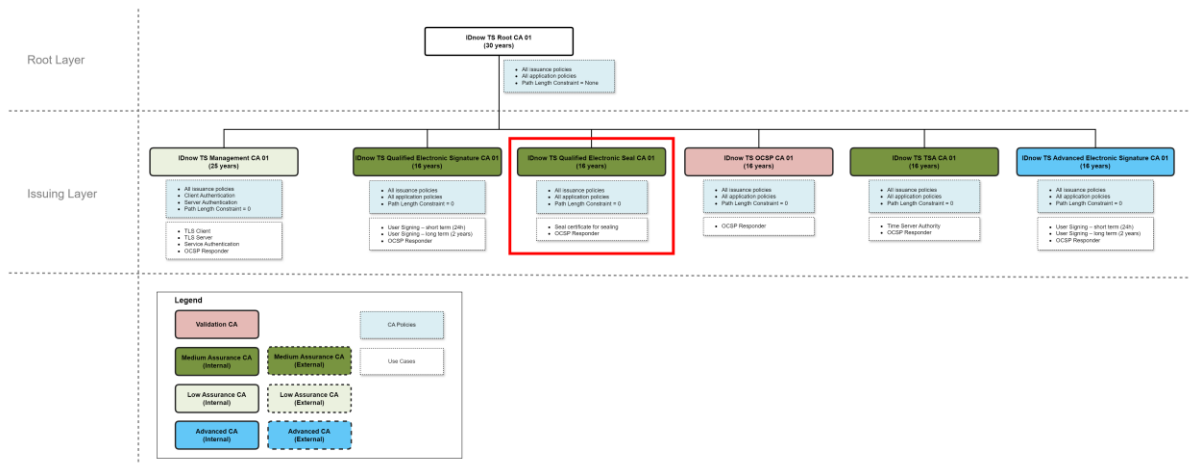
Change Log

Version	Version Date	Changes	Author
1.0	05.07.2024	Initial Version	Mateusz Kowalski
1.1	20.12.2024	Added OCSP Responder certificate information (chapter 2.3)	Mateusz Kowalski
1.2	23.01.2025	RSA key size range for the Seal Certificate extended from 4096-8192 to 3072-8192.	Mateusz Kowalski
1.3	29.01.2025	Added optional user notice qualifier in "Certificate Policies" section for the Seal Certificate.	Mateusz Kowalski

1. Introduction

The document describes the structure of digital certificates of IDnow Trust Services AB.

This document contains information about the IDnow Trust Services Qualified Electronic Seal CA [XX] certificate profiles and related end entity and CRL ones (where [XX] is 01,02,03...).



2. Certificate Body

2.1 CA Certificate

CA Certificate			
Field	Mandatory	Value	Description
Certificate Data			
Serial Number	Yes	<unique_serial_number>	Unique serial number of the certificate.
Version	Yes	3	Certificate format version.
Signature Algorithm	Yes	sha512RSA	Signature algorithm in accordance to RFC 5280.
Subject DN			
Common Name (CN)	Yes	IDnow TS Qualified Electronic Seal CA [XX]	Certificate authority name, where [XX] is 01,02,03...
Organization (O)	Yes	IDnow Trust Services AB	Organization name.
Organization Identifier (ORG_ID)	Yes	SE5594699489	Identification of the organization different from the organization name. Certificates may include one or more semantics identifiers as specified in clause 5.1.4 of ETSI EN 319 412-1.
Country (C)	Yes	SE	Country code: SE - Sweden (2 character ISO 3166 country code).
Issuer Name			
Common Name (CN)	Yes	IDnow TS Root CA [XX]	Certificate authority name, where [XX] is 01,02,03...
Organization (O)	Yes	IDnow Trust Services AB	Organization name.
Organization Identifier (ORG_ID)	Yes	SE5594699489	Identification of the organization different from the organization name. Certificates may include one or more semantics identifiers as specified in clause 5.1.4 of ETSI EN 319 412-1.

