ZealiD AB		Document name ZealiD TSA Practice Statement TSA PS		
Owner CEO	Class P	Category Steering	Date 2022-08-01	Revision 1

ZealiD TSA Practice Statement

Table of Contents

Revision History

Date	Revision	Comment	Contributor
2022-08-01	01	Initial practice statement	Tomas Zuoza

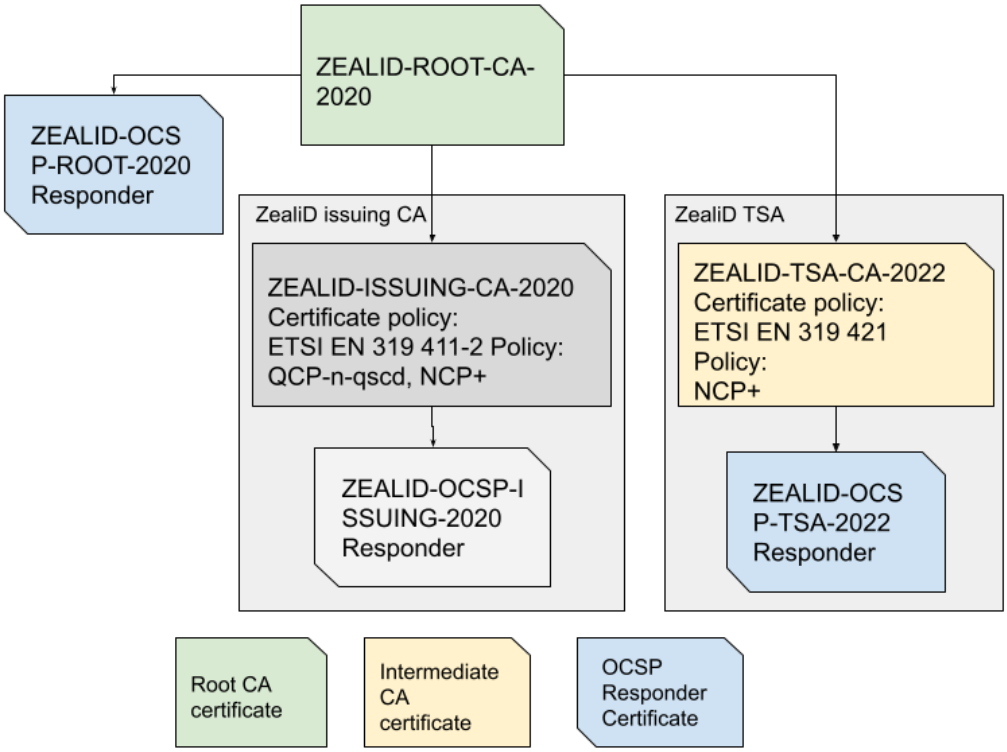
1. INTRODUCTION

ZealiD AB, SE556972-4288, (ZealiD) was founded in 2014. It is a Swedish limited liability company (Aktiebolag) held privately by private individuals, Collector Bank, NFT Ventures, Arbona Growth, J12 Ventures and Almi Invest. ZealiD is under the supervision of The Swedish Post and Telecom Authority (PTS) and the Swedish Data Protection Agency (IMY - Integritetsskyddsmyndigheten). The principal activities of ZealiD are offering trust services and related technical solutions to the global regulated industries with a focus on the European Union.

1.1. Overview

This TSAPS applies to ZealiD services for issuing Timestamps. Timestamps can be used in support of digital signature or for any implication that requires proof that a signature was created before a particular time. ZealiD uses it's own qualified timestamps to provision the highest level qualified signing. Each ZealiD qualified electronic signature includes a ZealiD qualified time stamp.

The certificate hierarchy is visually depicted below. ZealiD uses a common rootCA to issue and certify a ZealiD TSA CA keys. The TSA CA is then used to generate and certify a TSU key that is used to sign ZealiD TSTs.



1.2. Document name and identification

This TSAPS is titled “ZealiD TSA Practice Statement”. The Issuing TSAPS has the object identifier: OID 1.2.752.251.1.5.1.4.1.

1.3. Policy administration

1.3.1. Organization administering the document

This TSAPS is administered by ZealiD:

ZealiD AB
Registry code SE5569724288
Box 3437
111 56 Stockholm
Visiting Address: Norrlandsgatan 10

Head Office: +46 (0)10-199 40 00
Email: info@zealid.com
https://www.zealid.com

1.3.2. Contact person

Compliance Manager
Email: legal@zealid.com

1.3.3. Person determining TSAPS suitability for the policy

Compliance Manager determines suitability. Compliance Manager is responsible to review and propose updates to the TSAPS such that it is reviewed regularly, updated at least once per year or more frequently should regulatory changes arise as per section 1.3.4 of this TSAPS.

1.3.4. TSAPS approval procedures

The ZealiD Management Board, led by the CEO, is responsible for the trust service.

All TSAPS versions are subject to final confirmation and approval by the ZealiD Management Board and the amended TSAPS is enforced by the CEO and the Management Board. The practices defined within the TSAPS shall be implemented by the Management Board.

Spelling corrections, translation activities and contact details updates are documented in the version table of this TSAPS.

In case of substantial changes, a new TSAPS version is clearly distinguishable from previous ones.

The amended TSAPS along with the enforcement date, which cannot be earlier than 14 days after publication, is published electronically on the ZealiD website repository as well as communicated internally.

ZealiD publishes to its publicly available repository (24/7, 99% annual availability, which is contractually guaranteed by the hosting provider and provisions are made to be able to host via secondary provider in case of emergency).

2. References

The following documents contain provisions which are relevant to the ZealiD TSAPS:

[eIDAS regulation] 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;

[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 (General Data Protection Regulation) (Text with EEA relevance);

[ETSI EN 319 421] ETSI EN 319 421 V1.1.1 (2016-03) “Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps”;

[ETSI EN 319 422] ETSI EN 319 422 V1.1.1 (2016-03) “Electronic Signatures and Infrastructures (ESI);Time-stamping protocol and time-stamp token profiles;

[RFC 3161] IETF RFC 3161: “Internet X.509 Public Key Infrastructure Time-stamp Protocol (TSP)”.

[ZealiD CPS] ZealiD AB QeID Service Practice Statement.

3. Definitions and acronyms

3.1. Definitions

Term	Definition
Coordinated Universal Time	The time scale based on the second as defined in ITU-R Recommendation TF.460-6 (02/2002).

