ZealiD AB		Document name ZealiD TSPS		
Owner CEO	Class Public	Category Certification	Date 2023-05-24	Revision 16

ZealiD Trusted Registration Authority Practice Statement (ZealiD TSPS)

Table of Contents

Revision History

Version	Date	Change comment	Author
00B	2018-09-01	FIrst Re-Draft from other format	Multiple
00B	2019-01-18	Work document	Multiple
01	2019-02-01	Updates	Philip Hallenborg
01	2019-02-06	Updates	Robert Arnesson
02	2019-02-09	Updates	May-Lis Farnes
03	2019-02-10	Updates	Philip Hallenborg
04	2019-02-15	Small updates	May-Lis Farnes
05	2019-02-25	Wording, Errors	Pihlip Hallenborg
06	2019-05-08	Update after CAB document review	May-Lis Farnes, Tomas Zuoza
07	2019-05-27	Update to conform with template	Tomas Zuoza
08	2019-06-15	Updates deviation. Change name to TRA PS	Philip Hallenborg / Tomas Zuoza
09	2019-06-16	Updates structural changes	Philip Hallenborg
10	2019-06-17	Formatting	Tomas Zuoza
11	2019-06-18	6.7 more details added	Tomas Zuoza
12	2020-01-12	Multiple updates	Philip Hallenborg / Tomas Zuoza
13	2020-03-27	Multiple updates	Tomas Zuoza
14	2021-02-26	Added 4.2 to explain communication between RA and CA. Updated entry and exit logging procedures. Updated retention period to 12 years.	Tomas Zuoza
15	2022-05-23	1.3 updated to exclude sampling 3.1 updated to remove 3rd party data 3.2 updated to include NFC based identification. Removed 3rd party data and sampling requirements 5.4 updated to include NFC validation logging 6.7 updated to exclude sampling	Tomas Zuoza
16	2023-05-24	3.2.3 included a supplementing validation mechanism by a third party 5.4.1 Added saving of the third-party document	Tomas Zuoza

1. Introduction

1.1. Overview

ZealiD is a Registration Authority (RA) and identifies subscribers requesting qualified electronic signatures based on qualified certificates from a Certificate Authority (CA).

The purpose of the RA service is to provide CAs and in particular eIDAS Trust Service Providers (e.g. QTSP CAs) with compliant subscriber registration.

The ZealiD service under this Practice Statement (PS) is referred to as a Trusted Registration Authority and the PS as a Trust Service Practice Statement (TSPS). The RA Service is referred to as “trusted” in that it complies with eIDAS and thus is coined “TRA Service”. This TSPS is structured according to RFC 3647.

ZealiD performs identification of subscribers where the subscriber is a natural person and the qualified certificates are issued for the purpose of the subscriber signing documents on its own behalf.

The CA issues certificates, performs identification and authentication of subscribers and initiates or passes along revocation requests for certificates.

1.2. TRA Service Objective

TRA Service shall perform a successful identification of the natural person in a remote (online) environment. TRA Service determines that the subscriber is physically present with a level of assurance at least at the level of a human face-to-face identity verification session. The TRA Service will:

- Check for actual existence of the person in real life;

- Use dual sources of identification (Identity document and personal photo) to verify whether the ID document belongs to the natural person;
- Prove that the identified natural person is the same as specified;
- Check the legal authenticity of a national official ID document.

1.3. eIDAS Legality, ETSI standards and German State-of-the-art

The ZealiD Trust Service Policy governing this TSPS consist of the eIDAS designated standards:

- ETSI EN 319 401,
- ETSI EN 319 411-1,
- ETSI EN 319 411-2,
- ETSI TS 119 461.

ZealiD identification services support the identification of natural persons following the policy QCP-n-qscd.

ZealiD performs identity verification on natural persons only, where the subscriber and the subject are identical.

ZealiD uses an automated verification of identity method supported by mandatory identification vetting performed by a natural person (Registration Officer).

In doing so, ZealiD provides an identification method conforming to eIDAS article 24, paragraph 1d, providing equivalent assurance in terms of reliability to physical presence, which has been confirmed by a German conformity assessment body.

ZealiD TRA supports unattended remote identity proofing with hybrid and manual operation.

The identification of individual identity is done according to ETSI TS 119 461.

Where physical ID documents are used for the applicant identification, the TRA Service also fulfils related requirements under German Law (state-of-the-art):

- relevant provisions of Vertrauensdienstegesetz (VDG);
- relevant provisions of Anerkennung „innovativer Identifizierungsmethoden“ i. S. d. § 11 Absatz 3 VDG (AutoIdent);

1.4. Document name and identification

This practice statement is titled ZealiD Trusted Registration Authority Practice Statement (ZealiD TSPS). The Issuing TSPS has the object identifier: OID 1.2.752.251.1.5.51.2.15.

1.5. PKI participants

ZealiD can provide their ZealiD TRA Service as a standalone to CAs or include the service in its own CA.

All participating CAs need to comply with this TSPS and any CA’s Certificate Practice Statement needs to comply with this TSPS and relevant regulations, standards and PSs.

1.5.1. Certification Authorities (CA)

The requirements for the TRA Service will additionally be stated in the CA’s PS and are met under the standards:

- ETSI EN 319 411-2,
- ETSI EN 319 411-1,
- ETSI EN 319 401,
- CEN EN 419 241-1.

The CA will have its name in the “Issuer” field of the Issuing CA certificates.