Country (C)	Yes	SE	Country code: SE - Sweden (2 character ISO 3166 country code).
Validity			
Validity Period	Yes	16 years	Validity period of certificate from issuance date.
Not Before	Yes	<issuance_date_and_time>	First date of certificate validity.
Not After	Yes	<issuance_date_and_time> + 16Y	Last date of certificate validity.
Public Key Info			
Algorithm	Yes	RSA (4096 Bits)	RSA algorithm in accordance with RFC 4055.
Public Key	Yes	<public_key>	Public Key.
Extensions			
Extension	Values and Limitations		Criticality
Key Usage	Certificate Signing (Off-line CRL Signing) CRL Signing (06)		Critical
Basic Constraints	Subject Type=CA Path Length Constraint=0		Critical
Subject Key Identifier	SHA-1 hash of the public key		Non-critical
Certificate Policies	Certificate Policy [1]: PolicyIdentifier: 1.3.6.1.4.1.61867.2.1.1.1.1 PKIX CPS Pointer Qualifier (1.3.6.1.5.5.7.2.1) =CPS Pointer: https://trust-services.io/repository/Practice_Statement_IDnowTrustServicesAB.pdf		Non-critical
Authority Key Identifier	SHA-1 hash of the public key		Non-critical
Authority Information Access	Authority Information Access [1]: Access Method: CA Issuers (1.3.6.1.5.5.7.48.2) Access Location: URI: http://ca.trust-services.io/rootca[XX].cer		Non-critical
CRL Distribution Points	CRL Distribution Point [1]: Distribution Point Name: Full Name:		Non-critical
			Yes

	URI: http://crl.trust-services.io/rootca[XX].crl		
--	--	--	--

2.2 Seal Certificate

Seal Certificate			
Field	Mandatory	Value	Description
Certificate Data			
Serial Number	Yes	<unique_serial_number>	Unique serial number of the certificate.
Version	Yes	3	Certificate format version.
Signature Algorithm	Yes	sha512RSA	Signature algorithm in accordance to RFC 5280.
Subject DN			
Common Name (CN)	Yes	<common_name>	End certificate common name.
Organization (O)	Yes	<organization>	Organization name.
Organization Identifier (ORG_ID)	Yes	<organization_identifier>	Identification of the organization different from the organization name. Certificates may include one or more semantics identifiers as specified in clause 5.1.4 of ETSI EN 319 412-1.
Country (C)	Yes	SE	Country code: SE - Sweden (2 character ISO 3166 country code).
serialNumber	No	<serialNumber>	Subject Unique Identifier.
Issuer Name			
Common Name (CN)	Yes	IDnow TS Qualified Electronic Seal CA [XX]	Certificate authority name, where [XX] is 01,02,03...
Organization (O)	Yes	IDnow Trust Services AB	Organization name.
Organization Identifier (ORG_ID)	Yes	SE5594699489	Identification of the organization different from the organization name. Certificates may include one or more semantics identifiers as specified in clause 5.1.4 of ETSI EN 319 412-1.

Country (C)	Yes	SE	Country code: SE - Sweden (2 character ISO 3166 country code).
Validity			
Validity Period	Yes	24 hours < VALIDITY < =3 years	Validity period of certificate from issuance date.
Not Before	Yes	<issuance_date_and_time>	First date of certificate validity.
Not After	Yes	<issuance_date_and_time> + VALIDITY	Last date of certificate validity.
Public Key Info			
Algorithm	Yes	RSA (3072 - 8192 Bits)	RSA algorithm in accordance with RFC 4055.
Public Key	Yes	<public_key>	Public Key.
Extensions			
Extension	Values and Limitations		Criticality
Key Usage	Non Repudiation		Critical
Basic Constraints	Subject Type=End Entity Path Length Constraint=None		Critical
Subject Key Identifier	SHA-1 hash of the public key		Non-critical
Certificate Policies	Certificate Policy [1]: PolicyIdentifier: 1.3.6.1.4.1.61867.2.1.1.1.1 PKIX CPS Pointer Qualifier (1.3.6.1.5.5.7.2.1) =CPS Pointer: https://trust-services.io/repository/Practice_Statement_IDnowTrustServicesAB.pdf PKIX CPS User Notice Qualifier (1.3.6.1.5.5.7.2.2) = <custom_user_notice_text> Certificate Policy [2]: PolicyIdentifier: 0.4.0.194112.1.3		Non-critical Yes* *User notice qualifier is optional and contains a personalized text requested by the customer.
Extensions	Validity Assured General [1]: ETSIValAssuredCertMod (0.4.0.194121.0.1.0)		Non-critical Yes
QC Statements	QC Statement [1]: PKIX QCSyntax-v2 OID: 1.3.6.1.5.5.7.11.2 QC Statement [2]: Semantics		Non-critical Yes