Certification Practice Statement	One of the several documents that all together form the governance framework in which Certificates are created, issued, managed, and used.
CA Service	Trust service related to issuing Certificates, managing suspension, termination of suspension, revocation, modification and re-key of the Certificates. In this TSAPS the CA Service is called ZealiD QeID Service.
Conformity Assessment Body (CAB) / Certification Body	Official registered or accredited certification body that can assess and certify Trust Services
Network TIme Protocol (NTP)	Protocol to synchronize system clocks among a set of distributed time servers and clients as defined in RFC 5905.
Object Identifier	An identifier used to uniquely name an object (OID).
Relying Party	Entity that relies on the information contained within a Certificate or a Time Stamp. Relying parties are sometimes referred to as Customers.
Registration Authority	Entity that is responsible for identification and Authentication of Subjects of Certificates. Additionally, the Registration Authority may accept Certificate applications, check the applications and/or forward the applications to the Certificate Authority.
Secure Cryptographic Device	Device which holds the Private Key of the user, protects this key against compromise and performs signing or decryption functions on behalf of the user.
Subscriber	A natural person to whom the CA Service issue certificates and key as a service if he/she has requested it.
Subject	In this document, the Subject is the same as the Subscriber.

Terms and Conditions	Document that describes the obligations and responsibilities of the Subscriber with respect to using Time Stamping Authority Service. The Subscriber has to be familiar with the document and accept the Terms and Conditions upon usage of the Qualified Time Stamping Services.
Time-Stamping Authority	Entity that issues Time-Stamping tokens.
TSA Practice Statement (TSAPS)	One of the several documents that all together form the governance framework in which time-stamps are created, issued, managed, and used.
Time-Stamping Token (TST)	the data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time
Time-Stamping Unit (TSU)	A set of hardware and software which is managed as a unit and has a single private time-stamp signing key active at a time.
ZealiD	ZealiD AB, the legal entity and provider behind the Trust Service and CA Service; the brand name used facing users, customers, relying parties and the market in general.
ZealiD App	The brand name used facing consumers, customers, relying parties and the market in general. Mobile application the Subscriber is using for registration with the services and for applying and authenticating for the issuance of certificates (using the QeID service) and time-stamps (using the TRA service),
ZealiD QeID Service	The specific name of the CA Service issuing qualified electronic signatures.
ZealiD TSA Service	Trust service related to issuing qualified time stamps for ZealiD signatures.

3.2. Acronyms

Acronym	Definition
UTC	Coordinated Universal Time
CA	Certificate Authority
CAB	Conformity Assessment Body (eIDAS)
CP	Certificate Policy
TSAPS	TIme-Stamping Authority Practice Statement
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
ISMS	Information Security Management System (also sometimes referred to as “Management System”)
OCSP	Online Certificate Status Protocol
OID	Object Identifier, a unique object identification code
PKI	Public Key Infrastructure
PTS	Swedish Post & Telecom Authority
RA	Registration Authority
SB	Supervisory Body (eIDAS) - see PTS
TRA Service	Trusted Registration Authority Service provided by ZealiD under the brand name ZealiD
TSA Service	Time Stamping Authority Service provided by ZealiD under the brand name ZealiD

Refer to ZealID QeiD Certificate Practice Statement for additional definitions.

4. GENERAL CONCEPTS

4.1. General Policy Requirement Concepts

This policy references ETSI EN 319 401 for generic policy requirements. These policy requirements are based upon the use of public key cryptography, public key certificates and reliable time sources.

4.2. Time Stamping Services

ZealiD takes overall responsibility for the provision of the time stamping services, which include the following components:

- Time stamping provision: the service component that generates TSTs;
- Time stamping management: the service component that monitors and controls the operation of the time stamping services to ensure that the service provided is as specified in this ZealiD TSAPS.

ZealiD TSA adheres to the standards and regulations in section 2 of this document to keep trustworthiness of the time stamping service for Subscribers and Relying Parties.

4.3. Time Stamping Authority

ZealiD TSA is trusted by the users (i.e. Subscribers as well as Relying Parties) to issue TSTs. ZealiD TSA has overall responsibility for the provision of the time stamping services identified in section 5.2 as well as the responsibility for the operation of TSU that creates and signs on behalf of the TSA.

ZealiD TSA may operate several identifiable TSUs. TSU issuing qualified time stamps according to eIDAS Regulation, shall not issue non-qualified time stamps.

Currently ZealiD TSA is not operating any other TSU. ZealiD TSA issues only qualified time stamps.

ZealiD TSA operated one TSU which is identified in the TSU certificate used to sign TST. TSU certificates are available at ZealiD Repository: https://www.zealid.com/en/repository

4.4. TSA Subscriber

Subscribers identified in this TSAPS are natural persons within the scope of their electronic identity.

4.5. TSA Relying Party

Relying parties are defined as any Subscriber (as defined in Subscribers above) or any end-entity (also referred to as Customers) relying on the certificate issued by the ZealiD Time Stamping Authority.

4.6. Time Stamping Policy and TSA Practice Statement

ZealiD TSA Time stamping Policy is based on the Time stamping Policy specified in ETSI EN 319 421 and is applied to TSAs issuing TSTs.

This ZealiD TSA Practice Statement is a form of trust service practice statement as specified in ETSI EN 319 401 applicable to ZealiD TSA issuing TSTs.

5. TIME STAMPING POLICIES

5.1. General

ZealiD TSA issues the TSTs in accordance with ETSI EN 319 421 best practices time-stamp policy (BTSP).

The TSTs are issued with an accuracy of 1 second of UTC or better.

5.2. Identification

OID for BTSP: a best practices policy for time-stamping:

OID: 0.4.0.2023.1.1
itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy (1)

This OID is referenced in every TST issued by ZealiD.

6. POLICIES AND PRACTICES

6.1. Risk Assessment

ZealiD performs risk assessment regularly in order to evaluate business risks, IT risks and risks related to the TIme Stamping Authority functions. This includes identification of foreseeable risks that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Time stamp data or Time Stamp management processes; assessment of the likelihood and potential damage, as well as sufficiency of the security management, procedural controls, physical facilities and determination of the necessary security requirements and operational procedures.

ZealiD Management Board approves risk assessment, oversees risk mitigation and accepts any residual risks.

6.2. Trust Service Practice Statement

The ZealiD Management Board, led by the CEO, is responsible for the trust service.

All TSAPS versions are subject to final confirmation and approval by the ZealiD Management Board and the amended TSAPS is enforced by the CEO and the Management Board. The practices defined within the TSAPS shall be implemented by the Management Board.

Spelling corrections, translation activities and contact details updates are documented in the version table of this TSAPS.

In case of substantial changes, a new TSAPS version is clearly distinguishable from previous ones.

The amended TSAPS along with the enforcement date, which cannot be earlier than 14 days after publication, is published electronically on the ZealiD website repository as well as communicated internally.

ZealiD, as TSA, shall develop, implement, enforce and update this document containing the TSA Practice Statement to meet the requirements of its Time-Stamping policy.

All procedures and their correct implementation are audited annually by an independent external entity.

