IDnow Trust Services.

Qualified Trust Service Policy
IDnow Trust Services AB
version 1.0

Qualified Certificate for Electronic Signatures and Seals

Management of remote electronic signature and seal creation devices

Table of Contents

Document Information

Version	1.0
Version date	03.07.2024
Confidentiality level	Public
Approved by	Representative of IDnow Trust Services Management
Owner of the document	Chief Security Officer
Document name	Qualified Trust Service Policy IDnow Trust Services AB
Relevant for	External
Document OID	1.3.6.1.4.1.61867.2.1.2.1.1

Change log

Version	Version Date	Changes	Author
1.0	03.07.2024	Version 1.0	Adam Ptasiewicz

1. Introduction

1.1 Scope

The Qualified Trust Service Policy for Qualified Certificates for Electronic Signatures and Seals and Time Stamping, together with the Practice Statement of IDnow Trust Services AB, fulfills the role of the Certificate Policy for the following classes of certificates and type of services:

1. the issuance of **public key qualified certificates for electronic signatures and seals**, including registration of **subscribers and subjects**, certification of public keys and rekey,
2. the **revocation** of certificates and online status information
3. the issuance of **electronic timestamp certificates** and **OCSP certificates**.
4. creation of remote electronic signatures and seals with the use of a remote Qualified Signature Creation Device (RQSCD) on behalf of the Subject (signatory)
5. processing certificate subjects' data for certificate issuance.

Throughout this document:

- the use of the term “Policy” or “Trust Service Policy” refers to the present document,
- the use of the term “Practice Statement” refers to the Practice Statement of IDnow Trust Services AB.

The present document supplements the Practice Statement with the following elements in particular:

- description of the certificate life cycle
- certificate, CRL and OCSP profiles.

The structure and contents of the Policy are in accordance with the recommendation of RFC 3647 Certificate Policy and Practice Statement Framework. The current document follows the standards specified in the Practice Statement.

1.2 Overview of trust services

The purpose of the Trust Service Policy is to address the international community's requirements to provide trust and confidence in electronic transactions, as outlined in Regulation (EU) No. 910/2014.

This document supplements the Practice Statement with requirements for individual components defined in the Practice Statement and implementing the trust service. These components have been listed in the Practice Statement: Registration Authority, Certificate generation service, Remote QSCD provision service, TSA Service, and Central Component.

1.3 Document Name and Identification

The full name of this document is the Qualified Trust Service Policy for Qualified Certificates for Electronic Signatures and Seals and Time Stamping. This document is available in an electronic version at:

- ➔ https://trust-services.io/repository/
- ➔ OID 1.3.6.1.4.1.61867.2.1.2.1.1

The present document defines the certificate policy for the issuance of:

- qualified certificates for qualified electronic signatures,
- qualified certificates for qualified electronic seals,
- certificates for electronic timestamp services,
- certificates for status services.

The following table illustrates compliance with policies defined in ETSI EN 319 411-1 [REF. 6], ETSI EN 319 411-2 [REF. 7] ETSI TS 119 431-1 [REF. 13] standards.

Policy	Identifier	Compliance
NCP	itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncp (1)	All certificates
NCP+:	itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus (2)	All certificates
QCP-n	Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural (0)	Qualified certificates for electronic signatures (including certificates for qualified signatures)
QCP-l	itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal (1)	Qualified certificates for electronic seals (including certificates for qualified seals)

QCP-n-qscd	Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2	Certificates for qualified signatures
QCP-l-qscd	itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal-qscd (3)	Certificates for qualified seals
BTSP	itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy (1)	Certificates for qualified time stamps
NSCP	itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops(1) policy-identifiers(1) normalized (2)	Server Signing Service Component
EUSCP	itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops (1) policy-identifiers(1) eu-remote-qscd (3)	EU Server Signing Service Component

1.4 PKI Participants

The scope related to this item is addressed in the Practice Statement.

1.4.1 Certification authority

Certification Authorities (CAs) are operated by the trust service provider (TSP) that issue certificates and revocation lists.

Subsequent root certification authority of IDnow Trust Services AB (Root CAs) is operational:

- IDnow TS Root CA 01,

The list of Root CAs can be extended with any new version of this document.

There are the following types of subordinate CAs operated by IDnow Trust Services AB:

- IDnow TS Qualified Electronic Signature CA 01
- IDnow TS Qualified Electronic Seal CA 01

- IDnow TS OCSP CA 01
- IDnow TS TSA CA 01

The Trust Service Policy defines the list of subordinate Certificate authorities and their certificate profiles.

IDnow TS Management CA 01 is used only for management and infrastructure certificates. No qualified certificates are issued under this CA. Practices for IDnow TS Management CA 01 are defined in internal procedures and are hence out of scope in this document.

The list above can be extended in any new version of this document.

1.4.2 Registration Authorities

The scope related to this item is addressed in the Practice Statement.

1.4.3 Subjects and subscribers

The scope related to this item is addressed in the Practice Statement.

1.4.4 Relying partners

The scope related to this item is addressed in the Practice Statement.

1.4.5 Server Signing Application Service Component

IDnow Trust Services AB provides a service component employing a server signing application to create an electronic signature or seal value on behalf of a Subject.

1.4.6 Other participants

The scope related to this item is addressed in the Practice Statement.

1.5 Certificate Usage

IDnow Trust Services AB issues certificates for electronic signatures and electronic seals. Qualified certificates are issued to the subjects who accepted the terms of the provision of trust services by IDnow Trust Services AB as defined in the Policy and the Practice

Statement. At the time of issuance of the certificate, it becomes associated with a pair of public and private keys. These keys are generated and managed by IDnow Trust Services AB.

IDnow Trust Services AB Root CA issues certificates for operational CAs as indicated above.

Every qualified certificate issued by the IDnow Trust Services AB operational CA indicates that it is a qualified certificate, and the associated private key is held in the Qualified Signature Creation Device maintained on behalf of the subject.

There are the following types of qualified certificates and their applicability:

1. **Personal**

   Qualified certificates for qualified electronic signatures - certificate contains at least: name of the country, name of the subject and serial number of the certificate.

2. **Personal with additional data**

   Qualified certificate for qualified electronic signatures - certificates are used by individuals who are associated with a legal person; the certificate contains at least the name of the country, name of the subject, name of the legal person and serial number of the certificate.

3. **Legal person**

   Qualified certificates for qualified electronic seals - certificates are issued to legal persons. A qualified certificate for an electronic seal includes at least the name of the country, the name of the legal entity (subject), its registration or tax number, common name and serial number of the certificate.

1.5.1 Appropriate certificate use

Personal certificate use is restricted to the creation of qualified electronic signatures by the natural person and its validation by relying parties.

Personal certificates with additional data use are restricted to the creation of qualified electronic signatures by the natural person associated with the legal person and their validation by relying parties.

The use of legal person certificates is restricted to the creation of qualified electronic seals by the legal person and their validation by relying parties.

1.5.2 Prohibited certificate use

Qualified certificates should not be used in a manner incompatible with their declared purpose and field of application.

Certificates do not guarantee that the subject is trustworthy, operating a reputable business, or that the equipment into which the certificate has been installed is free from defects, malware, or viruses.

Certificates issued under this Policy may not be used where prohibited by the law.

1.6 Policy Administration

1.6.1 Organization responsible for administrating the document

This Policy is administered by IDnow Trust Services AB:

IDnow Trust Services AB
Box 16285
10325 Stockholm
Sweden

1.6.2 Contact

Email: info@trust-services.io.

1.6.3 Entities determining the validity of the principles contained in the document

The IDnow Trust Services AB is responsible for evaluating the timeliness and usefulness of Trust Service Policy and other documents, as well as the compatibility between these documents. All inquiries and comments concerning the contents of these documents should be directed to the address in this chapter 1.6.2.

1.6.4 Approval procedures

This Trust Service Policy is in effect until the release of the next valid version.

