IDnow
Trust Services.

Practice Statement
IDnow Trust Services AB

version 1.0

Public

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	Practice Statement IDnow Trust Services AB
Relevant for	External
Document OID	1.3.6.1.4.1.61867.2.1.1.1.1

Change log

Version	Version Date	Changes	Author
1.0	03.07.2024	Version 1.0	Adam Ptasiewicz

1 Introduction

1.1 Scope

The Practice Statement describes the general rules applicable to the qualified, trusted services IDnow Trust Services AB provides. Throughout this document, the term “Practice Statement” refers to the present document.

This document, together with Trust Service Policy, fulfils the role of the Certificate Policy for the following classes of certificate and type of service:

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 tokens** and **certificate status tokens**.
4. generating and managing electronic signature creation data on behalf of the Subject (signatory)
5. processing certificate subjects' data for certificate issuance.

The Practice Statement and Trust Service Policy define the roles of the CA, RQSCD and TSA.

The structure and contents of the Practice Statement are in accordance with the recommendation of RFC 3647. It fulfils also the requirements of the standards:

1. ETSI EN 319 401
2. ETSI EN 319 411-1/2
3. ETSI TS 119 431-1/2
4. ETSI EN 319 412-1/2/3
5. ETSI EN 319 412-5

Detailed requirements for issuing certificates are described in Trust Service Policy.

This document contains a declaration that the services provided under the Practice Statement comply with the following regulations:

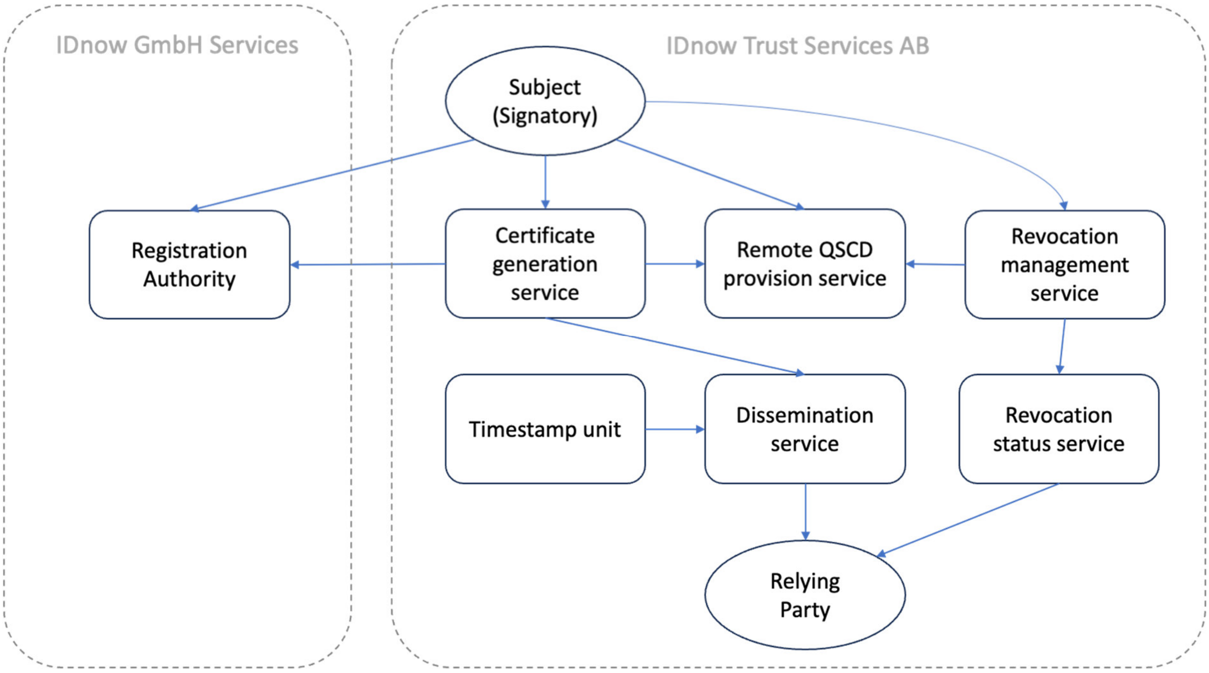
1. Regulation (EU) No 910/2014 (eIDAS)
2. REGULATION (EU) 2016/679 (General Data Protection Regulation - GDPR).

This Practice Statement defines parties, their obligations and responsibilities, procedures, and applicability range.

1.2 Overview of trust services

The following diagram shows a general overview of the IDnow Trust Services AB components of the qualified trust services:

- Issuing qualified electronic signature certificates in accordance with ETSI EN 319 411-1/2 standards
- Issuing qualified electronic seal certificates in accordance with ETSI EN 319 411-1/2 standards
- Issuing qualified time stamps in accordance with ETSI EN 319 421 standard
- Providing remote QSCD services based on certified devices ETSI EN 419 241-1/2 and ETSI TS 119 431-1/2 standards



The trust services are logically broken down in the present Practice Statement into the following component services CA, RQSCD and TSA to address requirements stated in clause 4.3 of ETSI EN 319 411-1.

- **CA Services**
    - **Registration authority**: verifies the identity and, if applicable, any specific attributes of a subject.

    - **Certificate generation service**: creates and signs certificates based on the identity and other attributes verified by the Registration service. This includes key generation.
    - **Dissemination service**: disseminates certificates to subjects, and if the subject consents, makes them available to relying parties. This service also makes TSP's terms and conditions and any published policy and practice information available to subscribers, subjects and relying parties.
    - **Revocation management service**: processes requests and reports relating to revocation to determine the necessary action. The results of this service are distributed through the revocation status service.
    - **Revocation status service**: provides certificate revocation status information to relying parties and other components.

- **RQSCD Service**
    - **Remote QSCD provision service**: manages QSCD on behalf of the subject, generates keys and creates signatures.

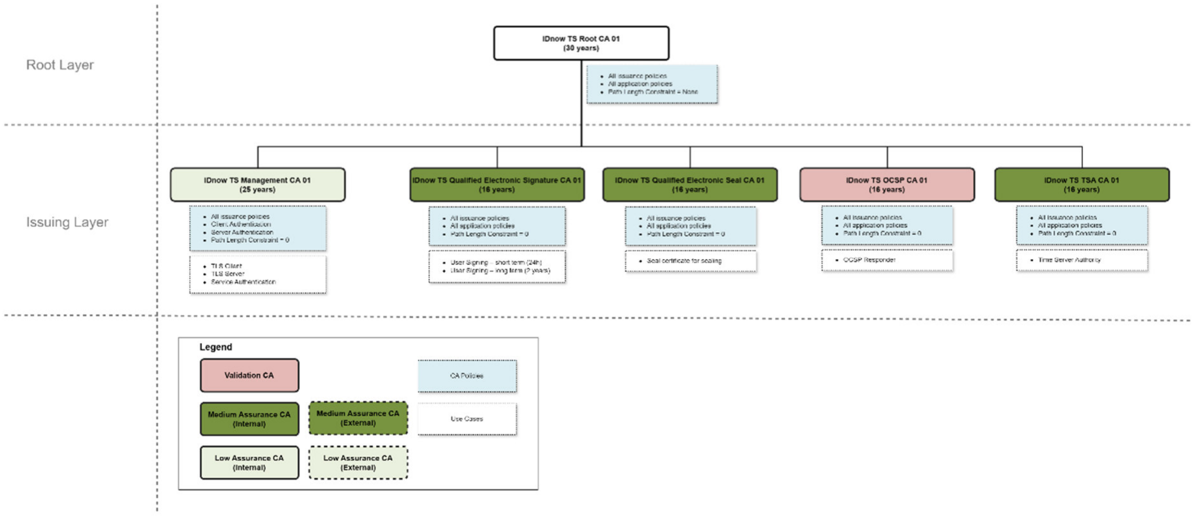
- **TSA Service**
    - **Timestamp unit**: provides time stamp service

This subdivision of services is only to clarify the Practice Statement and Trust Service Policy, and places no restrictions on any subdivision of implementing the TSP's services.