ZealiD makes the following documents publicly available:

- TSA Practice Statement (this TSAPS)
- Audit results
- Insurance policies
- TSA CA & TSU Certificates
- TSA CA & TSU Test Certificates
- Profiles
- Terms and Conditions ZealiD TSA Service
- Online Certificate Status Protocol

ZealiD issuingCA certificates shall be published on the national Trusted List upon receiving notification from the Supervisory Body and the EU publishes the List of the Trusted Lists (LOTL).

Time stamping token information:

Version: 1
Policy OID: 0.4.0.2023.1.1
Hash Algorithm: sha256 with RSA encryption

Key usage purposes:

TSA CA Key usage:

- keyCertSign
- keyCrlSign

TSU Key usage:

- digitalSignature
- timeStamping

OCSP Key usage:

- digitalSignature
- nonRepudiation
- ocspSigning

Key usage purposes & hashing algorithms:

TSA CA keys are RSA 4096 and uses sha384 hashing algorithm to sign OCSP keys.
TSA CA keys are RSA 4096 and uses sha256 hashing algorithm to sign TSU keys.
TSA OCSP keys are RSA 4096 and uses sha384 hashing algorithm to sign OCSP Responses.
TSU keys are RSA 4096 and uses sha256 hashing algorithm to sign TSTs.

6.3. Terms and Conditions

The published Terms and conditions contain further information about limitations of the Service, Subscriber's obligations, information for relying parties or limitations of liability, among others.
Terms and conditions are distributed on ZealiD public website (https://zealid.com/en/repository).

6.4. Information Security Policy

ZealiD implements an information security policy which all employees must adhere to. The information security policy is reviewed on a regular basis and when significant changes occur. Policy shall be approved by the Management Board.

6.5. TSA Obligations

ZealiD is a TRA participant in a trust relationship between TSA, Subscribers, Customers and Relying parties. This TSAPS shall form the basis of such a relationship with the following presentations and warranties from ZealiD.

ZealiD shall:

- provide its services consistent with the requirements and the procedures defined in this TSAPS and according to the policies under which this TSAPS is created.
- be responsible for the effective compliance with the procedures set forth in this TSAPS.
- provide the service in compliance with eIDAS regulation and related legal acts and standards.
- provide publicly published repositories with high electronic availability of all practice statements mentioned in this TSAPS.
- honour its part in Subscriber Terms and Conditions and secure Subscriber availability and access to the services set out in this TSAPS.
- protect the integrity and confidentiality of personal data and information acquired as part of service provisioning and not subject to publication.
- within 24 hours after having become aware of it, notify the Supervisory Body of any breach of security or loss of integrity that has a significant impact on the Trust Service provided.
- within 24 hours after initial discovery, notify the Swedish Authority for Privacy Protection (Integritetsskyddsmyndigheten) of any personal data breach.
- where the breach of security or loss of integrity or personal data breach is likely to adversely affect a natural or legal person to whom the Trusted Service has been provided, notify the natural or legal person of the breach without undue delay.
- in case of major compromise of the TSA operation or loss of calibration, shall make available to all Subscribers and Relying parties a description of the incident. Such description shall provide information that allows identifying the time-stamps which may have been affected, unless this breaches the privacy of the TSA Users or the security of the TSA Service.
- preserve all the documentation, records and logs related to Trust Services according to the sections 7.6.1 and 7.8.5.
- ensure a conformity assessment with a CAB on a recurring basis according to requirements.

- present the conclusions of the CAB to the Supervisory Body to ensure continual status of Trust Services in the Trusted List;
- have the financial stability and resources required to operate in conformity with this TSAPS.
- publish the terms of the compulsory Insurance Policy and the conclusion of CAB in the ZealiD online repository.
- secure that ZealiD employees do not have criminal records of intentional crime.

ZealiD further warrants that it has documented contracts with its subcontracting and outsourcing partners.

ZealiD has defined in these contracts liabilities and ensured that partners are bound to implement any requirements and controls required by ZealiD.

ZealiD has located its primary systems within two different secured facilities of a contracted hosting providers. ZealiD has ensured that those hosting providers meet relevant ZealiD requirements set forth in this TSAPS, in specific contractually adhere to requirements set forth in sections:

- Facility, Management and Operational Controls 7.7 - 7.8
- Personal Control 7.2.2 - 7.2.3
- Network security controls 7.8.3
- Audit 7.10

ZealiD places great effort into offering all potential service users, especially people with disabilities, the opportunity to access the TSA Service.

By opting for a smartphone application user interface ZealiD achieves specific accessibility benefits such as options for Subscribers and Subscriber applicants to:

1. Invert Colors;
2. Use Magnifier;
3. Select larger text sizes;
4. Zoom;
5. Shake to undo;

6. Subtitles and captioning;
7. Voice Control.

Options 1-4, 6 and 7 can also be accessed when using ZealiD repositories and sites on desktop web.

It is provided by ZealiD on an equal basis. ZealiD accepts that its services imply at least some sort of qualitative capabilities and legal capacity, but nonetheless truly aspires to provide trust services and related technical solutions in a nondiscriminating way.

6.6. TSA Subscriber Obligations

The Subscriber shall:

- Use all Trust Services in his/her name with correct and complete information in the application for the services;
- Where data submitted has changed, notify any and all corrections and amendments to the data in accordance terms & conditions and this TSAPS;
- Note that intentionally presented false, incorrect or incomplete information will lead to denial of application and may lead to a police report;

  The Subscriber shall use time-stamps in accordance with this TSAPS and service Terms and Conditions.

6.7. TSA Relying Party Obligations

A Relying Party shall:

- Review and observe the documentation, risks and liabilities related to the acceptance of the certificates and time stamps. The risks and liabilities have been set out in this TSAPS, and in the service Terms and Conditions.
- Review and observe all necessary means and methods of integration and data communication as set forth under developer.zealid.com.

- Verify the validity of certificates on the basis of validation services offered by ZealiD using the prescribed methods of data communication with appropriate cryptographic information.

6.8. Liability

ZealiD:

- is liable for the delivery of all its obligations specified in section 6.5. to the extent prescribed by Swedish law;
- maintains adequate insurance coverage and contracts covering ZealiD Trust Services and providing liability compensation.

ZealiD is not liable for:

- Non performance according to this TSAPS by Force Majeure;
- Loss of the proof value of validity confirmation due to Force Majeure.
- Any errors in checking certificates on the part of Relying parties;
- Any mistakes in the verification of the validity of Time Stamps.
- Any non-performance where this is due to mistakes made by the Supervisory Body, the Authority for Privacy Protection or any other public authority or Trusted List.

6.8.1. Limitations of liability
The limits of liability claims arising from this TSAPS are established in the insurance policy and can be found at https://www.zealid.com/repository.

6.8.2. Indemnities
Indemnities between the Subscriber and ZealiD are regulated in service based Terms and Conditions ZealiD TSA.