The affected parties may submit comments on intended changes within 14 working days of their announcement. After this deadline, if there are no significant reservations about the substantive content of the proposed changes, the new version of the Policy becomes valid with the validity date indicated in it. The prior version will be archived.

The decision to approve the new version of the Trust Service Policy is taken by the IDnow Trust Services AB Board.

The approved document is published and communicated to:

- employees,
- relying parties,
- subjects and subscribers,
- other parties listed in supplier registry 1.4.5.

1.7 Definitions and Acronyms

Definitions and abbreviations used in this document are at the end of it.

2. Publication and Repository Responsibilities

2.1 Repository

IDnow Trust Services AB provides a public document repository (details in chapter 2.2), which is available 24/7 and published at: [http://idnow.trust-services.io/en/repository/]

The repository is intended for the following entities: subjects, subscribers, and relying parties.

2.2 Information published by IDnow Trust Services AB

The public registry of IDnow Trust Services AB is a repository of current and previous electronic document versions.

The information published in the repository includes the following documents:

- Practice Statement – current and previous version
- Trust Service Provider Policy - current and previous version
- Time Stamping Authority Policy
- General Terms & Conditions for qualified trust services of IDnow Trust Services AB
- General Data Protection Regulation Policy
- Certificate Profiles
- CA Certificates
- Certificates Revocation Lists (CRLs)
- Additional information, such as notifications about incidents

IDnow Trust Services AB does not publish Subject Certificates.

2.3 Frequency of publication

Publications are issued with the following frequency:

- Trust Service Policy and Practice Statement - see chapter 9.12

- Trust services providers certificates of all authorities providing trust services functioning within IDnow Trust Services AB – upon every issuance of new certificates,
- Certificate Revocation List (CRL) – according to specific Trust Service Policy
- Supplementary information – upon every updating of it

2.4 Access to publication

IDnow Trust Services AB has implemented logical and physical mechanisms preventing unauthorized creation, removal and modification of the information published in the repository.

3. Identification and Authentication

3.1 Naming

3.1.1 Type of names

The certificates generally contain information regarding the issuer and the subject. In line with the [X.509] standard, these names are given as distinguished names.

3.1.2 Meaningful names required

The subject's distinguished name is unambiguous within all trust services provided by the IDnow Trust Services AB.

All the values in the subject information section of a Certificate are meaningful.

Section 3.1.4 defines the mandatory certificate data for unambiguous subject identification.

The use of pseudonyms of the subject is not allowed in certificates.

3.1.3 User anonymity

The use of pseudonyms of the subject is not allowed in certificates.

3.1.4 Rules for different names interpretation

The interpretation of names of fields included in certificates complies with ETSI TS 119 412-1 [REF.23] and ETSI EN 319 412 (Part: 2,3,4,5) [REF.:9,10,25,11]. The attributes of the distinguished name (DN components) of certificates are interpreted as follows:

DN component	Interpretation
givenName	*Given name(s)* of the natural person - According to the proof used for identification
sn (surname)	*Surname* of the natural person - According to the proof used for identification

Cn (common name)	*Common name:* The following variants are used: - Natural persons without a pseudonym: “Surname, name used”. - Legal entities: Official name of the legal person (company, public authority, association, etc.), if necessary, reduced to a meaningful name if the maximum number of 64 characters is exceeded.
serialNumber (serial number)	*Serial number*: number to ensure unambiguity of the name (typically the application number). Assigned to the natural or legal person Other product-specific uses of the field are possible.
O (organization name)	Official name of the subscriber or name of the legal person (including legal form) to which the subject belongs or to which he or she is otherwise affiliated (company, public authority, association, etc.) according to the proof of existence; if necessary, reduced to a meaningful name if the maximum number of 64 characters is exceeded.
Ou (organization unit)	*legal person unit* (department, division or other unit) of the organization
OrgID (organization identifier)	*Unambiguous legal person number of the legal person*. tax identification number, register number in the national commercial register or local identifier, recognizable on the European Union’s level according to point 5.1.4 ETSI TS 119 412-1 [REF.23]
c (country)	The notation of the country to be stated corresponds to [ISO 3166] and is set up as follows: • If an legal person O is listed in the DistinguishedName, the legal person 's place of business in the register determines the entry in the certificate. • If no legal person O is entered, the country is listed that was transmitted as the nationality of the subscriber during the identification process.
E-mail	The e-mail address of the applicant (optional)
Street	Postal address Street
Locality	Postal address City
State	Postal address (Federal) state
PostalCode	Postal address Postal code

Qualified certificates for natural persons include, as a minimum, the subject DN components: “cn”, “c”, “serialNumber”, “givenName” and “sn”.

Qualified certificates for legal entities include, as a minimum, the subject DN components: “cn”, “c”, “organizationName” and “organizationIdentifier”. It is not necessary to use all the DN components enumerated in the table above. Further components can be added. Additional DN components must comply with RFC 5280[REF.22], RFC 6818 [REF.24]and ETSI EN 319 412 [REF.8].

3.1.5 Uniqueness of the names

IDnow Trust Services AB ensures that subject’s distinguished names are unique by adding a requisite that guarantees such uniqueness.

IDnow Trust Services AB does not issue certificates with an identical pair of Common Name (cn) and Serial Number for more than one individual natural person.

IDnow Trust Services AB does not issue certificates, with an identical pair Common Name (cn) and organization identifier, for different legal persons.

3.1.6 Names verifications and disputes in this regard

Subjects and subscribers may not request certificates with content that infringes a third party's intellectual property rights. IDnow Trust Services AB does not require that a subject’s or subscriber’s right to use a trademark be verified. IDnow Trust Services AB reserves the right to revoke any certificate involved in a dispute.

3.2 Initial Identity Validation

The scope related to this item is addressed in the Practice Statement (clause 3.2).

3.2.1 Method to prove possession of key

The scope related to this item is addressed in the Practice Statement (clause 3.2.1).

3.2.2 Authentication of a legal person

The RA is responsible for the Legal Person authentication and verification process.

The official signatory for the legal person (organization) must use a qualified signature to sign the seal application. RA validates the signature and application.

Alternatively, the RA can validate a paper application with a wet signature and a physical identity document.

The legal person must provide an official register excerpt, and the official signatory must be listed on that excerpt. The Registration Officer will manually verify the application and the identification documents.

3.2.3 Authentication of Natural person

The initial identity validation is an outsourced service (Registration Authority) provisioned by IDnow GmbH, which is certified against ETSI EN 319 411-1/2 [REF.6/7] and ETSI TS 119 461 [REF.19] standards.

Registration Authority provides identity validation of natural persons only remotely. For this purpose, the following methods are offered:

- Unattended remote identity proofing
- Attended remote identity proofing
- Identity proofing and authentication previously carried out by the Registration Authority.

Each of these methods ensures that only the data needed to issue a certificate is collected and validated.

All evidence and attestations are collected by the Registration Authority in line with the following statements.

- The subject's identity is verified at the time of registration.
- Verification is done by appropriate means, confirmed in an agreement with the RA.
- Evidence is collected for the following data points:
    - full name (including surname and given names).
    - date and place of birth, reference to a nationally recognized identity document, or other attributes which can be used to, as far as possible, distinguish the person from others with the same name.
- All the information necessary to verify the subject's identity, specific attributes of the subject, and any limitations on its validity are recorded.
- Processing only of data required to capture the evidence of an identity that is sufficient to satisfy the requirements of the intended use of the certificate.

- RA provides evidence of following applicable data protection legislation within its registration process.

Registration Authority records and preserves identity data of all registered subjects.

If the initial identity verification is based on data validated by a financial institution regulated under the European AML Directive, it can only be used to create a short-term signature associated with that financial institution.

Authentication means may be issued to identified persons, allowing the issuance of a certificate without the need to re-confirm their identity. The RA manages authentication means.

3.2.4 Authentication of a natural person representing legal entity

Trust Service Policy specifies detailed provisions for the authentication of natural persons representing legal entities.

All provisions defined in 3.2.3 are applied accordingly.

