IDnow Trust Services.

Qualified Electronic Signature CA Certificate Profiles

IDnow Trust Services AB

Version 1.0

Public

IDnow
Trust Services.

Table of Contents

IDnow Trust Services.

Document Information

Version	1.0
Version date	05.07.2024
Confidentiality level	Public
Approved by	Representative of IDnow Trust Services Management
Owner of the document	System Administrator
Document name	Qualified Electronic Signature CA Certificate Profiles
Relevant for	External
Document OID	1.3.6.1.4.1.61867.2.1.3.1.1

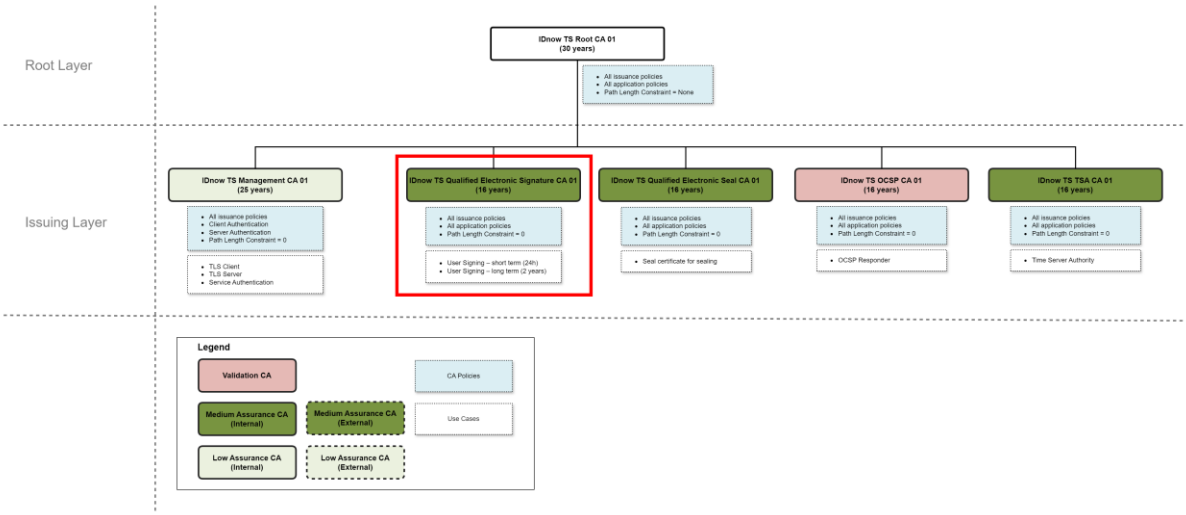
Change Log

Version	Version Date	Changes	Author
1.0	05.07.2024	Initial Version	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 Signature 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 Signature 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**	**Mandatory**
Key Usage	Certificate Signing (Off-line CRL Signing) CRL Signing (06)	Critical	Yes
Basic Constraints	Subject Type=CA Path Length Constraint=0	Critical	Yes
Subject Key Identifier	SHA-1 hash of the public key	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
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	Yes
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 Short-Term Certificate for Signing

Short-Term Certificate for Signing			
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.
Given Name (GN)	Yes	*<given_name>*	Subject first name.
Surname (SN)	Yes*	*<surname>*	Subject last name. *if person has only one name, only given name is required (it needs to match the identification document data). Valid for some countries.
Title (T)	No	*<title>*	Subject title.
Organization (O)	No	*<organization>*	Organization name.
Organization Unit (OU)	No	*<organization_unit>*	Organization Unit name.
E-mail (E)	No	*<email>*	E-mail address.
Street Address (S)	No	*<street>*	Street Address.
Postal Code (PC)	No	*<postal_code>*	Postal Code.
State or Province (S)	No	*<state_or_province>*	State or Province.
Locality (L)	No	*<locality>*	Locality.
Country (C)	Yes	SE	Country code: SE - Sweden (2 character ISO 3166 country code).
User ID (UID)	No	*<user_id>*	Subject User ID.
serialNumber	Yes	*<serialNumber>*	Subject Unique Identifier.
Issuer Name			
Common Name (CN)	Yes	IDnow TS Qualified Electronic Signature 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 hour / 12 hours / 24 hours	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> + 1H / + 12H / + 24H*	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	Non Repudiation	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
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 Certificate Policy [2]: PolicyIdentifier: 0.4.0.194112.1.2	Non-critical	Yes
Extensions	Validity Assured General [1]: ETSIValAssuredCertMod (0.4.0.194121.0.1.0)	Non-critical	Yes