The IDnow Trust Services AB operates a technological solution known as the Central Component, which acts as a hub between systems and participants. The Central Component ensures controlled process flow and service connectivity.

The diagram represents the PKI hierarchy, including all authorities required for the provision of the trust services:

- IDnow TS Root CA 01,
- IDnow TS Management CA 01
- IDnow TS Qualified Electronic Signature CA 01
- IDnow TS Qualified Electronic Seal CA 01
- IDnow TS OCSP CA 01,
- IDnow TS TSA CA 01,


Root Layer
Issuing Layer
IDnow TS Root CA 01 (30 years)
All issuance policies
All application policies
Path Length Constraint = None
IDnow TS Management CA 01 (25 years)
All issuance policies
Client Authentication
Server Authentication
Path Length Constraint = 0
TLS Client
TLS Server
Service Authentication
IDnow TS Qualified Electronic Signature CA 01 (16 years)
All issuance policies
All application policies
Path Length Constraint = 0
User Signing – short term (24h)
User Signing – long term (2 years)
IDnow TS Qualified Electronic Seal CA 01 (16 years)
All issuance policies
All application policies
Path Length Constraint = 0
Seal certificate for sealing
IDnow TS OCSP CA 01 (16 years)
All issuance policies
All application policies
Path Length Constraint = 0
OCSP Responder
IDnow TS TSA CA 01 (16 years)
All issuance policies
All application policies
Path Length Constraint = 0
Time Server Authority
Legend
Validation CA
Medium Assurance CA (Internal)
Medium Assurance CA (External)
Low Assurance CA (Internal)
Low Assurance CA (External)
CA Policies
Use Cases

1.3 Document Name and Identification

The full name of this document is „Practice Statement – IDnow Trust Services AB”. This document is available in an electronic version at https://trust-services.io/repository/.

The Practice Statement can be identified by any party through the following OID: 1.3.6.1.4.1.61867.2.1.1.1.1.

1.4 PKI Participants

The Practice Statement regulates the most important roles between the following parties:

- Certificate Authorities
- Registration authorities
- Subjects and subscribers
- Relying parties
- Supervisory body
- Other participants

1.4.1 Certificate Authorities

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

There are the following root certification authorities of IDnow Trust Services AB (Root CAs):

- IDnow TS Root CA 01,

The list of Root CAs above can be expanded in the next version of the present document.

There are the following types of subordinate Certificate authorities 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.

1.4.2 Registration authorities

IDnow Trust Services AB uses external identity proofing service provider as the Registration Authority Service. The Registration Authority performs the following functions:

- Identifies the subscriber or subject who submitted a request in accordance with the rules and procedures established by IDnow Trust Services AB,
- verifies the subject's identity at time of registration by appropriate means,
- collects and validates either direct evidence or an attestation from an authorized source, of the identity and if applicable, any specific attributes of subjects to whom a certificate is issued,
- verifiers accuracy and completeness of an electronic request for a qualified certificate.

1.4.3 Subjects and subscribers

The subject is an entity identified in a certificate as the holder of the private key; the subject can be:

- a natural person;

- a natural person identified in association with a legal person;
- a legal person.

The subscriber may be the subject itself or an entity acting on behalf of one or more distinct subjects to whom it is linked.

Any private or legal entity could be a subscriber of IDnow Trust Services.

Organizations interested in obtaining certificates issued by IDnow Trust Services AB for their employees can do so via their designated representatives, while individual subscribers must personally apply for a certificate themselves.

1.4.4 Relying parties

A relying party is a natural person or legal entity that relies on the trust services of IDnow Trust Services AB.

1.4.5 Other participants

IDnow Trust Services AB uses subcontractors and service providers, such as specialized data centres, for reliable and secure colocation and operation of server and network equipment, providers of identity proofing services, agents services, IT services and others. IDnow Trust Services AB requires subcontractors and providers to strictly follow procedures in accordance with the present document .

This practice statement defines the responsibility and accountability model for providing trust services. The relationship to service providers is prescribed in the outsourcing agreement, detailed in Chapter 5.

1.5 Certificate Usage

The scope related to this item is addressed in the Trust Service Policy.

1.6 Practice Statement Administration

1.6.1 Organization responsible for administrating the document

This Practice Statement is administered by IDnow Trust Services AB:

IDnow Trust Services AB
Box 16285
10325 Stockholm
Sweden
Company registration number: 559469-9489

1.6.2 Contact

The email contact is info@trust-services.io.

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

The IDnow Trust Services AB team is responsible for evaluating the completeness and accuracy of Practice Statement and other documents concerning PKI services, provided by IDnow Trust Services AB, 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 chapter 1.5.2.

1.6.4 Approval procedures

The Practice Statement remains in effect from the indicated start date of its validity until the publication of the subsequent valid version.

Comments on suggested modifications may be submitted by the affected parties within 14 working days of their announcement (as presented in chapter 9.12). After this deadline, if there are no significant reservations to the substantive content of the proposed changes, the new version of the Practice Statement becomes valid with the validity date indicated in it.

The IDnow Trust Services AB Board decides to approve the new version of the Practice Statement. All changes made in the document are recorded in the history of the document. The approved document is published and communicated to:

- employees,
- appointed trusted roles,
- relying parties,
- subjects and subscribers,
- other participants defined in 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 has a repository of publicly available documents along with previous versions at: https://trust-services.io/repository/.

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

It contains current and previous versions of these electronic documents:

- Trust service provider certificates
- Other (see chapter 2.2).

2.2 Information published by IDnow Trust services AB

The repository contains 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

2.3 Frequency of publication

Publications are issued with the following frequency:

- Trust Service Policy and Practice Statement - see chapter 9.10,

- 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

2.4 Access to publication

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

3. Identification and Authentication

3.1 Naming

3.1.1 Types of names

Type of names assigned to the Subject is described in the Certificate Profile in the Trust Service Policy.

3.1.2 Meaningful names required

The scope related to this item is addressed in the Trust Service Policy.

3.1.3 User anonymity

The scope related to this item is addressed in the Trust Service Policy.

3.1.4 Rules for different names interpretation

The scope related to this item is addressed in the Trust Service Policy.

3.1.5 Uniqueness of the names

The scope related to this item is addressed in the Trust Service Policy.

3.1.6 Names verifications and disputes in this regard

The scope related to this item is addressed in the Trust Service Policy.

3.2 Initial Identity Validation

The initial identity validation is an outsourced service (Registration Authority) provisioned by IDnow GmbH, which is certified against ETSI EN 319 411-1/2 and ETSI TS 119 461 standards. IDnow Trust Services AB ensures the accuracy of IDnow GmbH's services in provisioning initial identity validation for the issuance of qualified certificates.