- The evidence is collected for the following data:
  - full name of the subject.
  - date and place of birth, reference to a nationally recognized identity document, or other attributes of the subscriber which can be used to, as far as possible, distinguish the person from others with the same name;
  - full name and legal status of the associated legal person or other organizational entity (e.g. the subscriber);
  - any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity identified in association with the legal person, consistent with national or other applicable identification practices;
  - affiliation of the natural person to the legal person consistent with national or other applicable identification practices;
  - confirmation by the legal person and the natural person that the subject attributes also identify such organization.

3.2.5 Unconfirmed information

The certificate does not contain any unconfirmed information.

3.2.6 Criteria of interoperability

The scope related to this item is addressed in the Practice Statement.

3.3 Identification and Authentication for Re-key Requests

The scope related to this item is addressed in the Practice Statement.

3.4 Identification and Authentication for Revocation Requests

A subscriber or subject may request a revocation of the certificate. The request must be performed in person and by the subscriber or subject himself. For such a case, the subscriber or subject has to request the revocation using:

- Revocation request form at https://www.trust-services.io/
- Revocation request send by email to support@trust-services.io

Upon requesting the revocation, the subscriber or subject will get an email receipt confirming the reception of the request. The revocation request form is available from 00:00 CET to 24:00 CET, seven days a week.

If the certificate is still active IDnow Trust Services AB will authenticate the person submitting the revocation request using an Identity Proofing Service or assigned authentication means to ensure the person requesting the revocation is the subscriber or subject if necessary. The instructions for performing the remote identification proofing are sent to the subscriber or subject by email.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

The electronic signature certificate application is compiled in the Signature Application service, which serves as an interface with an external client service defined as Channel, and Identification and Authentication Services. The electronic seal certificate application is created in electronic form as part of the contract agreements.

The Certificate Applications are send to the Registration Authority.

4.1.1 Who can submit a certificate application

The Subscriber or Subject aiming to obtain a certificate interacts with Channel services, Signature Application and Registration Services. As part of this interaction, a certificate application is submitted in accordance with the conditions described in subsequent chapters of the Policy.

4.1.2 Enrollment process and responsibilities

Enrolment for electronic signature certificate starts when the signature request is sent by the Channel, after the content of all policies, terms and conditions are reviewed and accepted by the subscriber. All operations related to enrolment process are performed by the Signature Application. Depending on the use case, the Signature Application initiates the identification or authentication process of the entity, described in chapter 4.2.1.

Enrolment for electronic seal certificate starts with submision of the application in electronic form for certificate by the subscriber. The application must be signed with means of qualified electronic signature by the subscriber who is representative of the legal person.

All data collected during the enrolment process, is transferred through an encrypted communication channel to the Central Component, that is responsible for storage of enrolment and identification information, as described in chapter 4.2.1.

The allocation of the Signature Application responsibilities is regulated by the agreement with IDnow Trust Services AB.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Identification and authentication of the Subject need to be done before the certificate issuance. It can be done based on:

- an identification performed by the identity proofing provider, if it is a certificate request initiated by the Subject for the first time or after a change of personal related data,
- authentication means issued to registered users of IDnow Trust Services AB.

If the Subject verification is positive, the certificate issuance process begins.

Detailed initial identity validation is described in clause 3.2 of this Policy.

All registered users of IDnow Trust Services AB are authenticated with multi-factor authentication methods.

All secret information exchanged in verification protocols is encrypted.

4.2.2 Approval or Rejection of Certificate Applications

The final acceptance or rejection of a Subscriber application is determined by the Central Component. Based on initial verification by the RA the Subscriber applications will be approved if they meet the requirements in this Policy and Practice Statement.

IDnow Trust Services AB rejects applications for certificates where the validation of all items cannot be successfully completed. This also includes any discrepancies between the data in the application and the data stored in the IDnow Trust Services AB user registry.

If any additional data is required, IDnow Trust Services AB conducts the initial validation process according to this Policy (clause 3.2) to extend the user account with these data.

4.2.3 Time to Process Certificate Applications

IDnow Trust Services AB makes every effort to ensure that upon receiving the application for a certificate, the CA examines the application and issues a certificate as soon as possible.

4.3 Certificate Issuance

4.3.1 CA actions during certificate issuance

After verifying that Subject's identification data in the certificate request matches the identification data stored in the users' registry of IDnow Trust Services AB, the IDnow Trust Services AB certificate generation service automatically issues the corresponding certificate.

4.3.2 Notification to Subjects and Subscribers by the CA of issuance of a certificate

Subject and Subscriber, whose data is included in the certificate application, are informed about certificate issuance according to methods indicated in terms and conditions.

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

Subject is obligated to verify the accuracy of the data included in the issued certificate. If any irregularities are detected, the Subject must report immediately to the point of contact stated in clause 1.6.2 of this Policy.

4.4.2 Publication of the certificate by the CA

IDnow Trust Services AB does not publish Subject Certificates. Certificate validity can be checked through the OCSP service.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber and/or Subject private key and Certificate usage

Subscribers and Subjects are entitled to use their own private keys exclusively for those applications which are in conformity with the types of use stated in the certificate. They are required in such cases to use the Certificate and Private Key lawfully and in accordance with:

- the Policy and the Practice Statement
- the Terms and Conditions

The Subscriber can use a signing key pair for hash signing with the SHA512 hashing algorithm or another algorithm ensuring a higher level of security.

IDnow Trust Services AB hosts, secures and manages certificates and corresponding private keys in a conformant HSM/RQSCD.

The remote signature system technically excludes the signature with expired certificates. Subscriber can use the signing key pair for signing using various signature formats.

4.5.2 Relying party public key and certificate usage

The relying party is required to use the certificate and public key lawfully and in accordance with:

- the Policy and the Practice Statement.
- the Terms and Conditions.

The certificates issued by IDnow Trust Services AB can be used by all relying parties. However, they can only be relied upon if:

1. the certificates are used in line with the types of use shown within (key use, extended key use, restricting extensions, if applicable).
2. all other precautionary measures determined in agreements or otherwise were taken (see documents in the IDnow Trust Services AB repository) and if any restrictions in the certificate as well as any application-specific measures were taken by the relying party and found to be compatible.
3. the verification of the certificate-chain is carried out successfully and completely up to the trusted root certificate. This is done, to validate the trust status of the PKI (e.g. EU Trusted List according to eIDAS Regulation (EU) No 910/2014).
4. it is verified that the certificate is not listed as revoked on the associated Certificate Revocation List (CRL); alternatively the status of the certificate is checked positively

via the OCSP (Online Certificate Status Protocol) (i.e. a third party can determine via the OCSP status query that IDnow Trust Services AB has issued the requested certificate). If the check mechanism from number 3 did not work, the existence and validity of a certificate can be checked via the Online Certificate Status Protocol (OCSP).

4.6 Certificate Renewal

Renewal of Certificates is not allowed. To maintain the validity of the certificate, the use of the Certificate Re-key mechanism is supported - see clause 4.7

4.6.1 Circumstance for certificate renewal

No stipulation.

4.6.2 Who may request renewal

No stipulation.

4.6.3 Processing certificate renewal requests

No stipulation.

4.6.4 Notification of new certificate issuance to Subscriber

No stipulation.

4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6 Publication of the renewal certificate by the CA

No stipulation.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate Re-key

Key update takes place when the Subscriber (for an already registered Subject) requests the generation of a new key pair and the issuance of a new certificate confirming the association of their identity with the newly generated public key. The update of the keys always relates to the specific certificate indicated in the request; for this reason, the new certificate has identical content to the associated certificate. The only difference of a new public key is a new serial number, a new certificate validity period and a new electronic certificate from the CA.

4.7.1 Circumstance for certificate re-key

Updating of the Subscriber's certificate keys takes place when the Subscriber requests updating of the keys of the certificate he holds. The objective of an update request is to generate a new key pair and the issuance of a certificate for the same subject.