7. TSA MANAGEMENT AND OPERATION

7.1. Introduction

ZealiD applies various policies and procedures to ensure the trustworthiness of the timestamping service.

ZealiD TSA implements all practices described in the latter section.

7.2. Internal Organization

The TSA is provided by ZealiD. ZealiD implements information security practices, including personnel security, access controls, risk assessment, as appropriate for the timestamping services.

ZealiD organisational structure, role set-up, personnel hiring and management policies, routines and controls ensure ZealiD compliance to the regulations and standards binding for the provision of Time Stamping Services as referred in Chapter 2 of the TSAPS.

7.2.1. Personnel Security

ZealiD implements personnel security policies and procedures to ensure that employees and contractors support the trustworthiness of the TSPs service. In particular:

- ZealiD employs staff and, if applicable, subcontractors, who possess the necessary expertise, reliability, experience, and qualifications and who have received training regarding security and personal data protection rules as appropriate for the offered services and the job function.
- Trusted roles, on which the security of the operations depends, are clearly identified. Personnel exercises administrative and management procedures and processes that are in line with information security management procedures.

7.2.2. Procedural controls

Procedural controls are documented in ZealiDs internal routines. ZealiD personnel exercise administrative and management procedures and processes that are in line with the TSP's information security management procedures.

Personnel are provided training and all personnel are qualified according to knowledge and experience with respect to the trust service that is provided. Personnel competence is regularly assessed.

Managerial personnel have familiarity with security procedures for personnel, security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.

Access to ZealiD systems is periodically reviewed by the CTO.

Inventorying is conducted when there is a new hire or termination.

7.2.2.1. Trusted roles

ZealiD has established and documented necessary Trusted roles to run the TSA Service.

ZealiD Management Board appoints Trusted roles and appointees accept the role responsibilities as part of their role.

Defined roles
Security Officers: Overall responsibility for administering the implementation of the security practices.
System Administrators: Authorized to install, configure and maintain the TSP's trustworthy systems for service management.
System Operators: Responsible for operating the TSP's trustworthy systems on a day-to-day basis. Authorized to perform system backup. Personnel holding smart cards to unlock Master Key for operations.
System Auditors: Authorized to view archives and audit logs of the TSP's trustworthy systems.
Compliance Manager: Manages Compliance, Information Security including Risk Management and some aspects of Quality.
Incident Manager: Manages the process to restore normal service operation according to ZealiD's full information security policy as quickly as possible so as to minimize the impact to business operations.

ZealiD has several System Administrators with internal regulation.

The assignment is made person by person with a decree of the Management Board. See this section above for the details.

Employees in the Trusted Roles have job descriptions that define the functions and responsibilities related to the Trusted Role.

ZealiD ensures that personnel have achieved trusted status, and departmental approval is given before such personnel are:

- Issued access devices and granted access to the required facilities; or
- Issued electronic credentials to access and perform specific functions on ZealiD or other IT systems.

Operations of the TSA Service are managed by ZealiD personnel in Trusted Roles, but may actually be performed by a non-specialist, operational personnel (under supervision), as defined within ZealiD Routine Roles and Responsibilities.

All requirements and rules for or concerning personnel in Trusted Roles apply equally to personnel with the temporary or permanent employment contract.

7.2.2.2. Number of persons required per task

ZealiD has established, maintains and enforces monitoring and review procedures to ensure segregation of duties based on job responsibility and to ensure that multiple persons holding Trusted Roles are required to perform sensitive tasks.

7.2.2.3. Identification and authentication for each role

All Trusted Roles are performed by personnel qualified and assigned to this role by the Management Board. Proof-of-identity is performed by checking an official national ID (all staff). All identity checks are performed face-to-face as part of the initial New Personnel Registration process.

ZealiD has implemented an access control system, which identifies users and registers all ZealiD information system users. New personnel are

provided minimum access to email, chat and project management tools. User accounts with elevated privileges are created for personnel in specific roles that need access to the system in question.

Any access requires users to log in with their personal account. To access administrative commands explicit permission is necessary and auditing of the execution takes place.

ZealiD employs file system permissions to prevent misuse.

User accounts are locked as soon as possible when the role change dictates. Access logs and rules are audited on an ongoing basis and are combined with automated issuing alarms in case of abnormal suspicious activities.

7.2.2.4. Roles requiring separation of duties

Trusted Roles are separated and are staffed by different persons.

7.2.3. Personnel controls

7.2.3.1. Qualifications, experience, and clearance requirements

ZealiD executes structured hiring, qualification and continuous training process according to its policies and routines.

ZealiD line managers qualify personnel for each role according to its Routine Personnel Management. The controls apply for all types of personnel, such as employees, consultants, contractors or others.

ZealiD staff are provided relevant and timely training and have the experience and competence required to carry out the duties specified in role descriptions and employment contracts.

ZealiD ISMS defines a structured hiring process and continuous training process in the operational and security procedures.

ZealiD employees are required to:

- Demonstrate that they have not been convicted of intentional crime;
- Adhere to confidentiality clauses as part of their employment;
- Remain neutral with regards to financial or commercial interests that could constitute liabilities for personnel or ZealiD ("conflict of interest").

Employees in Line Management and Trusted Roles are further required to:

- Remain neutral and objective with regards to any interests conflicting with Trust Services operations.

Where ZealiD is a Trust Service Provider or is an RA certified by a Conformity Assessment Body, personnel in Trusted Roles are obliged to follow all required procedures without exceptions as defined in practice statements.

7.2.3.2. Background check procedures

ZealiD conducts the following procedures according to its Routine Personnel Management:

- Identity verification;
- Reference taking from previous employers;
- Background checks as far as legally permitted in respective jurisdictions.

ZealiD background checks are proportional to the level of information and security risks involved in the roles.

Background checks are conducted on all candidates for employment and trusted sub contractors performing the Trust Service providing operations with access to production data. Checks are updated periodically with dedicated questionnaires.

7.2.3.3. Training requirements

In addition to strict requirements on competence and experience at the time of hiring, ZealiD employees undergo regular training. It is key that all personnel have adequate training and necessary experience for the duties specified in the role description and employment contract, and maintain the necessary competency over time. Training includes:

- ISMS including Information and IT-security Policies, Routines, Descriptions and Records;
- New, updated and/or altered duties and competencies required for specific roles;
- Personal Data Protection.

7.2.3.4. Retraining frequency and requirements

Refresher training is conducted at least once per year, but typically takes place when changes occur and with monthly training events.

Individual training is done according to Individual Development Plans. All personnel receive ongoing training on all ISMS topics.

An update on new threats and security practices is conducted every 12 months or when there are new substantial changes in the area.

7.2.3.5. Job rotation frequency and sequence

No stipulation.

7.2.3.6. Sanctions for unauthorized actions

Personnel are bound by contractual employment obligation to carry out their duties according to internal rules.