3.2.1 Method to prove possession of key

Once a registration is completed, the subject's key pair is generated by IDnow Trust Services AB Remote QSCD Provision Service. Subject’s key is generated in remote QSCD on behalf of the subject.

For more information see section 6.1.2 of this Practice Statement.

3.2.2 Authentication of legal person

Trust Service Policy specifies detailed provisions to authenticate legal persons.

3.2.3 Authentication of Natural person

Trust Service Policy specifies detailed provisions of natural person authentication.

3.2.4 Authentication of a natural person representing legal entity

Trust Service Policy specifies detailed provisions of natural person representing legal entity authentication.

3.2.5 Unconfirmed information

The scope related to this item is addressed in the Trust Service Policy.

3.2.6 Criteria of interoperability

No stipulation.

3.3 Identification and Authentication for Re-key Requests

Re-key request is not allowed in IDnow Trust Services AB practices.

3.4 Identification and Authentication for Revocation Requests

The specific practice related to this item is addressed in the Trust Service Policy.

4. Certificate Life-Cycle Operational Requirements

The scope related to this item is addressed in the Trust Service Policy.

5. Management, Operational, and Physical Controls

This chapter describes the general practices for supervision over physical and operational controls used by IDnow Trust Services AB.

The basis for establishing controls is a formal risk management process which is regularly reviewed and revised. IDnow Trust Services AB approves the risk assessment and accepts the residual risk identified.

Wherever practices indicate the need to ensure security mechanisms in the context of outsourced IT infrastructure and operational processes, the outsourcing agreement between IDnow Trust Services AB, IDnow GmbH and ESYSCO Sp. z o.o. applies. IDnow Trust Services AB appoints a trusted role, overseeing subcontractors in fulfilling the relevant contracts within the supply chain.

5.1 Physical Security Controls

Physical controls have been implemented for data center and office locations, which are used to process and store the personal data of the enrollment process to prevent unauthorized access.

IDnow Trust Services AB draws up and maintains a list of persons authorized to access the premises hosting the information systems of the trust services. IDnow Trust Services AB implements mechanisms to log access to the premises hosting the information system of the trust services.

IDnow Trust Services AB defines and implements measures to ensure the confidentiality and integrity of access logs to the premises hosting the trusted services.

IDnow Trust Services AB uses a service provider for the operation of the datacenter. This party provides the hardware, racks, grid connection, electricity, and climate control for the operation of the servers. IDnow Trust Services AB takes over the from the operating-system level upwards.

The following measures have been implemented for the data center:

- Closed windows and doors
- Fire / Water controls

- Redundant connections / power supplies
- Door access records
- Danger alarm system
- Video surveillance
- Perimeter protection / porter cabins
- Supervision or monitoring of third parties
- Control of datacenter access
- Control tours
- Secure destruction / disposal

IDnow Trust Services AB operates an asset management and classification system in which all relevant systems are recorded and categorized based on their required level of security. The Chief Security Officer is responsible for the management and reviews the assets at least twice a year. It is ensured that the physical controls are in place to protect assets in accordance with their classification.

Visitors to areas occupied by IDnow Trust Services AB may access only if they are escorted by authorized personnel of IDnow Trust Services AB.

An important aspect of protection is the creation of security zones, including a perimeter with a high level of security. In the highest security perimeter, IDnow Trust Services AB stores Root CA systems and HSM devices used, among others, for certificate generation and revocation management services. Double access (dual control) is required for this area.

5.2 Procedural Controls

5.2.1 Trusted roles

The functions allocation of trusted roles is implemented in such a way as to minimize the risk of compromising of information leakage or conflicts of interests. A detailed allocation of the functions and responsibilities of roles is stipulated in the internal documents of IDnow Trust Services AB.

The following trusted roles are assigned by IDnow Trust Services AB:

- **Board Member of IDnow Trust Services AB** – responsible for correct management of IDnow Trust Services AB, determines directions of development of certification authority, responsible to manage Trust Service Policy and Practice Statement,
- **Chief Security Officer** – supervises implementation and handling of information system security procedures, initiates and supervises cryptographic key and shared secret generation; assigns rights in the field of security and user’s access privileges,

- **System Administrator** – installs hardware and software for operating system; initially configures the system and network resources;
- **System Operator** – handles standard system operations, including backup copies and transfer of current copies and archives to offsite locations,
- **Registration Officer** – verifies subjects' identity and correctness of submitted certification request; authorizes certification request; authorizes the identity proofing policies provided by external identity proofing providers,
- **System auditor** – monitors QTSP services to ensure compliance with policies and procedures; verifies the event logs and incident management process,
- **Outsourcing Contract Manager** – supervises the suppliers, validates agreements and monitors their compliance and execution.

5.2.2 Four-eyes principle

The four-eyes principle is the minimum requirement for particularly security-critical operations. This is ensured by technical and organizational measures, such as access authorization and verification of knowledge. When validating a subject, it is ensured that an experienced validation specialist is called upon and works according to the four-eyes principle. Security-critical systems used for certificate issuance are generally protected by multi-factor authentication.

5.2.3 Identification and authentication for each role

The IDnow Trust Services AB trusted roles are subject to identification and authentication in the following situations as a minimum:

- inclusion on the list of persons allowed to access infrastructure, system and network resources,
- formal nomination authorizing to perform the assigned role,
- handover of account credentials to information systems.

Every account is unique and assigned to one specific person.

5.2.4 Roles Requiring Separation of Duties

Each trusted role only has the rights arising from the user's role and related responsibilities.

Some roles may be combined or modified within a limited scope.. Both, the Chief Security Officer and System Auditor roles are segregated from other roles.

5.3 Personnel Security Controls

5.3.1 Qualifications, experience and clearances

IDnow Trust Services AB ensures that all personel with trusted roles relating to the CA operations are free from conflicting interests that might affect their impartiality.

If an employee is employed under an outsourcing agreement, all duties resulting from a trusted role are covered by the specified agreement. The outsourcing agreement defines the duties and principles of service performed by persons in trusted roles.

The reliability of employees is determined from all required documents (in particular police clearance certificate, credit worthiness information and CV) of that employee. In the evaluation of the police clearance certificate every entry to the employee in the certificate must be checked separately by the Chief Security Officer and approved or rejected. If there are no entries, no evaluation is required. If a country does not have one of the mechanisms listed above (e.g. no credit worthiness information), IDnow Trust Services AB may use other measures with an equivalent level of assurance regarding the reliability of the employee.

Disciplinary sanctions (including up to termination of contract) for policy or procedure violations by personnel are defined in the outsourcing agreement.

5.3.2 Personnel verification procedures

IDnow Trust Services AB verifies personnel information, including trusted roles, in the following areas:

- confirmation of previous employment.
- verification of recommendations.
- confirmation of educational degree.
- verification of criminal records.
- identity verification.

5.3.3 Training requirements

In addition to strict requirements on competence and experience at the time of hiring, IDnow Trust Services AB provides regular trainings for trusted roles. It is key that all personnel have adequate training and experience for the duties specified in the role description and the employment contract in order to maintain the necessary competency. Such trainings include:

- Regulations, procedures and documentation related to the occupied position;
- Responsibilities arising from roles and tasks;
- Disaster recovery procedure;
- Information security policies;
- Procedures and security controls implemented by a Certification Authority;
- Personal Data Protection.