If one of the following events occurs during the validity period of a qualified certificate:

- expiration of the validity of a qualified device for creating a qualified electronic signature and seal,
- expiration of the validity of cryptographic algorithms and other parameters related to them, operated by a qualified device for creating a qualified electronic signature and seal.
- change Subject data (e.g., last name after marriage) or
- expiration of the ID document.

Then IDnow Trust Services AB may start the process of issuing a qualified certificate during its validity for a new qualified signature and seal creation device that meets the security requirements.

Subscriber must complete the re-keying process for a new qualified signature and seal creation device in accordance with the instructions of IDnow Trust Services AB.

The keys may be updated by the Subscriber periodically, based on the parameters of the indicated certificate already in possession of the Subscriber. As a result of updating the keys, a new certificate is created with a new public key, certificate serial number and a different validity period.

4.7.2 Who may request certification of a new public key

Keys are updated only after the Subscriber's request and therefore must be preceded by the submission of an appropriate application.

4.7.3 Processing certificate re-keying requests

A request for a key update submitted by a Subscriber may concern the following:

- valid certificate,
- case when the Subscriber has a private key associated with the above-mentioned certificate.

Key certification may also apply to situations where:

- the Subscriber does not have a current and valid private key for signatures or seals,
- the Subscriber wants to obtain an additional certificate of a different type, but only as part of the certification policy in accordance with which he/she had issued at least one certificate (this certificate does not have to be valid).

Certificates of trust service providers of the IDnow Trust Services AB Certification Authority may also be subject to the Certification and Key Update Procedure. All Subscribers of the Certification Authority are informed about the occurrence of such an event.

IDnow Trust Services AB sends the Subscriber information about the upcoming expiry date of the certificate at least 3 days before the end of its validity.

4.7.4 Notification of new certificate issuance to Subscriber

The Subscriber and the authorized Subject whose data are included in the certification application are informed about the certificate issuance.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

See clause 4.4.1

4.7.6 Publication of the re-keyed certificate by the CA

See clause 4.4.2

4.7.7 Notification of certificate issuance by the CA to other entities

Information about the certificate issuance may be sent to the authorized Subject whose data is included in the certification application.

4.8 Certificate Modification

Certificate modification is possible only as part of the re-key process described in chapter 4.7.

4.9 Certificate Revocation

Revocation of the certificate is equivalent to an invalid certificate and results in the termination of the contract between the Subscriber and IDnow Trust Services AB. The Subject is prohibited to use any electronic signature, electronic seal or time stamping if the certificate is revoked or suspended.

IDnow Trust Services AB provides information about the current certificate status via the Certificate Revocation List (CRL) and the online certificate verification OCSP service. CRL and OCSP use the same database to determine certificate statuses.

IDnow Trust Services AB provides the certificate revocation service 24 hours a day.

4.9.1 Circumstances for revocation

The revocation of a certificate permanently ends the operational period of the certificate prior to the certificate reaching the end of its initial validity period. Prior to revoking a certificate, the Issuing CA shall verify that the revocation request was made by either the Subscriber or the Subject.

The Issuing CA should revoke a certificate if one or more of the following circumstances occur:

- Subject or Subscriber requests revocation using the IDnow Trust Services AB website.
- Subject notifies that the original certificate request was not authorized and does not retroactively grant authorization.
- IDnow Trust Services AB obtains a report that the Subject's Private Key corresponding to the Public Key in the certificate suffered a key compromise or no longer complies with the requirements.
- Subscriber has violated one or more of its obligations under the Terms and Conditions.
- IDnow Trust Services AB receives a notification that a certificate has been used incorrectly.
- Subject made a change (e.g. surname change) in the information contained in the certificate.
- the certificate was not issued in accordance with the Practice Statement and/or this policy.
- IDnow Trust Services AB obtains a report that a Certificate is no longer compliant with the Policy under which it has been issued.
- IDnow Trust Services AB notices that information in the certificate is not accurate or misleading.
- The authorization for IDnow Trust Services AB to issue certificates has been revoked or terminated.
- IDnow Trust Services AB gets notified about a possible compromise of the Private Key of the CA used for issuing the certificate.
- technical content or format of the certificate presents an unacceptable risk to Relying Parties.
- IDnow Trust Services AB receives information that cryptographic suites used in CA Certificates have been deemed non secure.

4.9.2 Who can request revocation

The Subject or Subscriber can request revocation of the Subject's certificates at any time. RA may request revocation of the Subject's certificates or submit a report of an event related to revocation based on Subject's application. CA may request revocation for any of the reasons listed in clause 4.9.1 of this Policy.

Respected Supervisory Body can request a revocation or submit a report of events that may cause revocation for a Subject's or CA's certificates at any time.

Relying Parties and other third parties may submit reports informing IDnow Trust Services AB of reasonable cause to revoke the certificate.

When the Subject requesting certificate revocation is not the owner of the given certificate (i.e. the Subscriber), the certification authority has to:

- check whether the requester is authorized to request the revocation (e.g. acts as a Subscriber's requester)
- notify the Subject about revocation or initiation of revocation process.

4.9.3 Procedure for revocation request

Certificate revocation requests may be submitted by Subjects from their registered user accounts at IDnow Trust Services AB . In this case, Subject's authentication involves re-entering account credentials and results in automatic revocation.

Certificate revocation requests may also be submitted by the Subject directly to IDnow Trust Services AB via the point of contact data as stated in 1.6.2. In this case, the Subject's authentication is done by a basic identity data check against the register of IDnow Trust Services AB users. Afterwards, the revocation request is forwarded to Registration Officers. A Registration Officer calls the phone number provided in the request and verifies the identity and eligibility of the person.

Subscribers, Relying Parties, and other third parties may submit requests to points of contact as stated in 1.6.2.

IDnow Trust Services AB will record each request for revocation, authenticate the source and take appropriate action to revoke the certificate if the request is authentic and approved.

4.9.4 Revocation request grace period

The Subscriber or Subject is required to request revocation immediately after verifying the loss or theft of the device.

4.9.5 Time within which CA must process the revocation request

All revocation requests for end entity certificates, both those generated automatically via user accounts and those initiated by IDnow Trust Services AB itself, must be processed within a maximum of 24 hours of receipt.

The IDnow Trust Services AB shall process revocation requests as follows:

- Before the next CRL is published, if the request is received two or more hours before regular periodic CRL issuance,
- By publishing it in the CRL following the next CRL, if the request is received within two hours of the regularly scheduled next CRL issuance, and
- Regardless, within 20 hours after receipt.

Once a decision has been taken to process revocation it is processed immediately and made available via OCSP with a maximum delay of 60 minutes.

4.9.6 Revocation checking requirement for Relying parties

Prior to relying on the information listed in a certificate, a Relying Party shall confirm the validity of each certificate in the certificate path, including checks for certificate validity, issuer-to-Subject name chaining, policy and key use constraints, and revocation status through CRLs or OCSP responders identified in each certificate in the chain.

4.9.7 CRL issuance frequency (if applicable)

Every certification authority being a part of IDnow Trust Services AB issues a separate Certificate Revocation List.

Every Certificate Revocation List is updated at least every 24 hours.

Certificate Revocation List for Root CA is updated at least every 12 months.

4.9.8 Maximum latency for CRLs (if applicable)

Each CRL is published without undue delay as soon as it is created (usually this is done automatically within a few minutes).

4.9.9 On-line revocation/status checking availability

IDnow Trust Services AB provides a real-time certificate status verification service. This service is carried out on the basis of OCSP as described in RFC6960. Using OCSP, it is possible to acquire certificate status information without requiring CRL.

OCSP response times are generally no longer than 10 seconds under normal network operating conditions.

4.9.10 On-line revocation checking requirements

Relying parties must check revocation information of a certificate on which they wish to rely.

For the status of Subject certificates:

IDnow Trust Services AB updates information provided via an OCSP every few minutes. OCSP responses have a maximum expiration time of seven days.

For the status of subordinate CA certificates the following applies:

IDnow Trust Services AB updates information provided via a CRL at least every twelve months and within 24 hours after revoking a subordinate CA certificate.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements related to key compromise

No stipulation.

