IDnow Trust Services.

Advanced Electronic Signature CA Certificate Profiles

IDnow Trust Services AB

Version 1.2

Public

IDnow Trust Services.

Table of Contents

IDnow Trust Services.

Document Information

Version	1.2
Version date	12.05.2025
Confidentiality level	Public
Approved by	Representative of IDnow Trust Services Management
Owner of the document	System Administrator
Document name	Advanced Electronic Signature CA Certificate Profiles
Relevant for	External
Document OID	1.3.6.1.4.1.61867.2.3.12.3.3

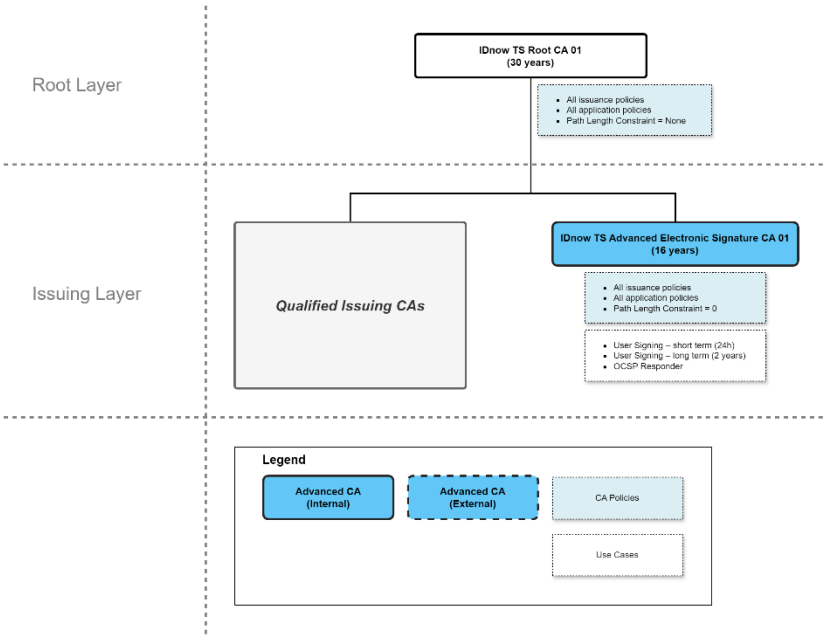
Change Log

Version	Version Date	Changes	Author
0.9	15.01.2025	Initial Version	Mateusz Kowalski
1.0	17.01.2025	Final review and adjustments.	Mateusz Kowalski
1.1	29.01.2025	Added the optional “Pseudonym” attribute into the Subject DN for the end certificate (chapter 2.2).	Mateusz Kowalski
1.2	12.05.2025	Added Short-Term End Certificate profile with ECDSA support. Introduced separation into RSA and ECDSA profiles	Wojciech Michalewski

1. Introduction

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

This document contains information about the IDnow Trust Services Advanced 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 Advanced 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: 1.3.6.1.4.1.61867.2.3.12.1.1 PKIX CPS Pointer Qualifier (1.3.6.1.5.5.7.2.1) =CPS Pointer: https://trust-services.io/repository/Practice_Statement_AES_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 AES Certificate for Signing

2.2.1 RSA

Short-Term AES Certificate for Signing (RSA)			
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-entity certificate common name.
Given Name (GN)	No	*<given_name>*	Subject first name.
Surname (SN)	No	*<surname>*	Subject last name.
Pseudonym (PSEUDONYM)	No*	*<pseudonym>*	Subject pseudonym. *it can be only set, if there is no Given Name AND Surname.
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)	No	SE	Country code: SE - Sweden (2 character ISO 3166 country code).
User ID (UID)	No	*<user_id>*	Subject User ID.
serialNumber	No	*<serialNumber>*	Subject Unique Identifier.
Issuer Name			
Common Name (CN)	Yes	IDnow TS Advanced 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 <= VALIDITY <= 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> + 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: 1.3.6.1.4.1.61867.2.3.12.1.1 PKIX CPS Pointer Qualifier (1.3.6.1.5.5.7.2.1) =CPS Pointer: https://trust-services.io/repository/Practice_Statement_AES_IDnowTrustServicesAB.pdf	Non-critical	Yes
Extensions	Validity Assured General [1]: ETSIValAssuredCertMod (0.4.0.194121.0.1.0) Validity Assured - Short Term [2]:	Non-critical	Yes

	id-etsi-ext-valassured-ST-certs (0.4.0.194121.2.1)		
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/aesignca[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/aesignca[XX].crl	Non-critical	Yes

2.2.2 ECDSA

Short-Term AES Certificate for Signing (ECDSA)			
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	sha512withECDSA	Signature algorithm in accordance to RFC 5280.
Subject DN			
Common Name (CN)	Yes	*<common_name>*	End-entity certificate common name.
Given Name (GN)	No	*<given_name>*	Subject first name.
Surname (SN)	No	*<surname>*	Subject last name.
Pseudonym (PSEUDONYM)	No*	*<pseudonym>*	Subject pseudonym. *it can be only set, if there is no Given Name AND Surname.
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)	No	SE	Country code: SE - Sweden (2 character ISO 3166 country code).
User ID (UID)	No	*<user_id>*	Subject User ID.
serialNumber	No	*<serialNumber>*	Subject Unique Identifier.
Issuer Name			
Common Name (CN)	Yes	IDnow TS Advanced 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 <= VALIDITY <= 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> + VALIDITY*	Last date of certificate validity.
Public Key Info			
Algorithm	Yes	ECDSA (P-256 / prime256v1 / secp256r1, P-384/secp384r1, P-521/secp521r1)	ECDSA algorithms in accordance with RFC 3279.
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: 1.3.6.1.4.1.61867.2.3.12.1.1 PKIX CPS Pointer Qualifier (1.3.6.1.5.5.7.2.1) =CPS Pointer: https://trust-services.io/repository/Practice_Statement_AES_IDnowTrustServicesAB.pdf	Non-critical	Yes
Extensions	Validity Assured General [1]: ETSIValAssuredCertMod (0.4.0.194121.0.1.0) Validity Assured - Short Term [2]: id-etsi-ext-valassured-ST-certs (0.4.0.194121.2.1)	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/aesignca[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/aesignca[XX].crl	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 AESign 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 Advanced 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	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
OSCP 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: 1.3.6.1.4.1.61867.2.3.12.1.1 PKIX CPS Pointer Qualifier (1.3.6.1.5.5.7.2.1) =CPS Pointer: https://trust-services.io/repository/Practice_Statement_AES_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 TS Advanced 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/aesignca[XX].crl		Non-critical	Yes