

# OCSP CA

# Certificate Profiles

# IDnow Trust Services AB

Version 1.0

# Table of Contents

|                            |    |
|----------------------------|----|
| Document Information ..... | 3  |
| Change Log .....           | 3  |
| 1. Introduction .....      | 4  |
| 2. Certificate Body .....  | 5  |
| 2.1 CA Certificate .....   | 5  |
| 2.2 OCSP Certificate ..... | 8  |
| 3. CRL .....               | 10 |

## 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         | OCSP CA Certificate Profiles                      |
| Relevant for          | External  |
| Document OID          | 1.3.6.1.4.1.61867.2.1.6.1.1                       |

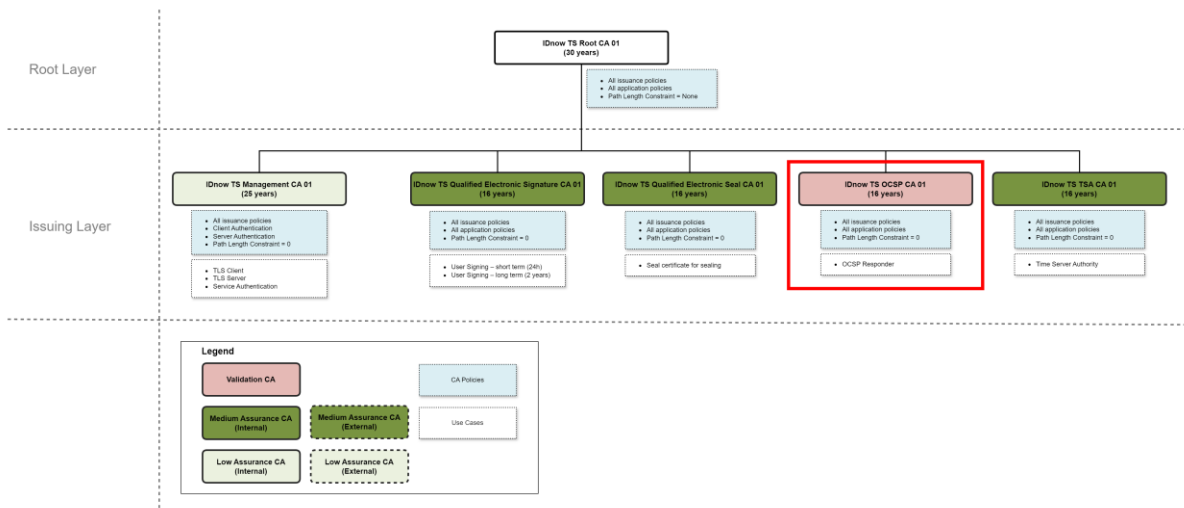
## Change Log

| 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 OCSP 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  |
| <b>Certificate Data</b>          |           |                         |  |
| 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.   |
| <b>Subject DN</b>                |           |                         |  |
| Common Name (CN)                 | Yes       | IDnow TS OCSP 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).   |
| <b>Issuer Name</b>               |           |                         |  |
| 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). |
| <b>Validity</b>              |   |                                |  |
| 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.                             |
| <b>Public Key Info</b>       |   |                                |  |
| Algorithm                    | Yes   | RSA (4096 Bits)                | RSA algorithm in accordance with RFC 4055.                     |
| Public Key                   | Yes   | <public_key>                   | Public Key.  |
| <b>Extensions</b>            |   |                                |  |
| <b>Extension</b>             | <b>Values and Limitations</b>   |                                | <b>Criticality</b>   |
| Key Usage                    | Certificate Signing (Off-line CRL Signing)<br>CRL Signing (06)  |                                | Critical   |
| Basic Constraints            | Subject Type=CA<br>Path Length Constraint=0   |                                | Critical   |
| Subject Key Identifier       | SHA-1 hash of the public key  |                                | Non-critical   |
| Certificate Policies         | Certificate Policy [1]:<br>PolicyIdentifier:<br>1.3.6.1.4.1.61867.2.1.1.1.1<br>PKIX CPS Pointer Qualifier<br>(1.3.6.1.5.5.7.2.1)<br>=CPS Pointer: <a href="https://trust-services.io/repository/Practice_Statement_IDnowTrustServicesAB.pdf">https://trust-services.io/repository/Practice_Statement_IDnowTrustServicesAB.pdf</a> |                                | Non-critical   |
| Authority Key Identifier     | SHA-1 hash of the public key  |                                | Non-critical   |
| Authority Information Access | Authority Information Access [1]:<br>Access Method: CA Issuers<br>(1.3.6.1.5.5.7.48.2)<br>Access Location:<br>URI: <a href="http://ca.trust-services.io/rootca[XX].cer">http://ca.trust-services.io/rootca[XX].cer</a>  |                                | Non-critical   |
| CRL Distribution Points      | CRL Distribution Point [1]:<br>Distribution Point Name:<br>Full Name:   |                                | Non-critical   |
|                              |   |                                | Yes  |

|  |  |  |  |
|--|--|--|--|
|  | URI: <a href="http://crl.trust-services.io/rootca[XX].crl">http://crl.trust-services.io/rootca[XX].crl</a> |  |  |
|--|--|--|--|

## 2.2 OCSP Certificate

| OCSP Certificate                 |           |                         |  |
|----------------------------------|-----------|-------------------------|--|
| Field                            | Mandatory | Value                   | Description  |
| <b>Certificate Data</b>          |           |                         |  |
| 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.   |
| <b>Subject DN</b>                |           |                         |  |
| Common Name (CN)                 | Yes       | IDnow TS 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).   |
| <b>Issuer Name</b>               |           |                         |  |
| Common Name (CN)                 | Yes       | IDnow TS OCSP 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><br>+ 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<br>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<br>(1.3.6.1.5.5.7.48.1.5)  | Non-critical                     | Yes  |
| Certificate Policies     | Certificate Policy [1]:<br>PolicyIdentifier:<br>1.3.6.1.4.1.61867.2.1.1.1.1<br>PKIX CPS Pointer Qualifier<br>(1.3.6.1.5.5.7.2.1)<br>=CPS Pointer: <a href="https://trust-services.io/repository/Practice_Statement_IDnowTrustServicesAB.pdf">https://trust-services.io/repository/Practice_Statement_IDnowTrustServicesAB.pdf</a> | Non-critical                     | Yes  |
| Authority Key Identifier | SHA-1 hash of the public key  | Non-critical                     | Yes  |

## 3. CRL

| CRL                              |   |                         |  |           |
|----------------------------------|---|-------------------------|--|-----------|
| Field                            | Mandatory                                   | Value                   | Description  |           |
| <b>CRL Data</b>                  |   |                         |  |           |
| Delta CRL                        | Yes   | No                      |  |           |
| Immediate Issue                  | Yes   | Yes                     |  |           |
| CRL Build Frequency              | Yes   | 1 / year                |  |           |
| Format                           | Yes   | DER                     |  |           |
| Signature Algorithm              | Yes   | sha512RSA               | Signature algorithm in accordance to RFC 5280.   |           |
| <b>Issuer Name</b>               |   |                         |  |           |
| Common Name (CN)                 | Yes   | IDnow TS OCSP 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).   |           |
| <b>Extensions</b>                |   |                         |  |           |
| Extension                        | Values and Limitations                      |                         | Criticality  | Mandatory |
| CRL Distribution Points          | http://crl.trust-services.io/ocspca[XX].crl |                         | Non-critical   | Yes       |