4.9.13 Circumstances for suspension

Not applicable.

4.9.14 Who can request suspension

No stipulation.

4.9.15 Procedure for suspension request

No stipulation

4.9.16 Limits on suspension period

No stipulation

4.10 Certificate Status Services

4.10.1 Operational Characteristics

IDnow Trust Services AB provides a Certificate status service in the form of a CRL distribution point, an OCSP responder or both in the certificates. OCSP certificate status request services are accessible over HTTP. The current CRL is published in the repository and available through the CRL distribution point over HTTP.

The formats and protocols of the services are described in sections 7.2 and 7.3 of this policy. The system time of the OCSP responder is synchronized daily using the DCF77 time signal and reliable time servers (NTP) on the Internet.

The URL of the OCSP service and CRL distribution point are included in the certificate.

4.10.2 Service Availability

IDnow Trust Services AB maintains an online Repository that applications can use to automatically check the status of unexpired Certificates issued by IDnow Trust Services AB.

Validation services for qualified electronic signatures and qualified electronic seals are also available 24/7 (without any planned outages).

4.10.3 Operational Features

No stipulation.

4.10.4 End of Subscription

The end of the subscription occurs in the following cases:

- Subject certificate validity period has expired and the Subscriber has not updated or modified his/her key,
- Subject's certificate was revoked and replaced by another certificate.

4.11 Key Escrow and Recovery

CA Private Keys are never escrowed. IDnow Trust Services AB does not offer key escrow services to Subjects.

4.11.1 Key escrow and recovery policy and practices

No stipulation.

4.11.2 Session key encapsulation and recovery policy and practices

No stipulation.

5. Management, Operational, and Physical Controls

5.1 Physical Security Controls

The scope related to this item is addressed in the Practice Statement.

5.1.1 Power and air conditioning

The scope related to this item is addressed in the Practice Statement.

5.1.2 Water exposure

The scope related to this item is addressed in the Practice Statement.

5.1.3 Fire prevention and protection

The scope related to this item is addressed in the Practice Statement.

5.1.4 Media storage

The scope related to this item is addressed in the Practice Statement.

5.1.5 Waste disposal

The scope related to this item is addressed in the Practice Statement.

5.2 Procedural Controls

5.2.1 Trusted roles

The scope related to this item is addressed in the Practice Statement.

5.2.2 Four-eyes principle

The scope related to this item is addressed in the Practice Statement.

5.2.3 Identification and authentification for each role

The scope related to this item is addressed in the Practice Statement.

5.2.4 Roles Requiring Separation of Duties

The scope related to this item is addressed in the Practice Statement.

5.3 Personnel Security Controls

5.3.1 Qualifications, experience and clearances

The scope related to this item is addressed in the Practice Statement.

5.3.2 Personnel testing procedures

The scope related to this item is addressed in the Practice Statement.

5.3.3 Training requirements

The scope related to this item is addressed in the Practice Statement.

5.3.4 Retraining Frequency and requirements

The scope related to this item is addressed in the Practice Statement.

5.3.5 Job rotation frequency and sequency

The scope related to this item is addressed in the Practice Statement.

5.3.6 Sanctions for unauthorized actions

The scope related to this item is addressed in the Practice Statement.

5.3.7 Contracts with the personnel

The scope related to this item is addressed in the Practice Statement.

5.3.8 Documentation available to Personnel

The scope related to this item is addressed in the Practice Statement.

5.4 Audit Logging Procedures

The scope related to this item is addressed in the Practice Statement.

5.4.1 Types of events recorded

The scope related to this item is addressed in the Practice Statement.

5.4.2 Frequency of processing log

The scope related to this item is addressed in the Practice Statement.

5.4.3 Retention time for Records

The scope related to this item is addressed in the Practice Statement.

5.4.4 Protection of records

The scope related to this item is addressed in the Practice Statement.

5.4.5 Backups of records

The scope related to this item is addressed in the Practice Statement.

5.4.6 Audit log accumulation system

The scope related to this item is addressed in the Practice Statement.

5.4.7 Notification system to event-Causing

The scope related to this item is addressed in the Practice Statement.

5.4.8 Vulnerability assessment

The scope related to this item is addressed in the Practice Statement.

5.5 Records Archival

5.5.1 Types of archives

The scope related to this item is addressed in the Practice Statement.

5.5.2 Retention period of archives

The scope related to this item is addressed in the Practice Statement.

5.5.3 Protection of archive

The scope related to this item is addressed in the Practice Statement.

5.5.4 Backup archives procedures

The scope related to this item is addressed in the Practice Statement.

5.5.5 Requirements for time-stamping the archives

The scope related to this item is addressed in the Practice Statement.

5.5.6 Archive storage

The scope related to this item is addressed in the Practice Statement.

5.5.7 Archival information access and verification procedures

The scope related to this item is addressed in the Practice Statement.

5.6 Key Changeover

The scope related to this item is addressed in the Practice Statement.

5.7 Compromise and Disaster Recovery

The scope related to this item is addressed in the Practice Statement.

5.7.1 Incident and compromise handling procedures

The scope related to this item is addressed in the Practice Statement.

5.7.2 Incidents, related to failures in hardware, software and/or data

The scope related to this item is addressed in the Practice Statement.

5.7.3 Private key compromise procedures

The scope related to this item is addressed in the Practice Statement.

5.7.4 Business continuity Management

The scope related to this item is addressed in the Practice Statement.

5.8 TSP Termination

5.8.1 Termination plan

The scope related to this item is addressed in the Practice Statement.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

The scope related to CA keys is addressed in the Practice Statement.

Subject private keys are generated and used in a Remote Qualified Signature Creation Device (QSCD). RQSCD complies with certification against EN 419 241-2[Ref. 16].

RQSCD supports cryptographic algorithms and key lengths defined in ETSI TS 119 312. The algorithm parameters to be used for signature creation are chosen so they can withstand the life of the subject's certificate.

The RQSCD environment protects all generated keys to ensure their confidentiality and integrity. Keys are not kept outside of the protected environment. Subject private keys are generated in advance and linked to the subject before certificate issuance.

RQSCD is initialized before generating or containing any signing key. Its technical mechanisms require at least two operators. RQSCD and certificate generation are maintained by the same entity under provisions of the present document.

The subject private signing keys are linked to the appropriate subject’s identity. The reference link is created after registration and initial identity validation specified in the chapter 3.2 of the present document. The technical process ensures that the subject identification data linked to the subject identity reference is the same as the one linked to the subject of the associated certificate.

The subject private key is used only once for the purpose of creating a certificate request PKCS#10 before its public key certificate is linked.

6.1.2 Private key delivery to subscriber

The scope related to CA keys this item is addressed in the Practice Statement.

The private keys are neither delivered to the subscriber nor the subject. They remain in the secured area of the RQSCD as long as they can be used.

Private keys managed on behalf of the user are secured by RQSCD. Access to the private keys are protected by the Signature Activation Module (SAM)according to the ETSI EN 419 241-2 [Ref. 16].

For issuance of short-term certificates, eID means associated with the subject private key are not issued to the subscriber. Keys are only used within the process's single session. Access to the keys is disabled once the process is terminated.

For issuance of long-term certificates, IDnow Trust Services AB associates the subject private key and certificate with identity provided by the Registration Service.

6.1.3 Private key delivery to certificate issuer

The scope related to this item is addressed in the Practice Statement.

6.1.4 CA public key delivery to relying parties

The scope related to this item is addressed in the Practice Statement.

6.1.5 Key sizes

The scope related to this item is addressed in the Practice Statement.

6.1.6 Public key parameters generation and quality checking

The scope related to this item is addressed in the Practice Statement.

6.1.7 Key usage purposes

The scope related to this item is addressed in the Practice Statement.

6.2 Private Key Protection and Cryptographic Module Engineering

6.2.1 Cryptographic module standards and controls

The scope related to this item is addressed in the Practice Statement.