	Validity Assured - Short Term [2]: id-etsi-ext-valassured-ST-certs (0.4.0.194121.2.1)		
QC Statements	QC Statement [1]: PKIX QCSyntax-v2 *OID: 1.3.6.1.5.5.7.11.2* QC Statement [2]: Semantics Identifier=0.4.0.194121.0.0.1 *OID: 1.3.6.1.5.5.7.11.2* QC Statement [3]: Semantics Identifier=0.4.0.194121.1.1 *OID: 1.3.6.1.5.5.7.11.2* QC Statement [4]: QC Compliance *OID: 0.4.0.1862.1.1* QC Statement [5]: QC Secure Signature Creation Device *OID: 0.4.0.1862.1.4* QC Statement [6]: QC Type=EtsiQctEsign (0.4.0.1862.1.6.1) *OID: 0.4.0.1862.1.6*	Non-critical	Yes
Authority Key Identifier	SHA-1 hash of the public key	Non-critical	Yes
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/qesignca[XX].cer Authority Information Access [2]: Access Method: OCSP (1.3.6.1.5.5.7.48.1) Access Location: URI: http://ocsp.trust-services.io	Non-critical	Yes
CRL Distribution Points	CRL Distribution Point [1]: Distribution Point Name: Full Name: URI: http://crl.trust-services.io/qesignca[XX].crl	Non-critical	Yes

2.3 Long-Term Certificate for Signing

Long-Term Certificate for Signing			
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.
Given Name (GN)	Yes	*<given_name>*	Subject first name.
Surname (SN)	Yes*	*<surname>*	Subject last name. *if person has only one name, only given name is required (it needs to match the identification document data). Valid for some countries.
Title (T)	No	*<title>*	Subject title.
Organization (O)	No	*<organization>*	Organization name.
Organization Unit (OU)	No	*<organization_unit>*	Organization Unit name.
E-mail (E)	No	*<email>*	E-mail address.
Street Address (S)	No	*<street>*	Street Address.
Postal Code (PC)	No	*<postal_code>*	Postal Code.
State or Province (S)	No	*<state_or_province>*	State or Province.
Locality (L)	No	*<locality>*	Locality.
Country (C)	Yes	SE	Country code: SE - Sweden (2 character ISO 3166 country code).
User ID (UID)	No	*<user_id>*	Subject User ID.
serialNumber	Yes	*<serialNumber>*	Subject Unique Identifier.

Issuer Name

Common Name (CN)	Yes	IDnow TS Qualified Electronic Signature CA [XX]	End certificate common 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**	**Mandatory**
Key Usage	Non Repudiation	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
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

	Certificate Policy [2]: PolicyIdentifier: 0.4.0.194112.1.2		
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 Identifier=0.4.0.194121.0.0.1 *OID: 1.3.6.1.5.5.7.11.2* QC Statement [3]: Semantics Identifier=0.4.0.194121.1.1 *OID: 1.3.6.1.5.5.7.11.2* QC Statement [4]: QC Compliance *OID: 0.4.0.1862.1.1* QC Statement [5]: QC Secure Signature Creation Device *OID: 0.4.0.1862.1.4* QC Statement [6]: QC Type=EtsiQctEsign (0.4.0.1862.1.6.1) *OID: 0.4.0.1862.1.6*	Non-critical	Yes
Authority Key Identifier	SHA-1 hash of the public key	Non-critical	Yes
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/qesignca[XX].cer Authority Information Access [2]: Access Method: OCSP (1.3.6.1.5.5.7.48.1) Access Location: URI: http://ocsp.trust-services.io	Non-critical	Yes
CRL Distribution Points	CRL Distribution Point [1]: Distribution Point Name: Full Name: URI: http://crl.trust-services.io/qesignca[XX].crl	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 TS Qualified Electronic Signature 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**	**Mandatory**
CRL Distribution Points	http://crl.trust-services.io/qesignca[XX].crl	Non-critical	Yes