	<p>Identifier=0.4.0.194121.0.0.1 <i>OID: 1.3.6.1.5.5.7.11.2</i></p> <p>QC Statement [3]: Semantics Identifier=0.4.0.194121.1.2 <i>OID: 1.3.6.1.5.5.7.11.2</i></p> <p>QC Statement [4]: QC Compliance <i>OID: 0.4.0.1862.1.1</i></p> <p>QC Statement [5]: QC Secure Signature Creation Device <i>OID: 0.4.0.1862.1.4</i></p> <p>QC Statement [6]: QC Type=EtsiQctEseal (0.4.0.1862.1.6.2) <i>OID: 0.4.0.1862.1.6</i></p>		
Authority Key Identifier	SHA-1 hash of the public key	Non-critical	Yes
Authority Information Access	<p>Authority Information Access [1]: Access Method: CA Issuers (1.3.6.1.5.5.7.48.2) Access Location: URI: http://ca.trust-services.io/qesealca[XX].cer</p> <p>Authority Information Access [2]: Access Method: OCSP (1.3.6.1.5.5.7.48.1) Access Location: URI: http://ocsp.trust-services.io</p>	Non-critical	Yes
CRL Distribution Points	<p>CRL Distribution Point [1]: Distribution Point Name: Full Name: URI: http://crl.trust-services.io/qesealca[XX].crl</p>	Non-critical	Yes

2.3 OCSP Certificate

OCSP Certificate			
Field	Mandatory	Value	Description
Certificate Data			
Serial Number	Yes	<unique_serial_number>	Unique serial number of the certificate.
Version	Yes	3	Certificate format version.
Signature Algorithm	Yes	sha512RSA	Signature algorithm in accordance to RFC 5280.
Subject DN			
Common Name (CN)	Yes	IDnow TS QESeal OCSP	End certificate common name
Organization (O)	Yes	IDnow Trust Services AB	Organization name.
Organization Identifier (ORG_ID)	Yes	SE5594699489	Identification of the organization different from the organization name. Certificates may include one or more semantics identifiers as specified in clause 5.1.4 of ETSI EN 319 412-1.
Country (C)	Yes	SE	Country code: SE - Sweden (2 character ISO 3166 country code).
Issuer Name			
Common Name (CN)	Yes	IDnow TS Qualified Electronic Seal CA [XX]	Certificate authority name, where [XX] is 01,02,03...
Organization (O)	Yes	IDnow Trust Services AB	Organization name.
Organization Identifier (ORG_ID)	Yes	SE5594699489	Identification of the organization different from the organization name. Certificates may include one or more semantics identifiers as specified in clause 5.1.4 of ETSI EN 319 412-1.
Country (C)	Yes	SE	Country code: SE - Sweden (2 character ISO 3166 country code).

Validity			
Validity Period	Yes	1 year	Validity period of certificate from issuance date.
Not Before	Yes	<issuance_date_and_time>	First date of certificate validity.
Not After	Yes	<issuance_date_and_time> + 1Y	Last date of certificate validity.
Public Key Info			
Algorithm	Yes	RSA (3072 - 8192 Bits)	RSA algorithm in accordance with RFC 4055.
Public Key	Yes	<public_key>	Public Key.
Extensions			
Extension	Values and Limitations	Criticality	Mandatory
Key Usage	Digital Signature	Critical	Yes
Extended Key Usage	OCSP Signer	Non-critical	Yes
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	Critical	Yes
Subject Key Identifier	SHA-1 hash of the public key	Non-critical	Yes
OCSP No Check	id-pkix-ocsp-nocheck (1.3.6.1.5.5.7.48.1.5)	Non-critical	Yes
Certificate Policies	Certificate Policy [1]: PolicyIdentifier: 1.3.6.1.4.1.61867.2.1.1.1.1 PKIX CPS Pointer Qualifier (1.3.6.1.5.5.7.2.1) =CPS Pointer: https://trust-services.io/repository/Practice_Statement_IDnowTrustServicesAB.pdf	Non-critical	Yes
Authority Key Identifier	SHA-1 hash of the public key	Non-critical	Yes

3. CRL

CRL			
Field	Mandatory	Value	Description
CRL Data			
Delta CRL	Yes	No	
Immediate Issue	Yes	Yes	
CRL Build Frequency	Yes	1 / day	
Format	Yes	DER	
Signature Algorithm	Yes	sha512RSA	Signature algorithm in accordance to RFC 5280.
Issuer Name			
Common Name (CN)	Yes	IDnow Trust Services Qualified Electronic Seal CA [XX]	Certificate authority name, where [XX] is 01,02,03...
Organization (O)	Yes	IDnow Trust Services AB	Organization name.
Organization Identifier (ORG_ID)	Yes	SE5594699489	Identification of the organization different from the organization name. Certificates may include one or more semantics identifiers as specified in clause 5.1.4 of ETSI EN 319 412-1.
Country (C)	Yes	SE	Country code: SE - Sweden (2 character ISO 3166 country code).
Extensions			
Extension	Values and Limitations		Criticality
CRL Distribution Points	http://crl.trust-services.io/qesealca[XX].crl		Non-critical
			Mandatory
			Yes