1.5.2. Registration Authority (RA)

ZealiD will perform a number of duties vis-a-vis the CA. These duties are:

- Control that all TRA Service operational procedures are performed in compliance with the present Trust Service Policy;
- Allow subscribers to apply for certificates via the TRA service;
- Report all security incidents to the CA;
- Manage the changes within this document upon validation of the CA.

ZealiD is acting as the RA in the following way:

- Provide full and comprehensive compiling of all identity verification above and forward to the CA;
- On behalf of the subscriber as an intermediary to request a qualified certificate to be issued by a CA;
- On behalf of the subscriber as an intermediary while setting up a smartphone app based electronic identity.

1.5.3. Subscribers

The subscribers identified in for ZealiD TRA Services are natural persons wishing to:

- request an identity verification for a qualified trust service;
- request a qualified certificate to be issued by a CA,

1.5.4. Relying parties

Relying parties are service providers that will

- forward subscribers to the TRA Service;
- request full and comprehensive packaging of all identity checks.

1.5.5. Other participants

No stipulation.

1.6. Certificate usage

1.6.1. Appropriate certificate uses

Certificates issued as a result of the ZealiD TRA Service are issued by the CA to:

- Subscribers for authentication and non-repudiation signing.

The exact details of certificate usage will be defined by the CA in its CPS.

1.6.2. Prohibited certificate uses

No Stipulation.

1.7. Policy administration

1.7.1. Organization administering the document

The TSPS has been implemented in the entire organization following a decision by the Management Board. This document is published and maintained by ZealiD AB Sweden. Policies set out by this TSPS are implemented throughout ZealiD organization. This TSPS is published and communicated to personnel and external parties.

1.7.2. Contact person

Mailing address:
ZealiD AB
Box 3437
11156 Stockholm

Visiting address:
Norrlandsgatan 10
111 43 Stockholm
Sweden

Contact:
email: support@zealid.com, legal@zealid.com
telephone: +46 (0)10-199 40 00 (EN, SE), +370 5 2078882 (EN, LT)

1.7.3. Person determining PS suitability for the policy

ZealiD Compliance Manager.

1.7.4. PS approval procedures

The Management Board Decision Routine describes the PS approval process. This process is monitored by the ZealiD Compliance Manager.

1.8. Definitions and acronyms

CA	Certification Authority
CRL	Certificate Revocation List
Control panel	The Control Panel is the front end och application for the RPs to configure the TRA Service and receive data
Customer	Customer is a RP, typically a finance service provider
ZealiD	Is the trading brand name of the legal entity ZealiD AB
ZealiD TRA	ZealiD Trusted Registration Authority
ZealiD TRA Service	ZealiD Trusted Registration Authority Service
ISO	International Organization for Standardization
OID	Object Identifier

Management System	Management System is ZealiDs internal Policies, Routines etc based on ISO 27001 and complying with relevant regulation and ETSI standards
NFC	Near Field Communication
Relying Party	Relying parties (RP) are defined as any Subscriber (as defined in Subscribers below) or any end-entity (also referred to as Customers) relying on the Services of ZealiD
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RFC	Request For Comments
SIS	Swedish Standards Institute
Subscriber	A Subscriber is a natural person seeking to sign documents electronically, set up an electronic identity, signing in with strong authentication and perform remote identification.
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UUID	Universally Unique Identifier

2. Publication and repository responsibilities

2.1. Repositories

ZealiD publishes to its publicly available repository https://zealid.com/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) the following documents:

- ZealiD TSPS (this document);
- Subscriber Terms and Conditions;

- Where applicable: Links to the repository of CA PS;
- Evidence of certification.

2.2. Publication of certification information

ZealiD makes the following documents publicly available:

- Trust Service Practice Statement (this TSPS);
- Audit Results;
- Insurance Policies;
- Terms and Conditions TRA Service.

2.3. Time or frequency of publication

Documentation listed under Repositories above are reviewed, updated and published with minimum delay when:

- any change is made or at least once per year;
- any legal, regulatory or otherwise mandatory requirement calls for an update.

Upcoming significant changes will be made public at least 14 days in advance.

Subscribers and relying parties will be notified via the ZealiD public repository and further according to the ZealiD Routine External Communication choice of appropriate channel.

2.4. Access controls on repositories

Information published in ZealiD's repository is public and not considered confidential information.

ZealiD has implemented all necessary security measures and enforced access control in order to prevent unauthorized access to add, delete, or modify entries into its repository. All TSPS versions are subject to final confirmation and approval by the ZealiD Management Board before publication. Publishing into ZealiD's repository is restricted to authorized employees of ZealiD with multi-factor

authentication access. The CEO and COO are the only ones who can publish the TSPS.

3. Identification and authentication

3.1. Naming

3.1.1. Types of names

No stipulation

3.1.2. Need for names to be meaningful

Within the ZealiD TRA Service, identification of a natural person is verified. This includes the name of the subscriber being checked against a copy of a government issued national ID document.

ZealiD collects the data of the user and checks it.

The following data will be collected, interpreted and vetted as a minimum:

- Full Name;
- Date of Birth;
- Government issued national ID document;
- Issuing country;
- Nationality;
- Type of identity number (i.e. personal number, document identification number OR tax identification number);
- Phone number;
- ID document issuing and expiry dates;
- Biometric picture and signature on ID Document;
- Facial image.

In addition to this data, email and/or mobile number of the subscriber is additionally collected.

3.1.3. Anonymity or pseudonymity of subscribers

All names are real names and have been checked against evidence in the form of a smartphone photo of the ID document, relayed to the TRA Service. Anonymity or pseudonymity is not allowed by ZealiD.