ZealiD has routines for disciplinary actions. Disciplinary actions for unauthorized actions may include warning, role change or termination depending on the severity of the unauthorized action. The actions in general follow local labour law stipulation on disciplinary actions.

7.2.3.7. Independent contractor requirements

ZealiD uses contractors in Trusted Roles. All contractors have documented contracts and follow routines set out in ZealiD's Routines for contractors. ZealiD delegates and defines the relevant requirements to the sub-contractor according to its role and tasks. The contractor is responsible for compliance with defined requirements and its personnel acting in Trusted Roles.

7.2.3.8. Documentation supplied to personnel

Personnel in Trusted Roles receive training and Trusted roles are documented and this documentation is provided as needed for the employee to perform job responsibilities.

7.3. Asset Management

ZealiD implements asset management policies and routines (including media handling) to ensure an appropriate level of protection of its assets including information assets.

An asset inventory is maintained, which includes all information assets and classification based on risk assessment.

7.4. Access Control

ZealiD implements access control management policies and procedures to ensure TSP system access shall be limited to authorized individuals.

Different security layers with respect to physical access and logical access ensure a secure operation of the timestamping service:

- Secured physical environment;
- Segregation of network segments;
- Segregation of duties;
- Firewalls;
- Network and Service Monitoring.

7.5. Cryptographic Controls

7.5.1. TSA Key Generation

7.5.1.1. TSA CA Key Generation

The signing keys of ZealiD TSA Service are created in accordance with the internal regulation of ZealiD: Protocol CA Key Ceremony. For the key ceremony of ZealiD TSA Service key pair generation for all issuing CA OCSP responders & TSU keys the commission is appointed by CEO with internal regulation. The number or commission members are limited to the bare minimum and consists of only trusted personnel. Procedure for ZealiD TSA Service key pair generation is carried out according to the detailed instructions created for the specific procedure. The creation of ZealiD TSA Service keys is observed by a commission, which after the creation of the keys draws up an appropriate deed containing the public key of the created pair of keys and the hash thereof.

The ZealiD TSA key pair generation, certification and the private key storage occur in the HSM, which is used for providing keys that at least meet the requirements established in the security standard ISO/IEC 15408, EAL 4+. The HSM protects the key from external compromise and operates in a physically secure environment. The hardware is located in a secure hosting center.

ZealiD has documented procedures for conducting ZealiD TSA Service key pair generation. Head of the commission creates a report proving that the ceremony was carried out in accordance with the stated procedure and that the integrity and confidentiality of the key pair was ensured. Report is signed by the commission members. The more detailed procedures for key ceremony, roles and responsibilities of participants during and after the procedure, requirements for report and collected evidence are defined in internal documentation of ZealiD.

3 years before before expiration of its TSA Service certificate, ZealiD generates a new TSA Service certificate for signing subject key pairs and apply all necessary actions - informing relying parties about the generation of the new certificate, switching new onboardings to the new

certificate and migrating existing user base to the new certificate over time, to avoid disruption of any operations that rely on the certificate and to allow all relying parties to become aware of key changeover. Common name of the TSA Service certificate always contains the number of the year in which it was created. The new TSA Service certificate is generated and distributed according to this practice statement.

7.5.1.2. TSU Key Generation

ZealiD TSU is using RSA key pair with 4096-bit modulus. This key pair is used only for signing TSTs.

TSU keys are generated using the HSM.

TSU key generation requires the presence of two System Operators and the Security Officer or System Auditor (minimum of 3 people).

ZealiD TSA and TSU keys are generated in HSMs certified according to EN 419 221-5 Common Criteria (ISO/IEC 15408), EAL 4+.

All cryptographic modules are associated with the same public key certificate.

7.5.2. TSU Private Key Protection

7.5.2.1. Key protection

The HSMs used by ZealiD TSA Service are certified according to Common Criteria (ISO/IEC 15408) using the Protection Profile CEN EN 419 221-5 (“Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services”).

ZealiD TSA Service verifies that HSM is not tampered physically after its installation, by checking the security seal.

ZealiD TSA Service verifies that HSM is functioning correctly during usage and retains it’s certification status.

The certified HSMs are operated according to their Certification Guidance Documentation.

The access to ZealiD MBK is divided into three parts that are secured by different persons in Trusted Roles. For actions with the private keys of ZealiD the presence of at least two authorized persons is required.

ZealiD TSA Private Keys (TSA CA, TSA OCSP and TSU) held in the HSM.

TSU private key is backed up and securely stored for the unlikely event of key loss due to unexpected power interruption of hardware failure. Key backup occurs as a part of key generation ceremony. Backed up private key remains secret and the integrity and authenticity is retained.

7.5.2.2. Key Backup

The private keys of the TSA are backed up to an encrypted physical media and stored off site.

Security Officer and a System Operator are required for configuration,

Security Officer and Backup/Restore Approval User for key backups.

7.5.2.3. Key Restoration

Restoration of the private key requires the presence of the Security Officer and a Backup/Restore Approval User for dual approval of configuration import.

The Backup/Restore Approval User is a temporary role during the restore process. It is created for one specific such task, and deleted right afterwards. The role is appointed and authorized by the Security Officer and the CTO. Due to its short-lived temporary character, the role authenticates by password.

At least two separate Master Backup Key smart cards are required if restoration is carried out in the new HSM.

7.5.2.4. Private key transfer into or from a cryptographic module

All ZealiD TSA Trust Service keys must be generated by and in the cryptographic module. ZealiD TSA Service generates Trust Service key pairs in the HSM in which the keys will be used.

Since redundant HSMs use the same MBK, such keys can be used on each of the HSM in the redundant group. Related data transfers are encrypted accordingly.

Restoration of the private key requires the presence of the Security Officer and a Backup/Restore Approval User.

7.5.3. TSU Public Key Certificate

TSU public keys are made available to Relying Parties in a public key certificate.

The certificate for TSU public key is issued by ZealiD TSA CA and is distributed on ZealiD public website (https://zealid.com/en/repository). Validity information is available in OCSP service reference located in the certificate.

When obtaining the TSA public key certificate, TSA verifies that the certificate has been correctly signed (including verification of the certificate chain to a trusted certification authority).

Only one certificate is issued to any specific TSU key. TSU certificates are not renewed.

ZealiD TSU does not issue any TST before the public key certificate is loaded into the TSU.

7.5.4. TSU Key Rekeying

TSU keys have the expected lifetime of 5 years. A certificate is issued for the whole expected lifetime.

Sufficient time before the expiration of the TSU certificate ZealiD TSA generates a new key for the TSU certificate. ZealiD informs Subscribers

and Relying Parties according to internal routines within a reasonable time about the activation of the new TSU certificate.