6.2.2 Private key (n out of m) multi-person control

The scope related to this item is addressed in the Practice Statement.

6.2.3 Private key escrow

The scope related to this item is addressed in the Practice Statement.

6.2.4 Private key backup

The scope related to this item is addressed in the Practice Statement.

6.2.5 Key Restoration

The scope related to this item is addressed in the Practice Statement.

6.2.6 Private key archival

The scope related to this item is addressed in the Practice Statement.

6.2.7 Private key transfer into or from a cryptographic module

The scope related to this item is addressed in the Practice Statement.

6.2.8 Private key storage on cryptographic module

The scope related to this item is addressed in the Practice Statement.

6.2.9 Method of activating private key

The scope-related CA keys are addressed in the Practice Statement.

Subject private keys activation are addressed in 6.3.1 of the present document.

6.2.10 Method of deactivating private key

The scope related to this item is addressed in the Practice Statement.

Subject private keys are enabled only for signature creation of specified documents to be signed as specified by Signature Activation Data (SAD). After signature creation private keys are disabled.

6.2.11 Method of destroying private key

The scope related to CA keys is addressed in the Practice Statement.

If the subject public key certificate is revoked, the corresponding subject private key is destroyed and cannot be recovered. A signing key is destroyed when requested by the subject or subscriber in a revocation process.

The Subject private key is destroyed immediately after subjects public key certificate expiration.

The destruction mechanism and procedure for the signing key are designed to eliminate all backups of the given signing key to prevent any potential reconstruction of the signing key.

6.2.12 Cryptographic Module Rating

The scope related to this item is addressed in the Practice Statement.

6.2.13 Public key archival

The scope related to this item is addressed in the Practice Statement.

6.2.14 Certificate operational periods and key pair usage periods

The scope related to this item is addressed in the Practice Statement.

6.3 Activation Data

6.3.1 Activation data generation and installation

The scope related to CA keys activation data is addressed in the Practice Statement.

IDnow Trust Services AB ensures that each subject is accurately identified and authenticated prior to permitting actions that could affect the authorized control over any signing key. To authenticate and activate the signing key, the subject must provide Signature Activation Data (SAD) to the Signature Activation Module (SAM).

Based on risk assessment outcomes, necessary controls are implemented to defend against threats to SAD and its usage, including online guessing, offline guessing, credential duplication, phishing, eavesdropping, replay, session hijacking, man-in-the middle, credential theft, spoofing, and masquerading attacks. Access control measures are in place to prevent subjects from accessing sensitive system objects and any functionalities that could allow control over another's signing key.

IDnow Trust Services AB guarantees that the representation of the document do be signed is controlled by the subject and signed solely with the subject's own signing key. Only representation of the document to be signed indicated by the SAD may be signed with an activated signing key.

IDnow Trust Services AB is responsible for validating the public key certificate prior to utilizing the associated signing key. The use of signing keys is restricted to scenarios explicitly consented to by the subject. Furthermore, the selection of algorithm parameters for signature generation by trusted systems is done with the longevity of the subject's certificate in mind, ensuring resistance throughout its valid period.

6.3.2 Activation data protection

The scope related to CA keys activation data is addressed in the Practice Statement.

SAD is collected and secured by the Signature Activation Protocol, used to control with a high level of confidence (at least SCAL2-Sole Control Access Level 2), a given signature operation, performed by a RQSCD on behalf of the subject, that this under sole control of the subject. Signature Activation Module (SAM) used in a tamper protected environment.

6.3.3 Other aspects of activation data

The scope related to this item is addressed in the Practice Statement.

6.4 Computer Security Controls

6.4.1 Specific computer security technical requirements

The scope related to this item is addressed in the Practice Statement.

6.4.2 Computer security rating

The scope related to this item is addressed in the Practice Statement.

6.5 Life Cycle Security Controls

6.5.1 System development controls

The scope related to this item is addressed in the Practice Statement.

6.5.2 Security management controls

The scope related to this item is addressed in the Practice Statement.

6.5.3 Life cycle security controls

The scope related to this item is addressed in the Practice Statement.

6.6 Network Security Controls

The scope related to this item is addressed in the Practice Statement.

6.7 Time synchronization

The scope related to this item is addressed in the Practice Statement.

6.8 Time-stamping

The scope related to this item is addressed in the Practice Statement.

7. Certificate and CRL Profiles

Profiles of certificates and CRLs are issued in line with norms of ETSI TS 119 412-1 and ETSI EN 319 412 (Parts 2,3,4,5).

7.1 Certificate Profile

7.1.1 Version number

Certificates issued are compliant with the X.509 V3 standard.

7.1.2 Certificate extensions

CA certificates contain the following critical and mandatory extensions:

Extension	OID	Parameter
Key Usage	2.5.29.15	Certificate Signing (Off-line CRL Signing) CRL Signing (06)
Basic Constraints	2.5.29.19	Subject Type=CA (Path Length Constraint)

CA certificates can include the following non-critical and mandatory extensions:

Extension	OID	Parameter
Authority Key Identifier	2.5.29.35	160-bit SHA-1 hash of the issuer public key
Subject Key Identifier	2.5.29.14	160-bit SHA-1 hash of the subject public key
Certificate Policies	2.5.29.32	Certificate Policy [1]: PolicyIdentifier: *<OID>* PKIX CPS Pointer Qualifier (1.3.6.1.5.5.7.2.1) =CPS Pointer: *<CPS_URI>*
Authority Information Access	1.3.6.1.5.5.7.1.1	Access Method: CA Issuers (1.3.6.1.5.5.7.48.2)

		Access Location: URI: *<issuingCA_CER_URI>*
CRL Distribution Points	2.5.29.31	Distribution Point Name: Full Name: URI: *<issuingCA_CRL_URI>*

Further extensions can be added; they must comply with [X.509], [RFC 5280], [RFC 6818], [ETSI EN 319 412] and [ETSI-ALG] or they must be described in a referenced document.

Subscriber and/or subject certificates contain the following critical extensions:

Extension	**OID**	**Parameter**
Key Usage	2.5.29.15	Non Repudiation
Basic Constraints	2.5.29.19	Subject Type=End Entity Path Length Constraint=None

Subscriber and/or subject certificates can include the following non-critical extensions:

Extension	**OID**	**Parameter**
Authority Key Identifier	2.5.29.35	160-bit SHA-1 hash of the issuer public key
Subject Key Identifier	2.5.29.14	160-bit SHA-1 hash of the subject public key
CRL Distribution Points	2.5.29.31	Distribution Point Name: Full Name: URI: *<issuingCA_CRL_URI>*
Certificate Policies	2.5.29.32	Certificate Policy [1]: PolicyIdentifier: *<OID>* PKIX CPS Pointer Qualifier (1.3.6.1.5.5.7.2.1) =CPS Pointer: *<CPS_URI>* **QCP-n-qscd:** Certificate Policy [2]: PolicyIdentifier: 0.4.0.194112.1.2

		QCP-l-qscd: Certificate Policy [2]: PolicyIdentifier: 0.4.0.194112.1.3
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)
qcStatements	1.3.6.1.5.5.7.1.3	QC Statement [1]: PKIX QCSyntax-v2 (1.3.6.1.5.5.7.11.2) QC Statement [2]: Semantics Identifier 0.4.0.194121.0.0.1 (1.3.6.1.5.5.7.11.2) **QCP-n-qscd:** QC Statement [3]: Semantics Identifier: 0.4.0.194121.1.1 (1.3.6.1.5.5.7.11.2) QC Statement [4]: QC Compliance (0.4.0.1862.1.1) QC Statement [5]: QC Secure Signature Creation Device (0.4.0.1862.1.4) QC Statement [6]: QC Type=EtsiQctEsign (0.4.0.1862.1.6.1) (0.4.0.1862.1.6) **QCP-l-qscd:** QC Statement [3]: Semantics Identifier: 0.4.0.194121.1.2

		(1.3.6.1.5.5.7.11.2) QC Statement [4]: QC Compliance (0.4.0.1862.1.1) QC Statement [5]: QC Secure Signature Creation Device (0.4.0.1862.1.4) QC Statement [6]: QC Type=EtsiQctEseal (0.4.0.1862.1.6.2) (0.4.0.1862.1.6)
Authority Information Access	1.3.6.1.5.5.7.1.1	Access Method: CA Issuers (1.3.6.1.5.5.7.48.2) Access Location: URI: *<issuingCA_CER_URI>* *Access Method: OCSP* *(1.3.6.1.5.5.7.48.1)* *Access Location: URI: <OCSP_URI>*
CRL Distribution Points	2.5.29.31	Distribution Point Name: Full Name: URI: *<issuingCA_CRL_URI>*

Further extensions can be added; they must comply with [X.509], [RFC 5280], [RFC 6818], [ETSI EN 319 412] and [ETSI-ALG] or they must be described in a referenced document. The detailed information about certificate profiles is published in separate documents publicly available on https://trust-services.io/repository/.