3.1.4. Rules for interpretation of name forms

The subject name must contain the full name of the (identical) subscriber. The name used is the name of the subject at the time the certificate was issued. The name of the subject used for the qualified certificate will always be taken from the identity document used to identify the subscriber. International letters are encoded in UTF-8. The data extracted from an identity document follows ICAO transcription rules where necessary.

3.1.5. Uniqueness of names

The uniqueness of each subject name is ensured by providing the full name of the subscriber together with two unique identifiers:

- Personal or ID Document number and;
- Unique ZealiD number.

3.1.6. Recognition, authentication and role of trademarks

No stipulation.

3.2. Initial identity validation

3.2.1. Method to prove possession of private key

No stipulation.

3.2.2. Authentication of organization identity

No stipulation.

3.2.3. Authentication of individual identity

ZealiD will authenticate the natural person remotely based on a subscriber self-service online process interacting with a machine followed by a mandatory manual process in the TRA Service.

The full name, the date and the place of birth and other data (see 3.1.2) are provided as evidence by the subscriber to ZealiD.

This is achieved by a module based approach. There are three modules in the TRA Service:

1. Liveness;
2. Identification Document:
    a. NFC based;
    b. Identity Document video based;
3. Manual Vetting.

The modules can be accessed by the subscriber via ZealiD App (iTunes or AppStore):

1. Subscriber selects language and country;
2. Subscriber performs a Liveness check according to instructions;
3. Subscriber uses a smartphone to take a picture of a valid government issued ID document:
    a. If the document is NFC enabled, ZealiD will read the data contained on the electronic chip;
    b. If the document does not contain NFC chip, ZealiD will ask the Subscriber to take a video of the document additionally to the photos;
4. Subscriber confirms the submitted information.

The data from the ID document is checked for ID document genuineness and validity according to national government ID issuing standards or where applicable ICAO standards.

In the case where a country document is not meeting the sufficient number of security features and additional process is implemented by ZealiD using a customer as a third party providing supplementing information. The information is delivered to ZealiD in a document signed with a qualified electronic signature by an authorised person. This document is consulted during identity proofing process and acts as an additional security feature. All other verification steps are conducted as regular.

All verification steps and their results are documented and stored by ZealiD.

If the authentication of the person is based on a subsequent remote authentication, the authentication is provided by the CA and uses at least two factor authentication as defined in ISO 29115 (knowledge, inherence or possession).

Any secret information exchanged in authentication protocols are cryptographically protected in transit. Two or more credentials implementing different authentication factors shall be used.

In the case of chain of remote authentication, the authentication factors are created during the initial identification which was performed in a way that provides equivalent assurance in terms of reliability to the physical presence.

If one of the authentication factors becomes unavailable (e.g. the user forgets a password), the user must perform a new identification process in the TRA service.

The TRA Service is open and accessible to the public (any natural person) with only the requirement to be capable of performing the identity verification process.

ZealiD TRA Service validation is done solely within a backend infrastructure controlled by ZealiD.

Acceptance and processing of natural persons is based only on the objective criteria stated in the field of operation of this TSPS and subject to the natural persons abiding by the obligations in the TRA Service Terms and Conditions.

The TRA Service is designed with disabled people in mind. Deaf users and blind users with tailored devices can complete the TRA Service requirements.

3.2.4. Non-verified subscriber information

No stipulation.

3.2.5. Validation of authority

No stipulation.

3.2.6. Criteria for interoperation

Certificates generated based on the information provided by ZealiD are compliant with ETSI EN 319 411-2 with the Trust Service Policy QCP-n-qscd.

3.3. Identification and authentication for re-key requests

No stipulation.

3.4. Identification and authentication for revocation request

No stipulation.

4. Certificate life-cycle operational requirements

4.1. Certificate Application

No stipulation.

4.2. Certificate application processing

The RA Service validates the Subscriber's identity as described in the TSPS. RA Service sends the Certificate requests to the CA. Application for a Subscriber will be generated automatically via the RA Service. All communications are secured with TLS encryption along with all information presented directly by the Subscriber during the application process.

The data exchange is done via encrypted communication where a unique identifier is used by the RA Service in order to authenticate it.

Before starting the authentication, the Subscriber shall accept RA Service Terms and Conditions.

5. Facility, management, and operational controls

The ZealiD Management Board defines and approves policies and practices related to information security for its trust services.

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 performs risk assessment regularly in order to evaluate business risks, IT risks and risks related to the registration authority functions. This includes risks related to physical facilities. These risk assessments determine the necessary security requirements and operational procedures.

ZealiD management board approves risk assessment, oversees risk mitigation and accepts any residual risks.

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.

ZealiD's Policies include the security controls and operating procedures for all physical facilities, systems and information assets providing the trusted services.

5.1. Physical controls

5.1.1. Site location and construction

ZealiD operations are conducted in ZealiD's premises in Sweden and Lithuania, and in premises of supporting contractors. The premises meet the requirements set forth in the internal policies and routines.

Physical controls have been implemented for the locations, which are used to process and store the personal data of the enrollment process in order to prevent unauthorized access to such premises. ZealiD is using facilities that have implemented physical and environmental security controls in order to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation.

For the security on premises ZealiD routines require:

- Closed windows and locked doors;
- Video surveillance;
- Physical access restriction with manned and unmanned doors/entries;
- Only authorized personnel are granted access to the premises;

- Supervision or monitoring of third parties;
- Logging of visitors.