5.3.4 Training Frequency and requirements

Trainings described in chapter 5.3.3 must be repeated or supplemented if and when significant changes to the Practice Statement and/or the Certificate were made.

5.3.5 Job rotation frequency and sequency

The Practice Statement does not define any requirements in this field.

5.3.6 Sanctions for unauthorized actions

Personnel are bound by contractual employment obligation to carry out their duties according to internal rules. Regarding the disciplinary process, the outsourcing agreement with IDnow GmbH applies.

5.3.7 Contracts with the personnel

Independent contractors and their personnel are subject to the same privacy protection and confidentiality conditions. Under a signed contract, the persons or consultants are subject to the same verification procedure as the defined by present document.

5.3.8 Documentation available to Personnel

Management of IDnow Trust Services AB provides their personnel with access to the following documents:

- Trust Service Policy,
- Practice Statement,
- Information Security Policy
- extracts from documentation corresponding to performed role, including emergency procedures,
- range of responsibilities and obligations associated with the acted role in the system.

5.4 Audit Logging Procedures

Audit log files are generated by IDnow Trust Services AB for all events related to security and CA services. Where possible, security audit logs are automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism is used. All security audit logs, both electronic and non-electronic, are retained and made available during compliance audits.

5.4.1 Types of events recorded

The logs contain the following information:

- start-up and shutdown of the logging functions; and
- availability and utilization of needed services with the Trust Service network; and
- system start-up and shutdown; and
- system crashes and hardware failures; and
- firewall and router activities

IDnow Trust Services AB uses external logging and monitoring which is protected against unauthorized access. Logging is controlled regularly for critical information or personal data.

Any alteration, deletion, or copying of data is logged with the help of log files through the IDnow software so that alterations of personal data are always traceable. The allocation to the appropriate employee and client accounts is always guaranteed.

In addition, it is ensured that IDnow logs the following events:

- Physical facility access
- Changes to trusted roles
- Backup management
- Log management
- Acceptance and rejection of certificate requests
- IT and network management, as they pertain to the CA systems
- Security management

5.4.2 Frequency of processing log

The logs and monitoring are regularly checked for discrepancies. Audit logs are reviewed periodically for any evidence of malicious activity and following each important operation.

5.4.3 Retention time for Records

Retention period for audit logs are at least 6 months. During this period, they are available online upon request by an authorized person. After this period, event records are archived.

5.4.4 Protection of records

Audit log is stored in a dedicated storage within IDnow Trust services AB infrastructure. Logs are signed or sealed.

Access to the event log is configured in such a way that:

- only authorized persons have the right to read log entries,
- only the system administrator with assistance of the Chief Security Officer may archive or erase files (after their archive) containing events,
- it is possible to detect every violation of integrity,
- no entity has the right to modify the contents of the event logs.

IDnow Trust Services AB ensures that the time used to record events as required in the audit log is synchronised with UTC at least once a day.

5.4.5 Backups of records

Backup copies of entries in the system logs are kept and reliably stored. The procedures require event logs to undergo backup in accordance with an approved schedule.

5.4.6 Audit log accumulation system

Automated audit data is generated and recorded at the application, network and operating system level. Non-electronically generated audit data is recorded by Trusted Roles.

IDnow Trust Services AB ensures mechanisms which do not allow for switching off the logging function of CA.

5.4.7 Notification system to event-causing

IDnow Trust Services AB systems are monitored 24/7/365 days by system operators and by automatic solutions. In the case of activities having an impact on the system security, the

Chief Security Officer and the system administrator are automatically notified. In other cases, the notification is addressed only to the system administrator.

When critical information is being transferred to authorized persons, in terms of system security situations are foreseen where the transfer is carried out by other, suitably secured communication means such as mobile phones, e-mail.

5.4.8 Vulnerability assessment

IDnow Trust Services AB has implemented a vulnerability management policy. Based on that, internal security audits of all systems and networks to find vulnerabilities must be executed in each quarter.

5.5 Records Archival

5.5.1 Types of archives

IDnow Trust Services AB archives all data and files related to:

- the registration information
    - All documents and data used in the process of identity verification are subjected to archiving
- the system security;
- all requests submitted by users;
- all keys and certificates used by the Certification Authorities and the Registration Authority;
- CRL

IDnow Trust Services AB keeps archives in a retrievable format. It could be paper or electronic form.

5.5.2 Retention period of archives

Archived data (paper and electronic) is stored for a minimum of 15 years. After this period, archived data may be destroyed.

5.5.3 Protection of archive

All archives are stored in dedicated storages outsourced to IDnow GmbH.

Access to the archive have only authorized persons performing trusted roles.

The media holding the archive data and the applications required to process the archive data are maintained to ensure that the archive data can be accessed for the required time period (long-term archive).

5.5.4 Backup archives procedures

The archive is backed up in a secure place to protect data and to enable restoring the system after a failure and stored .

Detailed procedures of performing backup copies are regulated by additional policies.

5.5.5 Requirements for time-stamping the archives

The Archives containing audit records are time-stamped by a qualified time-stamping service.

5.5.6 Archive storage

The archive collection system is an internal system of IDnow Trust Services AB.

5.5.7 Archival information access and verification procedures

IDnow Trust Services AB ensures the integrity of archived information through periodic testing and verification against the original data. This activity is carried out solely under the oversight of the Chief Security Officer and is documented.

5.6 Key Changeover

The key changeover procedure applies to the keys of certification authorities (IDnow Root CA) and other authorities’ keys used for providing the trusted services defined in Chapter 1.2, Overview of trust .

The exchange of keys of certification authorities is performed in a manner that ensures keeping the agreed minimum certificate validity period. Before the expiry of any certificate of a certain authority, a new and independent public key infrastructure is created under which a new pair of keys and a certificate of the new certification authority is generated. Both authorities operate until the old certification authority's certificate expires. The new Certification authority takes over the role of the expiring one and performs all activities related to servicing certificates: generating, suspending and revoking certificates, generating CRL.

The expiring certification authority processes only revoking and suspending certificates issued within its own infrastructure and generate CRLs until its operating activity ceases (the certificate expires).

A new Certification authority's certificate is published in the repository (chapter 2).

5.7 Compromise and Disaster Recovery

5.7.1 Incident and compromise handling procedures

IDnow Trust Services AB has implemented an incident management process. This process addresses the requirements of Article 19 of eIDAS and Article 23 of NIS2 including notification requirements to supervisory body in case of any breach of security or loss of integrity that has a significant impact on the trust services provided.

IDnow will inform without undue delay but in any event within 24 hours after having become aware of it, the Supervisory Body and, where applicable, other relevant bodies of any breach of security or loss of integrity that has a significant impact on the Trust Service provided.

IDnow will also inform natural persons without undue delay in case of a security breach or loss of integrity.

For any vulnerability, given the potential impact, IDnow either implements a plan to mitigate the vulnerability; or documents the factual basis for the determination that the vulnerability does not require remediation. Critical vulnerabilities are addressed within 48 hours after its discovery. The Chief Security Officer is responsible for this process as part of his/her overall responsibility for security.

Incidents could be submitted via the contacts defined in Section 1.5.2.

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

All information concerning the corruption of computing resources, software, and/or data is communicated to the Chief Security Officer, who then assigns the necessary tasks according to established incident, risk and change management procedures.

These procedures are designed to assess the severity of an attack, investigate the incident thoroughly, minimize its impact, and implement measures to prevent recurrence in the future.