The list of RQSCDs in Sweden is made publicly available on the website of the Swedish Post and Telecom Authority (PTS). IDnow Trust Services AB monitors the RQSCD certification status of the RQSCDs it uses. If the RQSCD certification status of the RQSCDs used is shorter than the regular certificate validity periods, customers will be informed in advance and the certificates will be issued with a shorter certificate validity period from the critical point in time.

However, if a certificate is mistakenly issued on a RQSCD with a certificate expiry date that is valid beyond the valid RQSCD certification status, the subject/subscriber will be informed in advance and the certificate will be revoked no later than the expiry date of the RQSCD.

If the TSP becomes aware of changes that affect the validity of the certificate, for instance, because the supervisory body has withdrawn the RQSCD certification status, all affected certificates with “esi4-qcStatement-4” (0.4.0.1862.1.4) according to ETSI EN 319 412-5 and which are affected by this change of the affected RQSCD certification status will be revoked. The subjects concerned and, if applicable, subscribers will be informed of this.

7.1.3 Algorithm Object Identifiers

The following signature algorithms are currently used in CA and subscriber and/or subject certificates and in time stamps:

- sha512 with RSA encryption with OID 1.2.840.113549.1.1.13

7.1.4 Name forms

In the subject (here: name of the subject/subscriber) and issuer (name of the issuer) fields, names are assigned according to [X.500] or [X.509] as DistinguishedName. The attributes described in section 3.1.4 can be assigned. Coding is carried out as UTF8 string or PrintableString for the C (Country) attribute.

7.1.5 Name constraints

“NameConstraints” is not used.

7.1.6 Certificate Policy Object Identifier

“CertificatePolicies” can contain the OID of Practice Statement supported.

7.1.7 Usage of Policy Constraints Extension

“PolicyConstraints” is not used.

7.1.8 Policy qualifier syntax and semantic

“PolicyQualifiers” can be used.

7.1.9 Processing Semantics for Critical Certificate Extensions

In service, CA and subscriber and subject certificates, the CertificatePolicies extension is not critical. Subscribers and relying parties are free to decide whether this extension is evaluated.

7.2 CRL Profile

7.2.1 Reason for Revocation

7.2.1.1 CA certificates

For revoked CA certificates, IDnow Trust Services AB states the reason for revocation in the reasonCode entry in the CRL. If an entry is required, IDnow Trust Services AB uses one of the following CRLReasons according to RFC 5280, section 5.3.1, whichever best matches the revocation reason:

- keyCompromise (1),
- cACompromise (2),
- affiliationChanged (3),
- superseded (4) or
- cessationOfOperation (5).

7.2.1.2 Subscriber and/or subject certificates

The subscriber must select a revocation reason. If the subscriber selects unspecified (0), the reasonCode entry in the CRL remains empty. IDnow Trust Services AB uses one of the following CRLReasons according to RFC 5280, section 5.3.1:

- unspecified (0)
- keyCompromise (1),
- affiliationChanged (3),
- superseded (4) or
- cessationOfOperation (5)

The TSP subsequently enters the following revocation reason as a CRL reason, if the subscriber violates the agreed terms and conditions:

- privilegeWithdrawn (9).

If there is evidence that a key has been compromised, but the subscriber failed to document the correct CRLReason, the TSP will then set this value to “keyCompromise”. If the TSP determines that the certificate private key was compromised before the revocation date specified in the CRL entry for that certificate, the TSP will then correct the revocation date. This backdating is an exception and does not usually apply.

7.2.2 Version number

The CRL list profile is compliant with the X.509 V2 standard.

7.2.3 CRL and CRL Entry Extensions

Revocation entries remain in the associated revocation lists after the respective certificate validity has expired.

Certificate revocation lists can contain the following non-critical extensions:

Extension	OID	Parameter
cRLNumber	2.5.29.20	Number of the certificate revocation list
Authority Key Identifier	2.5.29.35	160-bit SHA-1 hash of the issuer public key
expiredCertsOnCRL	2.5.29.60	The extension is used only for **QCP-n-qscd**, **QCP-l- qscd**
Reason Code	2.5.29.21	If this field is shown, then a CRLReason is used according to section

7.3 OCSP Profile

IDnow Trust Services AB provides an on-line certificate status verification service based on OCSP (Online Certificate Status Protocol) in accordance with RFC 6960. The service is provided in the authorized responder mode (Authorized Responder). Responses of the responder are authenticated with a special certificate issued for that purpose by the IDnow TS OCSP CA.

In addition to RFC 6960, the OCSP responder also supports positive information. (“Certificate is authentic and valid”).

The OCSP responder delivers the following replies:

- “good” if the responder identifies the certificate as not revoked,
- “unknown” if the responder cannot identify the status of the certificate and
- “revoked” if the responder identifies the certificate as revoked.

The “nextUpdate” field is set. The difference between the nextUpdate field and the thisUpdate is at least eight hours, however, it does not exceed 24 hours.

7.3.1 Version number

Responses of the OCSP services generated by the OCSP server are compliant with RFC 6960. The version corresponds to version V1.

7.3.2 OCSP extensions

The OCSP server response contains the OCSP Nonce Extension (OID 1.3.6.1.5.5.7.48.1.2) that contains a phrase which links the query with the response. The value in the OCSP response is the same as the phrase in the query. The purpose of the phrase is to prevent replay attacks on the OCSP server. Responses of the OCSP server do not contain private extensions.

This dedicated responder certificate shall contain the id-kp-OCSPSigning EKU and the id-pkix-ocsp-nocheck extension.

Responses of the OCSP server do not contain private extensions.

8. Compliance Audit and Other Assessment

8.1 Frequency or circumstances of assessment

The scope related to this item is addressed in the Practice Statement.

8.2 Qualification of auditors

The scope related to this item is addressed in the Practice Statement.

8.3 Auditor's relationship with IDnow Trust Services AB

The scope related to this item is addressed in the Practice Statement.

8.4 Audit scope

The scope related to this item is addressed in the Practice Statement.

8.5 Actions Taken as a Result of Deficiency

The scope related to this item is addressed in the Practice Statement.

8.6 Communication of results

The scope related to this item is addressed in the Practice Statement.

9. Other Business and Legal Matters

9.1 Fees

The scope related to this item is addressed in the Practice Statement.

9.2 Financial Responsibility

The scope related to this item is addressed in the Practice Statement.

9.3 Confidentiality of Business Information

The scope related to this item is addressed in the Practice Statement.

9.4 Privacy of Personal Information

The scope related to this item is addressed in the Practice Statement.

9.5 Intellectual Property Rights

The scope related to this item is addressed in the Practice Statement.

9.6 Representations and Warranties

The scope related to this item is addressed in the Practice Statement.

9.7 Warranty Disclaimer

The scope related to this item is addressed in the Practice Statement.

9.8 Limitations of Liability

The scope related to this item is addressed in the Practice Statement.

9.9 Indemnities

The scope related to this item is addressed in the Practice Statement.