For the security of manual vetting premises ZealiD routines additionally require:

- Alarm with response from security guards;
- Physically separate room from other ZealiD activities;
- Entry and exit to the premises is logged with the use of a video camera that is activated when movement is detected.

Where ZealiD utilizes IT systems at contractors, requirements are placed on them to meet and document security measures. ZealiD reviews contractor policies and practices and documents them in its management system.

ZealiD qualifies contractors according to an internal Routine Procurement Contractors. This Routine describes an evaluation process that specifically looks at contractor obligations vs. capabilities, compliance, policies and practices.

All external contractors are ISO 27001 certified and meet necessary physical security measures.

The hosting of hardware for ZealiD Backend is managed by Baltneta Lithuania.

ZealiD sites are physically protected with different layers.

5.1.2. Physical Access

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

Access to the highest tier requires the participation of two persons in Trusted Roles.

The employees of ZealiD may gain access to the facilities of the TRA 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 TRA Service hardware or software.

Common areas are outside the ZealiD TRA Service racks.

5.1.3. Power and air conditioning

The premises of ZealiD and contractors have industry standard power and air conditioning in place and are documented.

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.

5.1.4. Water exposures

The office premises and data centers have taken every reasonable precaution to minimise the impact of water exposure to the information systems.

5.1.5. Fire prevention and protection

The office premises and 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.

5.1.6. 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. Sensitive data is kept encrypted regardless of storage medium.

5.1.7. 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.

5.1.8. Off-site backup

The ZealiD TRA 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.

5.2. 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.

ZealiD contractors are contractually bound to follow ZealiD security policy and applicable routines. Personnel of contractors are trained and informed accordingly by ZealiD.

Personnel are provided training and all personnel and temp workers 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.

5.2.1. Trusted roles

ZealiD has established and documented necessary trusted roles to run its TRA Service.

Trusted roles are executed mainly by ZealiD personnel, but may be executed by contracting parties, like temp workers or/and by personnel of contractors, especially in data centers. In any case each individual has to fulfil all defined requirements for trusted roles before assignment to the trusted role. Trusted role specifics are regulated in the contracts with contractors as binding regulations.

ZealiD Management board appoints trusted roles of its personnel and temp workers and appointees accept the role responsibilities as part of their role.

Personnel of contractors foreseen for trusted roles are named to ZealiD and appointed by the contractor based on the contractual obligations.

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.
System Auditors: Authorized to view archives and audit logs of the TSP's trustworthy systems.
Registration Officer: Performs the manual vetting procedures defined by the TRA Service procedure and approves or rejects applicants.
Compliance Manager: Manages Compliance, Information

Security including Risk Management and some aspects of Quality.

ZealiD has a sufficient number of System Administrators assigned according to internal routines.

The assignment is made person by person with a decree of the CEO/the contractor's management. See clause 5.2.2 for details.

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

ZealiD and contractors ensure 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 TRA Service are managed by ZealiD and contractor's personnel in Trusted Roles.

5.2.2. Number of persons required per task

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

5.2.3. Identification and authentication for each role

All Trusted Roles are performed by persons qualified and assigned to this role by the Management Board.
Proof-of-identity of ZealiD personnel, temp workers or personnel of contractors that are qualified for Trusted roles 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. User account access is only given after filling out the New Personnel Registration form.

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.

5.2.4. Roles requiring separation of duties

ZealiD has routines to ensure segregation of duties and persons required per task. ZealiD staff and temp workers have job descriptions defined from the view point of roles fulfilled with segregation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness. Same rules apply for personnel of contractors as bound by specific contractual obligations.

5.2.5. Conflict of Interest

ZealiD personnel, temp workers in trusted roles are kept free from conflict of interest that might prejudice the impartiality of the TRA Service operations.

Same rules apply for personnel of contractors as bound by specific contractual obligations.

5.3. Personnel controls

5.3.1. Qualifications, experience, and clearance requirements

ZealiD executes structured hiring, qualification and continuous training processes to achieve security consciousness and awareness regarding personnel duties, organizational policies and procedures.

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 contractors are contractually bound to follow ZealiD security policy and applicable routines. Personnel of contractors are trained and informed accordingly by ZealiD.

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 Trusted Roles are further required to:

- Not participate in any activity regarding registration or identity verification his/her name or legal representative of him/her;
- Remain neutral and objective with regards to any interests conflicting with Trust Services operations.

ZealiD personnel in Trusted Roles are obliged to follow all required procedures without exceptions as defined in practice statements.

5.3.2. 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 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, minimum bi-annually, with dedicated questionnaires.

5.3.3. 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.

Additionally, employes having Registration Officers' roles undergo specific training that cover at least the following:

- Fraud prevention and detection of forgery;
- Communication training (when the Registration Officer is required to communicate with the applicant);
- Training on software and equipment used;
- Training on verification of documents and their security elements;
- Facial matching.

5.3.4. 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. All Registration Officers in addition receive ongoing training on the specific topics as indicated in the clause 5.3.3 above.

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

5.3.5. Job rotation frequency and sequence

No stipulation

5.3.6. 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 of employment depending on the severity of the unauthorized action. The actions in general follow local labour law stipulation on disciplinary actions.

ZealiD contractors are bound by contractual obligation to carry a financial liability in case of unauthorized actions. ZealiD also has a possibility to terminate a contract early in case of unauthorized actions.