5.7.3 Private key compromise procedures

Key compromise is handled according to Incident Management documentation. Because it also qualifies as a disaster,the business continuity plan is triggered.

5.7.4 Business continuity Management

IDnow Trust Services AB regularly conducts a risk analysis to identify any risk and countermeasures in its business and processes. Regarding identified risks, IDnow Trust Services AB implements appropriate technical or organizational risk treatment measures. Risks are regularly reviewed and revised. The management board is responsible approving the risk treatment and the acceptance risks.

IDnow Trust Services AB ensures that all necessary data for the CA operations, essential information and software are backed up and stored in a safe place, more than 5km from the primary site, suitable to allow IDnow to timely go back to operations in case of major incidents or disasters.

Back-up arrangements are regularly tested to ensure they meet the requirements for business continuity

IDnow Trust Services AB maintains a business continuity plan (BCP) which defines the relevant risks, remediation measures and acceptable recovery times. Essential to the BCP is also how to avoid reoccurance of the cause that triggered the BCP.

5.8 TSP Termination

5.8.1 Termination plan

IDnow Trust Services AB has a termination plan in case of cessation of the company operations.

Before Trust Services AB terminates a CA Service, the following procedures will be executed:

- informing all subscribers and subjects and other entities with whom IDnow Trust Services AB has contracts or other forms of established relations.
- making the best effort for making arrangements with other Trust Service Providers (Custodians) to transfer the provision of services for its existing customers;
- destroying the CA private keys, including backup copies or keys withdrawn from use in such a manner that they cannot be retrieved;
- secure disposal or destroying any hardware appliances related to this service depending on the security regulations;
- terminating the authorisation of all subcontractors to act on behalf of Trust Services AB by carrying out any functions related to the process of issuing qualified certificates.

IDnow Trust Services AB tries to reduce potential disruptions as a result of the cessation of the CA services.

IDnow Trust Services AB has arrangements to finance these minimum requirements in case of bankruptcy, or for any other financial gaps.

The issued certificate databases, together with the revocation information and PKI infrastructure certificates, are transferred to the reliable party authorised by the Supervisory Body.

IDnow Trust Services AB declares to maintain documents and data resulting from the Practice Statement and the Trust Service Policy as well as additional documents and data required to verify the correctness of the Trust Services for a period of 15 years from their creation.

6. Technical security controls

This chapter defines the technical security measures deployed by IDnow Trust Services AB to protect cryptographic keys for itself and on behalf of external users.

IDnow Trust Services AB secures its own keys and those of users based on the following technical standards:

- ETSI EN 419 241-1 [Ref. 15]
- ETSI EN 419 241-2 [Ref. 16]

HSMs used by IDnow Trust Services AB complies with the following standard:

- ETSI EN 419 221-5 [Ref. 17]

6.1 Key pair generation and installation

The chapter includes the practices of the key pair generation for IDnow Trust Services AB services.

6.1.1 Key pair generation

Procedures for key management govern the secure storage and utilisation of keys that are owned by the keyholder. The generation and storage of IDnow Root CA private keys, which impact the secure operation of the entire public key certification system, should receive special consideration.

The IDnow Root CA possesses as a minimum one certificate that is unique to it. The use of the private key associated with the public key present in the self-certificate is limited to the purpose of signing the intermediate CA public keys and generating a registry of revoked certificates and operational CA certificates that are essential for the issuance of certificates.

The function of the private keys maintained by each authority, which match the public keys contained in the certificates issued by IDnow Root CA for them, is similar.

Each certificate authority (CA) should possess key pairs that enable the signing of certificates and CRLs.

CA keys and keys for service certificates are generated in hardware security modules (HSM) located in the high-security zones.

The generation of IDnow Root CA keys and intermediate CAs takes place at the headquarters of IDnow TS AB, with the participation of a carefully chosen and trusted group of individuals, which includes a Chief Security Officer and a system administrator.

Firstly, a specialised cryptography area is established for a certain TSP operational subject.

Next, the keys are generated. The audit group is only required to generate CRL certificates and signing keys.

Those steps are performed by trusted roles in the presence of the Chief Security Officer and, if necessary, under the supervision of an independent auditor. Whenever CA keys are generated, an independent auditor is present if essential.

The auditor has the possibility to observe the key ceremony either through an onsite visit or by viewing a video recording to verify that the key generation process was carried out correctly. The key ceremony is recorded.

For the key ceremony four-eyes principle is always enforced.

Certificate Authority key pairs running under IDnow Root CA are generated on a designated, authenticated workstation, that is connected to a hardware security module that complies with the EN 419 221-5 "Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services.

CAs keys are generated according to the IDnow Root CA procedure for generating key pairs. The actions performed during the generation of key pairs are recorded, dated, and signed by each person present during the generation.

Records are kept for audits and joint reviews of systems.

6.1.2 Private key delivery to subscriber

Subscriber and subject keys are generated and stored by the TSP.

The keys are generated in hardware security module (HSM) in the secure environment of the trust service provider.

The private keys are not delivered to the subscriber nor subject. The private keys remain in the secured area of the remote QSCD as long as they are used.

Use of private keys managed on behalf of the user by the TSP are secured by Signature Activation Module (SAM) according to the following technical standard:

- ETSI EN 419 241-2 [Ref. 16]

6.1.3 Public key delivery to certificate issuer

The TSP does not accept any public keys from external bodies.

6.1.4 CA public key delivery to relying parties

The certificate of the CA contains a public key. The CA certificate is publicly available to the subscriber and subject for download. Additionally, the CA certificate is present on the Swedish Trusted List. The CA and service certificates are available from the public repository.

6.1.5 Key sizes

The keys of all certification authorities of IDnow Trust Services AB are RSA keys and have at least 4096 bits. Keys of the subscribers and subjects are RSA keys and have at least 3072 RSA bits.

6.1.6 Public key parameters generation and quality checking

Public key-generating parameters meet the requirements specified in the standards: ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 and ETSI TS 119 312 norms in their latest applicable version available at the moment of publication of the present document.

6.1.7 Key usage purposes

Private IDnow Root CA keys are exclusively used to sign CA certificates, service certificates, and certificate revocation lists. Operational CA keys are used to sign CA certificates, service certificates, subscriber and subject certificates and certificate revocation lists.

6.2 Private key protection and cryptographic module engineering

6.2.1 Cryptographic module standards and controls

Hardware security modules are protected against manipulation by suitable technical and organizational controls. The CA keys are protected by an HSM that was evaluated and certified according to security standards.

All HSMs protecting CA and PKI infrastructure keys are certified against EN 419 221-5.

All HSMs protecting subject keys are certified against EN 419 241-2.

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

The cryptographic modules on which the service CA, subscriber and subject keys are stored is located in the secure environment of the trust service provider. Two authorized people are needed to activate the respective private key and to access the private subscriber and subject keys.

6.2.3 Private key escrow

The TSP does not offer escrow of private subscribers and subjects keys.

6.2.4 Private key backup

A backup of the private CA keys is available. The backup procedure for CA keys must be conducted within the HSM by two authorized individuals, and it occurs within the secure environment provided by the trust service provider. The backup system adheres to the same requirements and procedures as the live system.

Service keys stored on a smart card lack security measures. To ensure availability, multiple service keys are stored on redundant smart cards.

The recovery process for private keys also necessitates the involvement of two authorized individuals. Additional copies of the private CA keys do not exist.