TSU key lifetime is limited by ZealiD TSA CA certificate validity. With a new TSA CA certificate, a new TSU key will be generated. TSU key validity shall not exceed it's own certificate validity.

7.5.5. End of TSU Key Life Cycle

ZealiD takes measures to permanently disable access to the TSU private keys after their expiry or revocation so that further use or derivation thereon is impossible.

7.6. Time Stamping

7.6.1. Time Stamping Issuance

ZealiD TSA offer time-stamping services using RFC 3163 Time Stamp Protocol over HTTPS transport. Time stamps are included as a part of qualified electronic signatures provided by ZealiD. ZealiD does not provide time stamps externally, separately from the signature.

ZealiD does not accept external hash submission for TST signatures.

ZealiD TSA CA, TSA OCSP and TSU keys are 4096-bit RSA keys. TSU key is used only for signing TSTs. TSA CA Keys are used to certify TSA OCSP and TSU keys. TSA OCSP keys are used to sign OCSP Response.

ZealiD TSA logs all issued TSTs. TSTs will be retained by the TSA for 12 years after the expiration or revocation of TSU Certificate. ZealiD can prove the existence of a particular TST on the request by a Relying Party. ZealiD might ask the Relying Party to cover the costs of such service.

ZealiD TSU does not issue any TST when the end of the validity of the TSU private key has been reached.

ZealiD OCSP Service is free of charge and publically available 24/7 at https://ocsp.zealid.com

ZealiD provides 24 hour availability of Certificate Status Services, 7 days a week with a minimum of 99.5% availability overall per year. This is ensured by ZealiD setting up high availability systems, providing network redundancy (connection) and power.

7.6.2. Clock Synchronization with UTC

All ZealiD TSA and ZealiD Backend components are synchronized daily with a Network Time Protocol (NTP) service Pool Server Stratum 1 for UTC time every 24 hours. Time derived from the time service shall be used for establishing the time of:

- Initial validity time of a TSA CA and TSU Certificates;
- Revocation of a TSA CA and TSU Certificates;
- Logging;
- Archiving;
- Issuance of timestamps.

Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events.

ZealiD TSA ensures that its clock is synchronized with UTC within the declared accuracy of 1 second using the NTP.

ZealiD TSA monitors its clock synchronization and ensures that, if the time that would be indicated in a TST drifts or jumps out of synchronization with UTC, this will be detected. In the case of a TST drift or jump out of synchronization with UTC, ZealiD TSA stops issuing time stamps until the issue is resolved. Information about the loss of clock synchronization will be made available in public media.

Local and remote NTP servers with Stratum 1 time sources are used for NTP reference. Monitoring of clock synchronization is done by comparing the time sources.

ZealiD TSA guarantees that the clock synchronization is maintained when a leap second is scheduled, as notified by the appropriate body. The change to take into account the leap second is carried out during the last minute of the day on which the leap second is scheduled. A record is

made of the exact time (as per the declared accuracy) when this change is made.

7.7. Physical and Environmental Security

ZealiD has implemented a Policy Information Security with a supporting Policy IT Security. These policies specify security measures that are required and define a set of routines specifying how security measures are implemented.

ZealiD's Policies include the security controls and operating procedures for all physical facilities, systems and information assets providing the trusted services. As part of regular training and communication, ZealiD management communicates information security policies and procedures to employees and relevant external parties as appropriate.

In addition, ZealiD supports its practices and information security objectives for Trust Services with several types of reviews, audits and controls.

7.7.1. Site location and construction

ZealiD operations are conducted in ZealiD's premises in Sweden and Lithuania, and in premises of supporting contractors.

ZealiD TSA Services are produced within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of Information and systems. The protection provided a high level of protection corresponding to the threat of identified risks. ZealiD ensures that physical access to critical services is controlled and that physical risks to its assets are minimised.

The primary locations for ZealiD TSA Services are managed in Sweden.

ZealiD sites are physically protected with different layers. All external contractors are ISO 27001 certified and implement necessary physical security measures.

ZealiD has put in place necessary security mechanisms to protect the data in transit and rest, e.g. two factor access control, encryption and logging in order to detect unauthorized use of, access to, or disclosure of sensitive information and systems content. The principle of minimum

access rights are implemented and only authorized resources can access the aforementioned systems.

7.7.2. Physical access

ZealiD contracted data centre for the ZealiD TSA Service is protected by six tiers of physical security, with access to the lower tier required before gaining access to the higher tier.

The employees of ZealiD may gain access to the facilities of the ZealiD TSA Services only as authorised resources notified on an approved list.

A log is kept for recording all entries and exits to the data center. The data center (location provider) has no independent access to the ZealiD TSA Service hardware or software.

Common areas are outside the ZealiD TSA Service racks.

7.7.3. Power and air conditioning

The premises of ZealiD and contractors have all necessary heating, ventilation, air conditioning systems to control the temperature and relative humidity. These are state-of-the-art documented industry facilities.

Furthermore, all relevant systems are provided with an uninterruptible power supply sufficient for a short period of operation in the absence of commercial power, to support either a smooth shutdown or to re-establish commercial power.

The data center has taken every reasonable precaution to minimise the impact of water exposure to the information systems.

7.7.4. Fire prevention and protection

The data centers have taken all reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. This includes high grade early smoke detection apparatus in conditioned modules and monitored automatic smoke detection. Measures comply with the highest fire prevention and protection standards.

7.7.5. Media storage

ZealiD keeps a register of systems and storage media. ZealiD has internal routines on how to decommission and destruct media or information on the media. Media storage lifetime at ZealiD is selected according to the required period of time for record retention.

7.7.6. Waste disposal

Media containing Sensitive Information are securely disposed of when no longer required.

Paper documents and materials with sensitive Information are destroyed before disposal or placed in a secure waste handling box. Media used to collect or transmit Sensitive Information are rendered unreadable before disposal.

7.7.7. Off-site Backup

The ZealiD TSA Service performs routine backups to multiple sites of critical system data, audit log data, and other sensitive information. The backup is both online and offline. There is no off-site backup for the HSM.

7.8. Operation Security

7.8.1. Specific computer security technical requirements

ZealiD ensures that the certification system components are secure and correctly operated, with an acceptable risk of failure.

The general guidelines for creating passwords (such as minimum length and password complexity) are the basis of the password policy. All employees are informed about the proper handling of passwords and have signed an appropriate guideline.

There is a defined timeout for sessions.

ZealiD certification services system components are managed in accordance with defined change management procedures. These

procedures include system testing in an isolated test environment and the requirement that change must be approved by the Security Officer. The approval is documented for further reference.

All critical software components of ZealiD are installed and updated from trusted sources only. There are also internal procedures to protect the integrity of certification service components against viruses, malicious and unauthorised software.