5.3.7. Independent contractor requirements

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

5.3.8. Documentation supplied to personnel

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

5.4. Audit logging procedures

5.4.1. Types of events recorded

ZealiD TRA Service logs at least the following events relating to the registration process:

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 • Firewall and switch activities • Activities of system user with super admin rights • Changes related to security policy • Changes in audit parameters • Encryption key rotation
ZealiD TRA events	• Registration • Backup • Storage • Archival • Destruction • Successful or unsuccessful processing of events • Result • Agent Name • Identification time • Transaction Number • ID number • Fraud reason • Facemap generated after liveness check • Identification changes (whether data was edited by the agent) • Review of changes (whether the data change was reviewed by another agent) • User data (birthday, birth name, city, country, first name, last name, gender,

	nationality, address, personal number (or other serial number)) ● Identity document information (type, expiration date, country, number, issuing authority, date of issue) ● Pictures of ID documents ● Name of receiving TSP
Video Based Registration	● Video sequence of the identity document ● Assigned pattern
NFC Based Registration	● NFC Signature validation result ● NFC Signature ● Personal photo extracted from NFC Chip

Log entries must also include:

- Date and Time
- Identity of the entry generator
- Attribute related to entry type

ZealiD TRA logs of identifications include:

- Identifying document presented during application
- Liveness check output
- When data extracted via NFC:
  - NFC Signatures and validation result
  - Personal photo extracted from NFC Chip
- Data pertaining to session (e.g. smartphone type) at registration
- Third-party document signed with QES supplementing document security features

Copies of applications and identification documents as well as subscriber agreement are securely transferred right after successful identification to the QTSP as part of the evidence package.

CTO reviews key inventory on an annual basis and records this within ISMS Records.

5.4.2. Frequency of processing log

Processing of logs is scheduled at regular intervals depending on the type of log. Instructions related to frequency and work procedure related to a particular logs, is detailed in internal documentation.

Audit logs are reviewed periodically for any evidence of malicious activity and following each important operation.

5.4.3. Retention period for audit log

Audit logs are retained for 12 years. Afterwards the logs are deleted, except for cases where it is legally required to keep logs for a longer period.

5.4.4. Protection of audit log

Audit log is stored encrypted in a dedicated storage within ZealiD infrastructure. Encryption of the log generates an HMAC verification hash to ensure integrity in case of restoration. The access to the audit log is given to a person who does not have administrative or operational access to ZealiD TRA Service hardware or software.

5.4.5. Audit log backup procedures

ZealiD performs regular backups of critical system data, audit log data, and other Sensitive Information. Audit log data backup is part of the general back-up system. ZealiD has defined backup strategy and policies in internal documentation.

5.4.6. Audit collection system (internal vs. external)

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. Manual log entries are generated by ZealiD TRA Service personnel.

5.4.7. Notification to event-causing subject

Notification is not provided automatically for log entries generated by subscribers.

5.4.8. Vulnerability assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. Security vulnerability assessments are performed, reviewed, and revised. These assessments are based on real-time automated logging data and are performed on a daily, monthly, and annual basis.

5.5. Records archival

Documentation related to the ongoing operation of the ZealiD TRA service is archived. The following section relates to the archiving of these documents.

5.5.1. Types of records archived

The following information is archived as a matter of ongoing operations:

- Registration requests (and Certificate requests) to CA;
- Revocation requests made to CA;
- Audit reports e.g. compliance with TSPS;
- All versions of ZealiD TSPS.

In cases where the information is in digital format, and has been digitally signed, all information required to validate the signature is also stored for the duration of the archiving time frame.

Identification data received during the identification process is transferred to the CA and is not archived by ZealiD TRA Service.

5.5.2. Retention period for archive

At least 12 years from the conception of the archive element. In case of Certificate issuance, this is the issuance date, or in case of a formal contract from the date of signing.

5.5.3. Protection of archive

Archives are stored securely and protected from unauthorized viewing, modification or deletion. This is achieved through a combination of physical and/or logical security measures.

Confidential information is not made available to external parties, other than by a court order or where required by law.

All Parties are aware of the rapid pace of development of technology and thereby acknowledge that technology used for archiving or making the archived material available can be made redundant. In such cases where the archived information is more than 12 years old and ZealiD TRA Service has no operational use for the redundant technology - ZealiD TRA Service will be under no obligation to retain this technology. In such a case, ZealiD TRA Service will make necessary equipment available to process the archives at an extra fee equivalent to the cost to ZealiD TRA Service.

5.5.4. Archive backup procedures

Information contained in the archives will be collected from the location of their inception and transferred securely to the location of the archives at regular intervals in time.

5.5.5. Requirements for time-stamping of records

All archived records will be time stamped with the date of their inception or execution.

5.5.6. Archive collection system (internal vs. external)

No stipulation.

5.5.7. Procedures to obtain and verify archive information

Integrity and usability of archives shall be validated at least every 12 months.

5.6. Key changeover

No stipulation.

5.7. Compromise and disaster recovery

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.

5.7.1. Incident and compromise handling procedures

Within the ISMS, an integral part of the ZealiD TRA Service, change and incident management procedures have been developed to allow for a controlled, structured and accountable handling of incidents (including security vulnerabilities or algorithm insufficiencies) as well as recovery from systems or application disasters. Detailed instructions can be found in the ZealiD Incident Management Routine and in the Information Security Management System. Finally, External Communication routine 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, the latter is available on ZealiD website, 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.

ZealiD ensures that CA will be informed within a time period which allows them to meet their 24 hour notification obligation.