9.10 Amendments

9.10.1 Procedure for amendment

This Policy is reviewed at least annually and may be reviewed more frequently. All changes are reviewed and approved by the IDnow Trust Services AB before publication. Changes to this Policy are indicated by appropriate versioning.

IDnow Trust Services AB will post appropriate notices on its websites for any major or significant changes to this Policy.

Modification proposals may be submitted by regular or electronic mail to the contact addresses of IDnow Trust Services AB. Suggestions and propositions should describe modifications, including their scope and justifications as well as means of contact to the individual requesting modification.

9.10.2 Notification mechanism of and comment period

Information about every significant modification is submitted to every affected party.

After the notification in advance, comments on suggested modifications may be submitted by the affected parties within 14 working days of their announcement.

The only items not requiring notifications in advance are amendments resulting from editorial modifications, amendments to the contact information of the person responsible for the document management, and changes with minor impact on few individuals.

9.10.3 Circumstances under which OID must be changed

No stipulation.

9.11 Dispute Resolution Procedures

The scope related to this item is addressed in the Practice Statement.

9.12 Governing Law

The scope related to this item is addressed in the Practice Statement.

9.13 Complaince with applicable law

The scope related to this item is addressed in the Practice Statement.

9.14 Miscellaneous Provisions

The scope related to this item is addressed in the Practice Statement.

10. Appendix

10.1 Definitions and Acronyms

auditor: person who assesses conformity to requirements as specified in given requirements documents

authentication: provision of assurance that a claimed characteristic of an entity is correct [SOURCE: ISO 27002:2022]

Certificate Policy (CP): named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements

Certificate Revocation List (CRL): signed list indicating a set of certificates that have been revoked by the certificate issuer

certificate: public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the certification authority which issued it

Certification Authority (CA): authority trusted by one or more users to create and assign certificates

Certification Authority Revocation List (CARL): revocation list containing a list of CA-certificates issued to certification authorities that have been revoked by the certificate issuer

Coordinated Universal Time (UTC): time scale based on the second as defined in Recommendation ITU-R TF.460-6

High security zone: specific physical location of the security zone (see ETSI EN 319 401 clause 7.8) where the Root CA key is held

incident handling: any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from an incident

incident: any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems

information security breach: compromise of information security that leads to the undesired destruction, loss, alteration, disclosure of, or access to, protected information transmitted, stored or otherwise processed [SOURCE: ISO 27002:2022]

Practice Statement : the current version of document issued by a IDnow Trust Services AB outlining practices, procedures, and guidelines related to providing trust services. It serves as a reference for customers and stakeholders to understand how the trust service provider operates and what standards they adhere to.

Publicly-Trusted Certificate (PTC): certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software

Registration Authority (RA): entity that is responsible for identification and authentication of subjects of certificates mainly

registration officer: person responsible for verifying information that is necessary for certificate issuance and approval of certification requests

relying party: natural or legal person that relies upon an electronic identification or a trust service

revocation: permanent termination of the certificate's validity before the expiry date indicated in the certificate

risk: potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of that incident

root CA: certification authority which is at the highest level within TSP's domain and which is used to sign subordinate CA(s)

secure cryptographic device: device which holds the user's private key, protects this key against compromise and performs signing or decryption functions on behalf of the user

secure zone: area (physical or logical) protected by physical and logical controls that appropriately protect the confidentiality, integrity, and availability of the systems used by the TSP

short-term certificate: certificate whose validity period, i.e. the period of time from notBefore through notAfter, inclusive, is shorter than the maximum time to process a revocation request as specified in the Practice Statement

subject: entity identified in a certificate as the holder of the private key associated with the public key given in the certificate

subordinate CA: certification authority whose Certificate is signed by the Root CA, or another Subordinate CA

subscriber: legal or natural person bound by agreement with a trust service provider to any subscriber obligations

trust anchor: entity that is trusted by a relying party and used for validating certificates in certification paths

Trust Service Policy (Policy): set of rules that indicates the applicability of a trust service to a particular community and/or class of application with common security requirements

Trust Service Provider (TSP): entity which provides one or more trust services

trust service: means electronic services normally provided for remuneration by the Trust Services Provider which consists of:

- the creation, verification, and validation of electronic signatures, electronic seals or electronic time-stamps, electronic registered delivery services and certificates related to those services, or
- the creation, verification and validation of certificates for website authentication; or the preservation of electronic signatures, seals or certificates related to those service

vulnerability: weakness of an asset or control that can be exploited by one or more threats [SOURCE: ISO 27002:2022]

EU Qualified Certificate: Qualified Certificate as specified in Regulation (EU) No 910/2014

Qualified electronic Signature/Seal Creation Device (QSCD): As specified in Regulation (EU) No 910/2014

10.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

- CA Certification Authority
- CARL Certification Authority Revocation List
- CPS Certification Practice Statement
- CRL Certificate Revocation List

- DIS Dissemination Services
- FIPS Federal Information Processing Standard
- LCP Lightweight Certificate Policy
- NCP Normalized Certificate Policy
- NCP+ Extended Normalized Certificate Policy
- OCSP Online Certificate Status Protocol
- OID Object Identifier
- PDF/A Portable Document Format/Archive
- PIN Personal Identification Number
- PKI Public Key Infrastructure
- PTC Publicly-Trusted Certificate
- RA Registration Authority
- RQSCD Remote QSCD
- SDP Subject Device Provisioning
- SSL Secure Socket Layer
- TLS Transport Layer Security
- TLS/SSL Transport Layer Security/Secure Socket Layer protocol
- TSP Trust Service Provider
- QTSP Qualified Trust Service Provider
- TSA Time Stamp Authority
- UTC Coordinated Universal Time

10.3 References

- **[Ref. 1] Regulation (EU) No 910/2014 (eIDAS)**: Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- **[Ref. 2] REGULATION (EU) 2016/679 (General Data Protection Regulation - GDPR)**: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
- **[Ref. 3] DIRECTIVE (EU) 2022/2555 (NIS2)**: DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148
- **[Ref. 4] ETSI EN 319 401 standard :** ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

- **[Ref. 5] ETSI EN 319 403 standard** : ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers
- **[Ref. 6] ETSI EN 319 411-1 standard :** ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- **[Ref. 7] ETSI EN 319 411-2 standard :** ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
- **[Ref. 8] ETSI EN 319 412-1 standard :** ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
- **[Ref. 9] ETSI EN 319 412-2 standard :** ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate Profile for certificates issued to natural persons.
- **[Ref. 10] ETSI EN 319 412-3 standard :** ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate Profile for certificates issued to legal persons
- **[Ref. 11] ETSI EN 319 412-5 standard :** ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
- **[Ref. 12] ETSI TS 119 312 standard** : ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites for providing trust services
- **[Ref. 13] ETSI TS 119 431-1 standard :** ETSI TS 119 431-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev
- **[Ref. 14] ETSI TS 119 431-2 standard :** ETSI TS 119 431-2 "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation"
- **[Ref. 15] EN 419 241-1 standard :** EN 419 241-1 "Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements", produced by CEN
- **[Ref. 16] EN 419 241-2 standard :** EN 419 241-2 "Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing", produced by CEN
- **[Ref. 17] EN 419 221-5 standard :** EN 419 221-5 "Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services"
- **[Ref. 18] ETSI EN 319 422 standard** : ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
- **[Ref. 19] ETSI TS 119 461 standard** : ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects

- **[Ref. 20] RFC 3647**: RFC 3647 Certificate Policy and Practice Statement Framework published by Internet Engineering Task Force (IETF)
- **[Ref. 21] ETSI TS 119 431-1 standard:** ETSI TS 119 432 V1.1.1 “Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation”
- **[Ref. 22] RFC5280**: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- **[Ref. 23] ETSI TS 119 412-1 standard**: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
- **[Ref. 24] RFC 6818:** Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- **[Ref. 25] ETSI EN 319 412-4 standard :** ETSI EN 319 412-4 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates

IDnow Trust Services AB
Box 16285
103 25 Stockholm
Sweden

info@trust-services.io
www.trust-services.io