All media containing production environment software and data, audit, archive, or backup information are stored within ZealiD with appropriate physical and logical access controls designed to limit access to authorised personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic). Media management procedures and backup of records and data to different media types protects against obsolescence and deterioration of media within the period of time that records are required to be retained. Media containing Sensitive Information are securely disposed of when no longer required. All removable media are used only for the intended period of the user (either by time or by number of uses).

The performance of ZealiD services and IT systems and their capacity is monitored by System Administrators and changes are done when necessary according to internal change management procedure.

ZealiD TSA Service hardware is physically located in a secure location with multiple access and logic controls.

Incident response and vulnerability management procedures are documented in an internal document. Monitoring system detects and alarms of abnormal system activities that indicate potential security violation, including intrusion into the network.

Paper documents and materials with Sensitive Information are securely disposed of. Media used to collect or transmit Sensitive Information are rendered unreadable before disposal.

ZealiD security operations include: operational procedures and responsibilities, secure systems planning and acceptance, protection from malicious software, backup, network management, active

monitoring of audit logs event analysis and follow-up, media handling and security, data and software exchange.

ZealiD has implemented security measures and enforced access control in order to avoid unauthorized access and attempts to add, delete or modify information in applications related to the services, including certificates and revocation status information. User accounts are created for personnel in specific roles that need access to the system in question. The rights are then reviewed by the CTO. When leaving the company, the withdrawal of access rights takes place within a maximum 24 hours.

ZealiD's personnel are authenticated before using critical applications related to the services. Multi-factor authentication for all accounts capable of directly causing certificate issuance is enforced. All users must log in with their personal account, and administrative commands are only available with explicit permission and auditing of the execution. File system permissions and other features available in the operating system security model are used to prevent any other use. User accounts are removed as soon as possible when the role change dictates. Access rules are audited annually.

7.8.1.1. Computer security rating

ZealiD uses standard computer systems.

7.8.2. Life cycle technical controls

7.8.2.1. System development controls

An analysis of security requirements is carried out at the design and requirements specification stage of any systems development project undertaken by ZealiD; or an analysis is carried out on behalf of ZealiD to ensure that security is built into the Information Technology's systems.

The software will be approved by the Security Officer and shall originate from a trusted source. New versions of software are tested in a testing environment of the appropriate service and their deployment is conducted according to documented change management procedures. Changes to systems are documented.

7.8.2.2. Security management controls

Measures are implemented In the information system of ZealiD TSA Service, including all workstations for guaranteeing the integrity of software and configurations, as well as for detecting fraudulent software and restricting its spread.

Only the software directly used for performing the tasks is used in the information system.

7.8.2.3. Life cycle security controls

ZealiD TSA Service policies, assets and practices (including ZealiD TSAPS) for information security are reviewed by a person which is responsible for administering and maintaining them at planned intervals or in case of significant changes to ensure their continuing suitability, adequacy and effectiveness.

The configurations of ZealiD TSA Service systems are regularly checked for changes that violate ZealiD TSA Service security policies. A review of configurations of the issuing systems, security support systems, and front-end/internal support systems occurs at least on a quarterly basis.

The Security Officer approves changes that have an impact on the level of security provided. ZealiD TSA Service has procedures for ensuring that security patches are applied to all systems within a reasonable time period after they become available, but not later than one month following the availability of the security patch. In case of a critical vulnerability, the security patch is deployed within 48 hours. The reasons for not applying any security patches will be documented.

ZealiD manages the registration of information assets and classifies all information assets into security classes according to the results of the regular security analysis consistent with the risk assessment. A responsible person has been appointed for all important information security assets.

7.8.3. Network Security

ZealiD TSA Service network is divided into zones by security requirements. Communication between the zones is restricted. Only the protocols needed for ZealiD TSA Service services are allowed through the firewall.

There are separate and dedicated firewalls in place. Access to the administrative interfaces of IT equipment is not directly accessible from the public Internet. For the most critical tasks a separate workstation is used.

The front-end systems are in a DMZ protected by a firewall and TLS offload servers. Actual security critical services and corresponding HSMs run in a secure zone that is separated by dedicated firewall and has no direct Internet access.

The SAM Appliance, which contains the TSU, is in a high security zone and is air-gapped from all the other networks. ZealiD TSA Service systems are configured with only these accounts, applications, services, protocols, and ports that are used in the Trust Service operations.

ZealiD ensures that only personnel in Trusted Roles have access to a secure zone and a high security zone.

The cabling and active equipment along with their configuration in ZealiD's internal network is protected by physical and organisational measures.

The transfer of Sensitive Information outside ZealiD's internal network is encrypted.

Communication between distinct trustworthy systems is established through trusted channels that are logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

The security of ZealiD's internal network and external connections is constantly monitored to prevent all access to protocols and services not required for the operation of the Trust Services.

TSU systems are configured with only these accounts, applications, services, protocols, and ports that are necessary for ZealiD TSA operations.

7.8.4. Incident Management

Within the ISMS, an integral part of the ZealiD TSA Service, change and incident management procedures have been developed to allow for a controlled, structured and accountable handling of incidents as well as recovery from systems or application disasters.

Detailed instructions can be found in the ZealiD Routine Incident Management and in the Information Security ISMS. Finally, Routine External Communication governs the means of communication that is deemed necessary by the Incident Evaluation Team.

The incidents can be submitted using either internal or external submission forms (https://www.zealid.com/contact), or as an email to support@zealid.com

The response time by the Incident Evaluation Team is determined by the severity of the incident, but is no longer than 24 hours on working days.

The objective of Incident Management is the immediate response and recovery of availability and the continuous protection of ZealiD TSA service.

The critical vulnerability is addressed no later than 48 hours after its discovery; the vulnerability is remediated or a mitigation plan is created and implemented to reduce the impact of vulnerability or a decision has been made and documented that remediation is not required.

In the event of an emergency, ZealiD will inform all the Subscribers and Relying Parties immediately (or at least within 24 hours of the crisis committee's decision) of the emergency situation and proposed solution through public information communication channels.

ZealiD 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 as national CERT of any breach of security or loss of integrity that has a significant impact on the ZealiD TSA Service provided.

If breach is likely to involve personal data and is likely to result in high risk to the rights and freedoms of the natural person, ZealiD will notify Swedish Authority for Privacy Protection without undue delay, but at least within 24 hours after initial discovery of the personal data breach.

7.8.5. Collection of Evidence

ZealiD ensures that all relevant information concerning the operation of the Trust Services is monitored and recorded for providing evidence for the purpose of legal proceedings. This information includes the archive records that are required for proving the validity of Trust Service Certificates and the audit log of the Trust Service operation.