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

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 Data Protection Inspectorate without undue delay, but at least in 24 hours after initial discovery of the personal data breach.

5.7.2. Computing resources, software, and/or data are corrupted

In such cases where computing resources, software, and/or data have been identified as corrupt, appropriate steps are taken for incident investigation, appropriate escalation and incident response. If necessary, ZealiD's internal documentation in the ISMS, Compromise and disaster recovery plan may be applied.

5.7.3. Entity private key compromise procedures

No stipulation.

5.7.4. Business continuity capabilities after a disaster

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

ZealiD has implemented ZealiD TRA Service infrastructure in a redundant configuration to minimise the impact of disasters. In addition, important information with respect to restoring the

ZealiD TRA Service is backed up for disaster recovery purposes. In order to recover information that is managed under dual control, dual control is needed also.

5.8. CA or RA termination

5.8.1. RA Termination

ZealiD has a documented Termination Plan for its TRA Service which describes the process of a service termination. Stakeholders affected by any termination will be informed with an advance notice of 3 months by public means and/or ZealiD Website and/or email according to the Termination Plan and Routine External Communication.

5.8.2. CA Termination

No stipulation.

6. Technical security controls

A group of authorized administrators is accountable to implement controls of the security policies. For this task, they have access to a dedicated network segment that is used for administration only.

ZealiD has separate production and development environments.

6.1. Key pair generation and installation

No stipulation.

6.2. Private key protection and cryptographic module engineering controls

No stipulation.

6.3. Other aspects of key pair management

No stipulation.

6.4. Activation data

No stipulation.

6.5. Computer security controls

6.5.1. Specific computer security technical requirements

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

ZealiD TRA service system components are managed in accordance with defined change management procedures. These procedures include system testing in a physically separated test environment and the requirement that changes must be approved by a second authorized person (four eye principle). 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 identification service components against viruses, malware and unauthorised software. A central device management service is used to enforce security policy throughout the workstations.

All media containing production environment software and data, audit, archive, or backup information are stored under control of 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, or 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 is 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. Changes are performed according to internal change management procedures. Hardware maintenance may also be performed by ZealiD contractor personnel that have a Trusted Role status.

ZealiD TRA Service hardware is physically located in a secure location with physical and logical access controls.

Incident response and vulnerability management procedures have been defined. An automated monitoring system detects and alarms in case of abnormal system activities that indicate potential security violation, including intrusion into the network.

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

ZealiD has implemented security measures and enforced access control according to the principle of least-privilege in order to avoid unauthorized access and attempts to add, delete or modify information in applications related to the services.

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

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 annually. When leaving the company,

the withdrawal of access rights takes place within less than 24 hours.

ZealiD's personnel are identified and authenticated before using critical applications related to the services. Multi-factor authentication is required for all accounts capable of performing or reviewing identifications. All users must log in with their personal account, and administrative commands are only available with explicit permission and auditing of the execution. 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 a password management guideline.

Login sessions have a defined timeout.

File system permissions and other features available in the operating system security model are used to prevent unauthorized use.

6.5.2. Computer security rating

ZealiD uses industry-standard computer systems.

6.6. Life cycle technical controls

6.6.1. 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.

6.6.2. Security management controls

ZealiD TRA Service policies, assets and practices (including ZealiD TSPS) 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 TRA Service systems are regularly checked for changes that violate ZealiD TRA Service security policies. A review of configurations of security support systems and front-end/internal support systems occurs continuously, at least on a quarterly basis.

The Security Officer approves changes that have an impact on the level of security provided. The ZealiD TRA 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 six months following the availability of the security patch. In case of a critical vulnerability, the security patch is deployed within 48 hours. The reason for not applying a specific security patch will be documented. Patches may not be deployed due to introducing potentially more severe vulnerabilities, disabling security features that are extensively used to secure ZealiD systems, not being certified or similar.

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.

6.6.3. Life cycle security controls

No stipulation

6.7. Network security controls

The ZealiD network has segments for different systems and / or locations according to risk assessment and the purpose of the system. Networks between data centers are physically separate, while the network segments within the ZealiD Backend system are maintained via logical separation.

Internal traffic between the ZealiD backend systems is transported over internal networks. Other communication may be carried over the public internet. Network traffic is encrypted with TLS where required. Firewalls have been set up specifically denying all traffic that is not explicitly allowed on public-facing interfaces.

Security checks, such as vulnerability scans or patching are done according to a schedule defined in the IT Security Review routine. Any check is performed at least once a year.

Vulnerability and penetration tests are performed by an external specialized company:

- At least once per year for penetration tests; or at least once per quarter for vulnerability test
- After major network or system changes;
- When requested by a relying party or regulating bodies

The transfer of data to the relying party is always encrypted.

The transfer of data to and from a TSP is always TLS encrypted with authentication via dedicated credentials.

There is no physical transfer of data.

ZealiD ensures the secure operation of all technical systems by “hardening”. This includes in particular:

- Removal of unnecessary software/services
- Removal of unnecessary accounts
- Data encryption
- Full-disk encryption

- Multi-factor authentication
- Dual control for administration
- Transport encryption
- Auditing of logs
- Modifying the configurations in regards to security
- If necessary activation of security components
- Protection of network ports

6.8. Time-stamping

All systems have their time with a timezone reference against UTC synchronised through NTP at least daily.

7. Certificate, CRL, and OCSP profiles

No stipulation.

8. Compliance audit and other assessments

8.1. 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 Chapter 1.1 and 9.15).