6.2.5 Key Restoration

No stipulation.

6.2.6 Private key archival

Private keys of certification authorities are not archived and are immediately destroyed upon cessation or expiration.

IDnow Trust Services AB will not archive private keys once they have expired

6.2.7 Private key transfer into or from a cryptographic module

Transfers of private CA keys to or from the HSM are limited to backup and recovery purposes. Adherence to the four-eyes principle is compulsory. Private CA keys exported from/imported to another HSM are protected by encryption.

Transfer of subject private keys is not allowed.

6.2.8 Private key storage on cryptographic module

The private keys for CA and service certificates are encrypted in the HSM.

Subject private keys are secured with compliance to the following technical standards :

- ETSI TS 119 431-1 [Ref. 13]
- ETSI TS 119 431-2 [Ref. 14]
- ETSI TS 119 432 [Ref. 21]

6.2.9 Method of activating private key

The Root CA and CA service keys can only be activated according to the four-eyes principle by the authorized roles and for the permitted types of use (keyCertSign, cRLSign).

Private subject keys are activated by the end-entity using the authentication features and for the permitted types of use. It is the subject’s responsibility to protect its authentication credentials.

6.2.10 Method of deactivating private key

The private keys for CA and service certificates are deactivated by termination of the connection between the HSM and the application by the Trusted Roles provided for this purpose.

6.2.11 Method of destroying private key

When the scheduled lifetime of the private CA keys expires, these keys are deleted by the trusted roles provided for this purpose. The lifetime is determined in accordance with ETSI TS 119 312. This is accomplished by deleting the private key on the HSM and simultaneously deleting the backups on data media. When use of the HSM is terminated, the private keys in the device are deleted. When files containing the private subject key are deleted, the private key is then also destroyed.

6.2.12 Cryptographic module rating

The TSP operates suitable hardware-based and software-based key generators.

Signature creation data managed on behalf of subjects are generated in a qualified electronic signature and seal creation devices (QSCD) which meets the requirements specified in Annex II of eIDAS Regulation and published on the list of Qualified electronic Signature Creation Devices (QSigCDs) as defined in point 23 of Article 3 of Regulation 910/2014, Qualified electronic Seal Creation Devices (QSealCDs) as defined in point 32 of Article 3 of Regulation 910/2014, and Secure Signature Creation Devices (SSCDs) benefiting from the transitional measure set in Article 51(1) of Regulation 910/2014.

6.2.13 Public key archival

Public service, CA and subject keys are archived in the form of the generated certificates . Public CA keys are stored for at least 20 years after their expiration.

6.2.14 Certificate operational periods and key pair usage periods

The term of validity of the service and CA keys and certificates is variable and shown in the certificate. The maximum possible validity period totals 30 years. The term of validity of the subject keys and certificates is variable and shown in the certificate. The maximum possible validity period totals 36 months.

6.3 Activation data

6.3.1 Activation data generation and installation

The activation data of the service and CA keys is requested by the HSM. Adherence to the four-eyes principle is compulsory.

The Trust Service Policy addresses the scope related to the authentication means of subjects.

6.3.2 Activation data protection

The activation data of the service and CA keys comprises two secrets, with authorized employees knowing one each. Only authorized employees can access the activation data.

The subject is responsible for protecting his or her authentication means.

6.3.3 Other aspects of activation data

No stipulation.

6.4 Computer security controls

6.4.1 Specific computer security technical requirements

IDnow Trust Services AB ensures that the TSP's system components are secure and correctly operated with an acceptable risk of failure.

The following computer security functions are provided by the operating system, or through a combination of operating system, software, and physical safeguards. The TSP's components include the following security mechanisms:

- Require authenticated logins for trusted role;
- Provide discretionary access control with least privilege;
- Provide security audit capability (protected in integrity);
- Require use of strong password policy;
- Require use of cryptography for session communication;
- Provide controls for malicious code protection;
- Provide means to maintain software and firmware integrity and up to date;

- For accounts capable of directly causing certificate issuance, Issuing CA shall enforce multifactor authentication.

Only system administrators can access the server system and always through encrypted connections. All accesses are personalized and protected by multifactor authentication.

6.4.2 Computer security rating

No stipulation.

6.5 Life Cycle Security Controls

6.5.1 System development controls

The development of systems under the control of IDnow Trust Services AB is covered by an outsourcing agreement with IDnow GmbH. All development work is carried out by a subcontractor. In this scope, IDnow Trust Services AB ensures:

- supervision of the development process through participation in requirements analysis at every stage of the development project.
- provision of testing environments.
- supervision of the software acceptance process before deployment to production.

Furthermore, the control of cryptographic module creation includes requirements imposed on the design, manufacture, and delivery. The subcontractor does not define its own requirements in that matter. Hardware security modules are subjected to a specialized commissioning procedure.

All hardware will undergo inspection during the commissioning process to verify compliance with the supply specifications, ensuring that no evidence of tampering is detected.

6.5.2 Security management controls

Security controls are implemented within the information security policy of IDnow Trust Services AB to ensure the integrity of software and configurations, as well as the containment of fraudulent software..

Current configurations and changes of IDnow Trust Services AB systems are documented according to change management procedures.

6.5.3 Life cycle security controls

Policies, assets and practices for information security are regularly reviewed by a Chief Security Officer. The implemented controls are verified as part of the risk assessment procedure.

The security controls are evaluated by various methods, such as: penetration tests, configuration audits, internal audits.

6.6 Network Security Controls

IDnow Trust Services AB's networks are segmented as follows:

- High security zone (protected area of the certification authority including the key servers, certificate issuance servers) with no direct Internet access;
- Normal security zone based on ISO 27001 controls including:
  - operators workstations
  - administrators workstations
  - DMZ area with frontend systems

All systems contain malware scanners that run automatically in the background and are also automatically updated. IDnow Trust Services AB uses security gateways (firewalls) or if necessary appropriate additional solutions such as application firewalls, next generation firewalls, intrusion prevention,intrusion detection etc.

Security checks, such as vulnerability scans with subsequent evaluation and mitigation are carried out:

- at least once per quarter or
- on request by CA/Browser Forum or
- after any system or network changes that the CA determines as significant.

The vulnerability scans will be conducted by a specialized external company. In addition, IDnow Trust Services AB performs penetration tests through an external specialized company:

- at least once per year or
- on request by the CA/Browser Forum or
- after any system or network changes that the CA determines as significant.

All personal data that is transmitted between the Registration Authority and the Certificate Authority is encrypted via VPN and TLS. The network for the processing of CA's data is physically segregated from the office network.

The transfer of the data to the subject or subscriber is always encrypted (TLS, SFTP, S/MIME, etc.).

IDnow Trust Services AB ensures the secure operation of all technical systems by "hardening". This includes in particular:

- Removal of unnecessary software/services
- Removal of unnecessary accounts
- Modifying the configuration in regard to security
- Activation of additional security components
- Protection of network ports
- Regular software updates

The security of IDnow Trust Services AB's internal network and external connections is constantly monitored to detect any abnormal events.

Any changes in the configuration of network devices require the prior approval of the Chief Security Officer.

6.7 Time synchronization

All trust services components are regularly synchronized with a reliable time service. IDnow Trust Services AB uses NTP source clocks to establish the correct time for:

- Initial validity time of a CA Certificate.
- Revocation of a CA Certificate.
- Posting of CRL updates.
- Issuance of Subject end entity Certificates.