ZealiD's information systems leave an audit log of:

Category	Log details
General events	• Software installation, patches and updates • Backup related information • Boot and shutdown • Boot and shutdown of logging (audit) function • Time synchronization and detection of loss of synchronization • All requests and reports relating to revocation, as well as the resulting actions. • Availability and Capacity utilization
General Security events	• System account creation • Access attempts • Configuration changes to Firewalls, Switches, Intrusion detection systems, and load balancers • System crashes or other anomalies • Hardware failures • PKI System access attempts • Firewall and Switch activities • Activities of system user with super admin rights • Changes related to security policy • Changes in audit parameters
Trust Service certificates	• All events relating to the life cycle of keys and Certificates managed by ZealiD, including CA keys and Certificates and TSU key pairs; • Timestamping events (including associate certificate and key); • OCSP queries for non-issued certificates.

Log entries must also include:

- Date and Time;
- Identity of the entry generator;
- Attribute related to entry type;
- Success or failure of the audited event.

Audit logs are retained and accessible for 12 years.

Additionally, ZealiD TSA logs all issued TSTs and retains them for 12 years after the expiration or revocation of TSU certificate within ZealiD Archive.

7.8.6. Business Continuity Management

Backups of the logs of all issued TSTs by ZealiD TSA are kept in off-site storage.

In case of compromise or disaster, ZealiD executes according to a Continuity Plan. It guarantees a robust set of procedures as well as physical and logical security measures to minimize the impact of disaster. All procedures have been developed to minimize potential impact and restore operations within a reasonable period of time. The Continuity Plan is tested annually to determine whether they meet requirements and business continuity needs.

In order to ensure the business continuity capabilities after a disaster ZealiD periodically organises crisis management training. ZealiD internal documentation defines how crisis management and communication take place in emergency situations.

ZealiD has implemented ZealiD TSA Service infrastructure in a redundant configuration to minimise the impact of disasters. In addition, important information with respect to restoring the ZealiD TSA Service is backed up for disaster recovery purposes.

7.8.7. Incident and compromise handling procedures

Within the ISMS, an integral part of the ZealiD TSA Service, change and incident management procedures have been developed to allow for a controlled, structured and accountable handling of incidents as well as recovery from systems or application disasters.

Detailed instructions can be found in the ZealiD Routine Incident Management and in the Information Security ISMS. Finally, Routine External Communication governs the means of communication that is deemed necessary by the Incident Evaluation Team.

The incidents can be submitted using either internal or external submission forms (https://www.zealid.com/contact), or as an email to support@zealid.com

The response time by the Incident Evaluation Team is determined by the severity of the incident, but is no longer than 24 hours on working days.

The objective of Incident Management is the immediate response and recovery of availability and the continuous protection of ZealiD TSA service.

The critical vulnerability is addressed no later than 48 hours after its discovery; the vulnerability is remediated or a mitigation plan is created and implemented to reduce the impact of vulnerability or a decision has been made and documented that remediation is not required.

7.8.8. TSU private key compromise

If the TSU private key is compromised or suspected to be compromised or calibration lost, ZealiD will inform Subscribers and Relying Parties and will stop using the compromised key. ZealiD TSA will revoke the TSU certificate. The latter actions will be carried out in accordance with the Management Board decisions, external communication routines and business continuity plan.

7.8.9. Loss of clock synchronization

In case of loss of clock synchronization, ZealiD TSA suspends its operations to prevent further damage. Business continuity plan is activated to restore the service.

7.9. TSA Termination and Termination Plans

The ZealiD TSA Service is terminated:

- With a decision of ZealiD Management Board;

- With a decision of the authority exercising supervision over the supply of the service;
- With a judicial decision;
- Upon the liquidation or termination of the operations of ZealiD.

Before ZealiD terminates a TSA Service the following procedures will be executed:

- ZealiD informs all Subscribers and other entities with which ZealiD has contracts or other forms of established relations. In addition, this information will be made available to other Relying Parties;
- ZealiD makes the best effort for doing arrangements with other Trust Service Providers (Custodians) to transfer the provision of services for its existing customers;
- ZealiD will revoke all of its TSU certificates;
- ZealiD ensures that events of TSA that are logged are retained in a way that they cannot be deleted or destroyed;

ZealiD's will notify all interested parties of any termination of the TSA Service by means of email, website information, press releases and via its supervisory body.

ZealiD does not assume liability for any loss or damage sustained by the user of the service as a result of such termination provided that ZealiD has given the notice of termination through public information communication channels for at least one month in advance.

ZealiD has a plan to cover the costs to fulfill minimum requirements as far as permitted by Swedish commercial and bankruptcy law in case the TSP terminates.

ZealiD ensures that potential disruptions to Subscribers and Relying Parties are minimised as a result of the cessation of ZealiD's services, and in particular,

- it ensures the continued maintenance of information required to verify the correctness of ZealiD TSTs for 12 years and
- audit logs are retained and accessible for 12 years.

7.10. Compliance

7.10.1. Frequency or circumstances of assessment

The conformity of information systems, policies, practices, facilities, personnel, and assets of ZealiD are assessed by a CAB pursuant to the eIDAS regulation, ETSI Standards and relevant national law (see Section 2 and 4.6).

Conformity is assessed at least every 2 years and when any major change is made to Trust Service operations.

ZealiD's internal auditor carries out internal reviews and audits on a rolling yearly schedule.

7.10.2. Identity/qualifications of assessor

ZealiD's CAB is accredited according to ISO/IEC 17065. The CAB is competent to carry out conformity assessments of Qualified Trust Service Providers and its services.

7.10.3. Assessor's relationship to assessed entity

The auditor of the CAB shall be independent from ZealiD and ZealiD assessed systems. The internal auditor shall not audit his/her own areas of responsibility.

7.10.4. Topics covered by assessment

The conformity assessment covers the conformity of the information system, policies and practices, facilities, personnel, and assets with eIDAS regulation, respective legislation and standards.

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

Activities subject to internal auditing are the following:

- Quality of Service;
- Security of Service;
- Security of operations and procedures.

The CAB audits ZealiD protection of subscriber data, security policy, performance of work procedures and contractual obligations, as well as compliance with TSAPS and service-based policies and practice statements.

The CAB and the Internal Auditor also audit these parts of the information system, policies and practices, facilities, personnel, and the assets of contractors that are related to providing ZealiD Trust Services (e.g. including RAs).

7.10.5. Actions taken as a result of deficiency

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

ZealiD makes efforts to stay compliant and fulfill all requirements of the deficiency on time. ZealiD management is responsible for implementing a corrective action plan. ZealiD assesses the deviations or non compliance items and prioritizes appropriate actions to be taken. If any deviations relate to the protection of personal data, the Supervisory Body shall inform the data protection authority.

7.10.6. Communication of results

Certificate(s) for trust service(s) resulting from conformity assessment audits conducted pursuant to the eIDAS regulation, corresponding legislation and standards, are published on ZealiD's website https://www.zealid.com/repository.

ZealiD submits the resulting conformity assessment report to the Supervisory Body within three working days.