Conformity is assessed at least yearly and when any major change is made to Trust Service operations and on demand (e.g. by SB).

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

8.2. Identity / qualifications of assessor

ZealiD's CAB is accredited according to ISO/IEC 17065 and ETSI EN 319 403. The CAB is competent to carry out conformity assessments of Qualified Trust Service Providers and its services.

8.3. Assessor's relationship to assessed entity

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

8.4. Topics covered by assessment

The conformity assessment covers the conformity of information systems, 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:

- TSPS, Service Definition, Terms & Conditions, Subscriber Agreement
- TRA Service and systems
- ISMS (Routines, Policies, Controls and Records).

The CAB audits ZealiD protection of subscriber data, accuracy and implementation of security policy, performance of work procedures and contractual obligations, as well as compliance with TSPS.

8.5. Actions taken as a result of deficiency

Depending on the severity of the deficiency the following actions may be taken:

- Auditor may note the deficiency in the report
- An action plan can be developed and steps taken to remedy the deficiency. This could include a revision to the ZealiD TSPS or to applied procedures.
- If the deficiency is judged to have risks for the operation of the ZealiD TRA Service actions has to be taken without any delay.

8.6. 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.

9. Other business and legal matters

9.1. Fees

Users do not pay any fees for using the TRA Service.

Fees for the TRA Service are subject to contractual agreements between ZealiD and its customers.

ZealiD does not charge a fee for reading and or accessing this TSPS. Any other use is not permitted.

9.2. Financial responsibility

The provisions of Swedish law on indemnification are binding for all parties.

ZealiD (ZealiD AB) is audited by PriceWaterhouseCoopers Sweden and meets all requirements of Swedish limited companies.

ZealiD describes its financial stability in internal documentation (Documentation of Financial Stability) - the documentation is updated on an annual basis following financial assessments. The purpose of the assessment is to verify that ZealiD has the resources required to operate in conformity with this PS and the requirements of eIDAS.

The financial responsibility is complemented with multiple insurance types (see below).

9.2.1. Insurance coverage

ZealiD has adequate levels of Professional Liability insurance coverage to support its business practices. Insurance coverage is reviewed annually.

The level of insurance will at minimum be reviewed yearly according to internal routines. For the purpose of meeting eIDAS requirements, insurance certificates are published on https://www.zealid.com/repository.

9.2.2. Other assets

No stipulation.

9.2.3. Insurance or warranty coverage for end-entities

No stipulation.

9.3. Confidentiality of business information

9.3.1. Scope of confidential information

All personal data is considered confidential. Confidential information includes any information provided by subscribers for purposes of identity verification.

All information not required to be public by law, regulation or applicable standards is considered confidential.

ZealiD will disclose information required by law or a court decision.

9.3.2. Information not within the scope of confidential information

Any information not listed as confidential or intended for internal use is public information. ZealiD reserves the right to

publish non-personalised and anonymised statistical data about its services.

9.3.3. Responsibility to protect confidential information

All confidential information will be protected against unauthorized access, modification or deletion using physical, logical and/or procedural security.

9.4. Privacy of personal information

ZealiD TRA Service processes Personal Data in accordance with applicable national legislation (Sweden), and strictly adheres to subscriber rights pertaining to data protection set forth in General Data Protection Regulation (GDPR).

9.4.1. Privacy plan

ZealiD strives to minimize the risks for the individual when processing personal data. ZealiD strictly adheres to the principles and regulations required by GDPR. ZealiD services are designed with privacy in mind.

ZealiD has a GDPR Policy and a data protection officer (DPO) appointed and registered with the Swedish Data Protection Agency. The DPO can be reached at dpo@zealid.com

TRA Service is a subscriber initiated and self-service type process including multiple levels of consent.

9.4.2. Information treated as private

Swedish Data Privacy law and GDPR define what information shall be treated as private. Further information to be treated as private can be contractually agreed upon.

9.4.3. Information not deemed private

Information included in a certificate issued by a CA based on the TRA Service is not deemed private.

9.4.4. Responsibility to protect private information

ZealiD ensures protection of personal information by implementing security controls as described in chapter 5 of this TSPS.

All personnel must protect private information from disclosure to non-authorized parties.

9.4.5. Notice and consent to use private information

ZealiD will use private information only with the explicit notice and consent from the individual owner of the personal data.

ZealiD Subscriber terms & conditions describe under which circumstances the subscriber grants ZealiD his/her notice and consent to use his/her personal data.

9.4.6. Disclosure pursuant to judicial or administrative process

Where ZealiD is required by law, court of law or law enforcement requests to disclose personal data ZealiD will comply. The information shall be given only to the requesting authority or the customers themselves.

9.4.7. Other information disclosure circumstances

No stipulation.

9.5. Intellectual property rights

ZealiD is the exclusive holder of all intellectual property rights to this TSPS.

9.6. Representations and warranties

9.6.1. CA representations and warranties

No stipulation.

9.6.2. RA representations and warranties

ZealiD is a TSP participant in a trust relationship between TSP, Subscribers, Customers and Relying Parties. This TSPS shall form the basis of such a relationship with the following representations and warranties from ZealiD.