Clock adjustments are auditable events.

6.8 Time Stamping

IDnow Trust Services AB uses a qualified time-stamping service for archiving purposes.

IDnow Trust Services AB ensures regular reviews of its time-stamping service (status of QTSP and heartbeat) - at least every 24 hours.

7. Certificate and CRL Profiles

The scope related to this item is addressed in the Trust Service Policy.

8. Compliance Audit and Other Assessment

Trust services provided by IDnow Trust Services AB are audited for compliance with the practices outlined in this document and particularly with eIDAS regulation.

Audit results are part of the management information and are used to demonstrate compliance and improve the service.

8.1 Frequency or circumstances of assessment

The conformity of information systems, policies, practices, facilities, personnel and assets of IDnow Trust Services AB are assessed by a CAB pursuant to the eIDAS regulation, ETSI standards and relevant national law.

Conformity is assessed at least every 2 years and when any major change is made to Trust Service operations. Changes in the manner of service delivery are made in consultation with the CAB and appropriate supervisory body.

IDnow Trust Services AB has appointed system auditor who conducts internal reviews and audits in accordance with its audit program.

8.2 Qualification of auditors

External audits are conducted by a Conformity Assessment Body (CAB) accredited according to ISO/IEC 17065, as outlined by ETSI EN 319 403, with a focus on meeting the requirements specified in the eIDAS Regulation (EU) No 910/2014. The CAB is authorized to perform conformity assessments of Qualified Trust Service Providers and their services.

The internal audit is performed by IDnow employees with the necessary experience and qualification related to public key infrastructures, secure operation of information technology systems and information security in general.

8.3 Auditor’s relationship with IDnow Trust Services AB

IDnow Trust Services AB has chosen an auditor who is entirely independent from the organization.

8.4 Audit scope

The CAB audits all parts of the information system used to provide Trust Services.

The audit by the Conformity Assessment Body covers the entire IDnow Trust Services AB operations for the provision of qualified certification services under consideration of all standard and standardization documents related to the Regulation (EU) No 910/2014:

- documentation;
- archives;
- information data related to the issuance and management of qualified certificates;
- physical and information security and reliability of the technological system and management;

The scope of internal audits includes:

- verification of the TSP’s activity and its compliance with the Trust Service Policy and Certification Practice Statement;
- comparison of the practices and procedures outlined in this document with their practical implementation during operation;
- verification of the processes performed by the Registration Authority;
- other areas, facts and activities related to the IDnow Trust Services AB infrastructure.

8.5 Actions Taken as a Result of Deficiency

The reports of internal and external audits are submitted to the management board.

Where the CAB identifies deviations or non-compliance in the assessment, the Supervisory Body requires from TSP to remedy these to fulfil requirements within a time limit set by the Supervisory Body.

IDnow Trust Services aims for full compliance and timely correction of non-conformities. IDnow Trust Services AB management is responsible for implementing a corrective action plan.

IDnow Trust Services AB evaluates violations or instances of non-compliance and prioritizes necessary actions to address them. If any violations pertain to the protection of personal data, the Supervisory Body will inform the data protection authority.

8.6 Communication of results

The results of the performed internal and external audits are properly archived.

The certification document received by the Conformity Assessment Body may be published on IDnow Trust Services AB's website.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Trust Service Pricing

Specified in relevant Terms and Conditions or agreement with Subscriber.

9.1.2 Prices for revocation or status information

IDnow Trust Services AB does not charge a fee for qualified certificates revocation, publishing certificates in CRLs and making CRLs published in the repository (or elsewhere) accessible to relying parties.

9.1.3 Prices for other services

Fees for services can be specified in the Subscriber's or Relying Party's agreement.

9.1.4 Rules for cost refunds

IDnow Trust Services AB handles refund requests case-by-case.

9.2 Financial Responsibility

9.2.1 Insurance cover

IDnow Trust Services AB has the insurance policy which complies with the legal requirements in the countries where IDnow Trust Services AB operates, in particular Sweden and Germany. This includes compliance with Article 24 paragraph 2c of the eIDAS Regulation.

9.2.2 Other resources for maintaining operations and compensation for damage

According to relevant agreements IDnow Trust Services AB may give some additional warranties.

9.2.3 Insurance or warranty for end users

Refer to 9.2.1 Insurance cover.

9.3 Confidentiality of Business Information

9.3.1 Scope of confidential business data

IDnow Trust Services AB has implemented an information security policy with the main objective of ensuring the security of subscriber data. Specifically, all personal data is considered confidential. Any information not required to be public by law, regulation, or applicable standards is also treated as confidential.

9.3.2 Business data not treated as confidential

Any information not listed as confidential or intended for internal use is public information. Information considered public is listed in clause 2.2 of this document.

Additionally, non-personalized statistical data about IDnow Trust Services AB's services is also considered public information.

9.3.3 Responsibilities for the protection of confidential business data

IDnow Trust Services AB protect private information from being disclosed and available to third parties.

9.4 Privacy of Personal Information

IDnow Trust Services AB takes all the necessary measures so that personal data are protected and stored confidentially according to the European Regulation 679/2016 (GDPR).

The scope of personal information processed by IDnow Trust Services AB, along with the processing conditions and the rights of the data subjects, are detailed in the GDPR Policy of IDnow Trust Services AB. Before entering into an agreement with IDnow Trust Services AB, subscribers and subjects have the opportunity to review the rules outlined in the GDPR Policy.

9.5 Intellectual Property Rights

The trust services operated by IDnow Trust Services AB belong to it. All trademarks, patents, brand marks, licenses, graphic marks, etc., used by IDnow Trust Services AB are intellectual property of their legal owners.

9.6 Representations and Warranties

9.6.1 CA obligations

IDnow Trust Services AB does guarantee that it:

- provides its services consistently with the requirements and the procedures defined in this Practice Statement and in accordance with the policies under which this Practice Statement is established
- provides services in compliance with eIDAS regulation and related legal acts and standards
- maintains a publicly available repository of relevant documents and information.
- adheres to and implements the procedures outlined in this document.
- issues certificates containing accurate data at the time of the registration
- ensures that certificates do not contain any mistakes resulting from negligence or procedural violations by individuals confirming applications for certificate issuance or issuing certificates
- does not copy or store private keys of its subject outside of HSM devices
- protects the integrity and confidentiality of personal data
- informs the Conformity Assessment Body and National Supervisory Body of any changes to a public key used for the provided Trust Services.
- notifies the Supervisory Body within 24 hours of becoming aware of any security breaches or loss of integrity that significantly impacts the Trust Service provided
- notifies the Swedish Authority for Privacy Protection within 72 hours of initial discovery of any personal data breaches
- informs affected natural or legal persons without undue delay if a breach of security, loss of integrity, or personal data breach is likely to adversely affect them.
- preserve all documentation, records and logs related to Trust Services as outlined in chapter 5.4 and 5.5.
- maintains the financial stability and resources necessary to operate in accordance with this Practice Statement.
- hires employees with the knowledge, qualifications and experience appropriate for providing trust services.

IDnow Trust Services AB further warrants that it has documented agreements with its subcontracting and outsourcing partners. These contracts include defined liabilities and ensure that partners are bound to compliance.

9.6.2 Registration Authorities obligations and warranties

The Registration Authority is an outsourced service provisioned by IDnow GmbH, which is certified against ETSI EN 319 411-1/2 and ETSI TS 119 461 standards.

IDnow Trust Services AB ensures the accuracy of IDnow GmbH's policies in provisioning initial identity validation for the issuance of qualified certificates.

The outsourcing agreement in this regard specifically includes obligations regarding the confidentiality of processed information, including personal data, and imposes responsibilities for the processing, storage, archival and destruction of data.

9.6.3 Time Stamp Authority obligations and warranties

IDnow Trust Services AB guarantees the following:

- utilization of technology, operational procedures, and security management procedures to prevent any possibility of manipulating time.
- application of at least the parameters of cryptographic algorithms as specified in document ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites for providing trust services.
- specification of at least one hash function algorithm that may be used to compute the hash value of data subject to timestamping.
- provision of UTC time in the electronic timestamp token with an accuracy of up to 1 second.
- uninterrupted access (24/7/365) to support services, with accessibility and accuracy guaranteed even if multiple users are simultaneously associated with the application, excluding technical maintenance times.
- issuance of Timestamp Tokens in accordance with ETSI EN 319 422 Time-stamping protocol and time-stamp profiles.

The detailed conditions of the timestamping service re addressed in the Trust Service Policy for Qualified Time Stamp Service.

9.6.4 Subjects and Subscribers’ obligations and warranties

Subject and Subscriber are obliged to the following:

- complying with the terms and conditions of the trust services provided by IDnow Trust Services AB.
- providing truthful data in applications submitted to the registration authority.
- immediately informing IDnow Trust Services AB about any errors, defects, or changes in the certificate.
- protecting the credentials necessary for the use of IDnow Trust Services AB services and for signature creation against misuse, loss, disclosure, manipulation, or unauthorized use; neither communicating nor disclosing them to third parties, and maintaining sole control of them.
- no use of revoked or expired certificates.
- halting the use of IDnow Trust Services AB services as soon as they become aware that the IDnow Trust Services AB system has been compromised.
- initiating revocation in the case of a potential or actual security violation (or suspicion of a security violation) regarding their private keys.
- using qualified certificates and the corresponding private keys only for the purposes stated in the certificate and in accordance with the aims and restrictions stated in the Practice Statement and Trust Service Policy.

Subject shall be solely responsible for the maintenance of his/her private key and certificates.

9.6.5 Relying Party Obligations and warranties

If the Relying party verifies qualified signatures or qualified seals, it is obligated to use compliant software or services following subsequent requirements:

- verify if the certificate that supports the given signature or seal was qualified and and issued according to the present document;
- verify if a qualified IDnow Trust Services AB trust service issued the qualified certificate and if the certificate was valid at the time of signing;
- verify if the signature validation data corresponds to the data provided to the relying party;
- verify if the integrity of the signed data has not been compromised.

The relying party must protect the private data of the subject included in the certificate.

The relying party should refrain from using unknown or unprotected systems provided by a third party for validation.

9.6.6 Representations and warranties of other participants

No stipulation.

9.7 Warranty Disclaimer

IDnow Trust Services AB:

- is liable for the performance of all its obligations specified in clause 9.6.1 to the extent prescribed by the legislation of Sweden.
- has a compulsory insurance policy and maintains relevant contracts with suppliers providing liability compensation

IDnow Trust Services AB is not liable for:

- damages resulting from Subscriber private keys not being kept secret
- Any errors in checking certificates on the part of Relying parties;
- the non-performance of its obligations if such non-performance is due to faults or security problems of the Supervisory Body, the Swedish Data Protection Authority, Trusted List or any other public authority;
- Non performance according to this Practice Statement by Force Majeure;

9.8 Limitations of Liability

The limits of liability claims arising from this document are established in the insurance policy that can be requested by email from support@trust-services.io.

9.9 Indemnities

Indemnities between the Subscriber and IDnow Trust Services AB are regulated in Subscriber agreements.

9.10 Amendments

9.10.1 Procedure for amendment

This Practice Statement is reviewed at least annually and may be reviewed more frequently. All changes are reviewed and approved by the IDnow Trust Services AB Board before being made public. Changes to this Practice Statement are indicated by appropriate versioning.

IDnow Trust Services AB will post a notice on its website of any major or significant changes to this Practice Statement, as well as any appropriate period by which the revised Practice Statement is deemed to be accepted.

9.10.2 Notification mechanism and comment period

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

After notifications in advance, affected parties may submit comments on suggested modifications within 14 working days of their announcement. Modification proposals may be submitted via regular mail or electronic mail to the contact addresses of IDnow Trust Services AB. The proposals should include descriptions of the modifications, their scope, justifications, and contact details of the sender.

The only items not requiring notifications in advance include amendments resulting from the implementation of editorial modifications, changes to the contact information of the person responsible for document management, and changes that do not have a significant impact on a considerable group of individuals.

9.10.3 Circumstances under which OID must be changed

No stipulation

9.11 Dispute Resolution Procedures

All disputes between the parties will be settled by negotiations. If parties fail to reach an amicable contract, the dispute will be resolved at the court of the location of IDnow Trust Services AB or another court specified in the agreement.

The Subscriber or other party can submit their claim or complaint on the following email: info@trust-services.io.

9.12 Governing Law

This Practice Statement is governed by the jurisdiction of the European Union and Sweden.

9.13 Complaince with applicable law

The set of legal acts with which IDnow Trust Services AB declares compliance is indicated in chapter 1.

9.14 Miscellaneous provisions

9.14.1 Entire contract

IDnow Trust Services AB mandates that each Registration Authority (RA) and other participants comply with this Practice Statement through contractual obligations.

IDnow Trust Services AB also requires each party using its products and services to enter into an agreement that delineates the associated terms and conditions.

9.14.2 Assignment

Any entities operating under this Practice Statement may not assign their rights or obligations without the prior written consent of IDnow Trust Services AB. Unless specified otherwise in a contract with a party, IDnow Trust Services AB does not provide notice of assignment.

9.14.3 Severability

If any provision of this document is held invalid or unenforceable by a competent court or tribunal, the remainder of the document remains valid and enforceable. Each provision that limits liability, disclaims warranties, or excludes damages is severable and independent from any other provision.

9.14.4 Enforcment

Any waiver or lack of immediate implementation of any right under this document does not create a continuing waiver of such right or authorize an expectation of withdrawal from its implementation.

9.14.5 Force Majeure

IDnow Trust Services AB and other parties cannot be held responsible for any consequences caused by circumstances beyond a reasonable control, including but without limitation to

- war,
- acts of government or the European Union,
- export or import prohibitions,
- breakdown or general unavailability of public telecommunications networks and logistics infrastructure,
- general shortages of energy, fire, explosions, accidents, strikes or other concerted actions of workmen, lockouts, sabotage, civil commotion and riots.

Communication and performance in the case of Force Majeure are regulated between the parties with the contracts.

Non-fulfilment of the obligations arising from this document and/or relevant service-related Policies is not considered a violation if such non-fulfilment is occasioned by Force Majeure

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 unforgeable 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 Practice Statement 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. (present document)

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
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] ETSI TS 119 412-1**
- **[Ref. 23] ETSI EN 319 412-4 standard**

- **[Ref. 24]** [RFC 5280]: RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- **[Ref. 25]** [RFC 6818]: RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

IDnow Trust Services AB
Box 16285
103 25 Stockholm
Sweden

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