ZealiD shall:

- Provide its services consistent with the requirements and the procedures defined in this TSPS and according to the policies under which this TSPS is create;
- Identify, analyse and evaluate risks, and take appropriate measures of treatment accordingly to the results of assessment, ensuring appropriate level of security;
- Review and revise risk assessment at least on a yearly basis;
- Provide and obtain the Management Board approval for the revised risk assessments, as well as all residual risks associated with each risk assessment;
- Be responsible for the effective compliance with the procedures set forth in this TSPS;
- Provide the service in compliance eIDAS regulation and related legal acts and standards;
- Provide publicly published repositories with high electronic availability of all practice statements mentioned in this TSPS;
- Honour its part in ZealiD TRA terms and conditions and secure Subscriber availability and access to the services set out in this TSPS;

- 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 Data Protection Authority (Datainspektionen) 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;
- Preserve all the documentation, records and logs related to Trust Services according to the clauses 5.4 and 5.5;
- 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 TSPS;
- 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 TSPS, in specific contractually adhere to requirements set forth in chapters:

- Facility, Management and Operational Controls 5.1 and 5.1.1 - 5.1.8
- Personal Control 5.3.2 - 5.3.8
- Network security controls 6.7
- Audit 8.4

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

ZealiD further warrants that it manages privacy in accordance with GDPR and that all necessary measures are taken in order to protect the individual and minimize any impact of data processing.

ZealiD will make every reasonable effort to inform relying parties and subscribers of their respective rights and obligations.

9.6.3. Subscriber representations and warranties

Users of the TRA service warrant that all documents, representations and information provided in the registration process are accurate, complete and truthful.

9.6.4. Relying party representations and warranties

No stipulation.

9.6.5. Representations and warranties of other participants

No stipulation

9.7. Disclaimers of warranties

No stipulation.

9.8. Limitations of liability

Limitations of Liability relating to elements of damages recoverable and the amount of damages recoverable shall be stipulated in contractual agreements between ZealiD and its customers.

Limitations of liability stipulated in TRA Service Terms & Conditions apply.

9.9. Indemnities

ZealiD makes no claims as to the suitability of certificates issued under this TSPS for any purpose whatsoever. Relying parties use these certificates at their own risk. ZealiD has no obligation to make any payments regarding costs associated with the malfunction or misuse of certificates issued under this TSPS.

Indemnification regulation under Swedish law is binding.

9.9.1. Indemnification by Subscribers

Users and CAs issuing qualified certificates based on the TRA Service may be required to, if permitted by applicable law, to indemnify ZealiD for:

- failure to disclose a material fact on the identity verification with the intent of deception;
- submission of false or misrepresenting facts on the user identity;
- failure to protect the personal data or to otherwise make necessary effort to prevent the loss, compromise, disclosure, modification, or unauthorised use of the users personal data.

9.10. Term and termination

9.10.1. Term

This ZealiD TSPS becomes effective upon publication and remains valid until such time when a new version or replacement is published, or information to that effect is published on

https://www.zealid.com/repository.

9.10.2. Termination

This TSPS remains in force until a new version is announced and published or when it is terminated due to Trust Service or ZealiD's termination. In the event of ZealiD's or the Trust Service termination, ZealiD is obliged to ensure the protection of personal and confidential information.

9.10.3. Effect of termination and survival

Conditions and effects resulting from the termination of this document will be communicated in the ZealiD TSPS.

The following obligations and limitations of this TSPS shall survive: section 9.6 (Representations and Warranties), section 9.2 (Financial Responsibility), and section 9.3 (Confidentiality of Business Information).

9.11. Individual notices and communications with participants

No stipulation.

9.12. Amendments

9.12.1. Procedure for amendment

ZealiD Management can amend this TSPS. Only changes that do not affect the security level of the described procedures and regulations can be made to this ZealiD TSPS without notice. Changes that do not affect security include linguistic changes and minor rearrangements. Changes can be in the form of an amendment or a new version of the TSPS published to the repository.

9.12.2. Notification mechanism and period

Changes that require notification will be made to this ZealiD TSPS 14 days after notification.

Notification will be published on https://www.zealid.com/repository.

Changes that affect the terms of an agreement with ZealiD TSPS will be notified to the appropriate contact or signatory of the agreement.

9.12.3. Circumstances under which OID must be changed

No stipulation.

9.13. Dispute resolution provisions

ZealiD TRA Service supports CAs with identification for registration purposes. For disputes with users and relying parties the dispute resolution procedures of the issuing CAs apply.

ZealiD provides a simple tool to submit complaints available on the website (https://www.zealid.com/contact). Alternatively ZealiD can be contacted via support@zealid.com.

All disputes between the parties will be settled by negotiations. If parties fail to reach an amicable contract, the dispute will be resolved in the District Court of Stockholm, Sweden.

9.14. Governing law

Applicable law is the law of the Kingdom of Sweden.

9.15. Compliance with applicable law

ZealiD Statement of Applicability for its TRA Service include primarily:

- 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
- 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) effective from 2018-05-25

9.16. Miscellaneous provisions

9.16.1. Entire agreement

No stipulation.

9.16.2. Assignment

No stipulation.

9.16.3. Severability

Should parts of any of the provisions in this TSPS be deemed incorrect or invalid, this shall not affect the validity of the remaining provisions until the TSPS is updated.

The process for updating this TSPS is described in section 9.12.

9.16.4. Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5. Force Majeure

ZealiD and other parties cannot be held responsible for any consequences caused by circumstances beyond his 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 TSPS and/or relevant service-related Policies and/or Practice Statements is not considered a violation if such non-fulfilment is occasioned by Force Majeure.

None of the parties shall claim damage or any other compensation from the other parties for delays or non-fulfilment of this TSPS and/or relevant service-related Policies and/or Practice Statements caused by Force Majeure.

9.17. Other provisions

No stipulation.