ZealiD QeID Service Certificate Practice Statement

Table of Contents

1. INTRODUCTION **12**
1.1. Overview 12
1.2. Document name and identification 13
1.3. PKI participants 13
1.3.1. Certification authorities 14
1.3.2. Registration authorities 14
1.3.3. Subscribers 14
1.3.4. Relying parties 14
1.3.5. Other participants 14
1.4. Certificate usage 14
1.4.1. Appropriate certificate uses 14
1.4.2. Prohibited certificate uses 15
1.5. Policy administration 15
1.5.1. Organization administering the document 15
1.5.2. Contact person 15
1.5.3. Person determining CPS suitability for the policy 15
1.5.4. CPS approval procedures 16
1.6. Definitions and acronyms 16
1.6.1. Definitions 16
1.6.2. Acronyms 20
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES **22**
2.1. Repositories 22
2.2. Publication of certification information 22
2.3. Time or frequency of publication 23
2.4. Access controls on repositories 23
3. IDENTIFICATION AND AUTHENTICATION (I&A) **24**
3.1. Naming 24
3.1.1. Types of names 24
3.1.1.1. Subscriber 24
3.1.1.2. Issuing CA 24
3.1.2. Need for names to be meaningful 25
3.1.3. Anonymity or pseudonymity of Subscribers 25
3.1.4. Rules for interpreting various name forms 25
3.1.5. Uniqueness of the names 25

3.1.6. Recognition, authentication, and role of trademarks 25
3.2. Initial identity validation 25
3.2.1. Method to prove possession of private key 25
3.2.2. Authentication of organization identity 26
3.2.3. Authentication of individual identity 26
3.2.4. Non-verified Subscriber information 27
3.2.5. Validation of authority 27
3.2.6. Criteria for interoperation 27
3.3. Identification and authentication for re-key requests 27
3.3.1. Identification and authentication for routine re-key 27
3.3.2. Identification and authentication for re-key after revocation 27
3.4. Identification and authentication for revocation request 27
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 27
4.1. Certificate Application 27
4.1.1. Who can submit a certificate application 27
4.1.2. Enrollment process and responsibilities 28
4.1.3. QSCD and Annual Control 29
4.2. Certificate application processing 29
4.2.1. Performing identification and authentication functions 29
4.2.2. Approval or rejection of certificate applications 30
4.2.3. Time to process certificate applications 30
4.3. Certificate issuance 30
4.3.1. CA actions during certificate issuance 30
4.3.2. Notification to Subscribers by the CA of issuance of certificate 31
4.4. Certificate acceptance 31
4.4.1. Conduct constituting certificate acceptance 31
4.4.2. Publication of the certificate by the CA 32
4.4.3. Notification of certificate issuance by the CA to other entities 32
4.5. Key pair and certificate usage 32
4.5.1. Subscriber private key and Certificate usage 32
4.5.2. Relying party public key and Certificate usage 32
4.6. Certificate renewal 33
4.6.1. Circumstance for certificate renewal 33
4.6.2. Who may request renewal 33
4.6.3. Processing certificate renewal requests 33
4.6.4. Notification of new certificate issuance to subscriber 33

4.6.5. Conduct constituting acceptance of a renewal certificate 33
4.6.6. Publication of the renewal certificate by the CA 33
4.6.7. Notification of certificate issuance by the CA to other entities 33
4.7. Certificate re-key 34
4.7.1. Circumstance for certificate re-key 34
4.7.2. Who may request certification of a new public key 34
4.7.3. Processing certificate re-keying requests 34
4.7.4. Notification of new certificate issuance to subscriber 34
4.7.5. Conduct constituting acceptance of a re-keyed certificate 34
4.7.6. Publication of the rekeyed certificate by the CA 34
4.7.7. Notification of certificate issuance by the CA to other entities 34
4.8. Certificate modification 34
4.8.1. Circumstance for certificate modification 35
4.8.2. Who may request certificate modification 35
4.8.3. Processing certificate modification requests 35
4.8.4. Notification of new certificate issuance to subscriber 35
4.8.5. Conduct constituting acceptance of modified certificate 35
4.8.6. Publication of the modified certificate by the CA 35
4.8.7. Notification of certificate issuance by the CA to other entities 35
4.9. Certificate revocation and suspension 35
4.9.1. Circumstances for revocation 35
4.9.2. Who can request revocation 36
4.9.3. Procedure for revocation request 37
4.9.4. Revocation request grace period 38
4.9.5. Time within which CA must process the revocation request 38
4.9.6. Revocation checking requirement for Relying parties 39
4.9.7. CRL issuance frequency (if applicable) 39
4.9.8. Maximum latency for CRLs (if applicable) 39
4.9.9. On-line revocation/status checking availability 39
4.9.10. On-line revocation checking requirements 39
4.9.11. Other forms of revocation advertisements available 39
4.9.12. Special requirements re key compromise 39
4.9.13. Circumstances for suspension 40
4.9.14. Who can request suspension 40
4.9.15. Procedure for suspension request 40
4.9.16. Limits on suspension period 40

4.10. Certificate status services 40
4.10.1. Operational characteristics 40
4.10.2. Service availability 40
4.10.3. Optional features 41
4.11. End of subscription 41
4.12. Key escrow and recovery 41
4.13. Key escrow and recovery policy and practices 41
4.14. Session key encapsulation and recovery policy and practices 41
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 41
5.1. Physical controls 42
5.1.1. Site location and construction 42
5.1.2. Physical access 43
5.1.3. Power and air conditioning 43
5.1.4. Water exposures 44
5.1.5. Fire prevention and protection 44
5.1.6. Media storage 44
5.1.7. Waste disposal 44
5.1.8. Off-site backup 44
5.2. Procedural controls 45
5.2.1. Trusted roles 45
5.2.2. Number of persons required per task 46
5.2.3. Identification and authentication for each role 48
5.2.4. Roles requiring separation of duties 48
5.3. Personnel controls 48
5.3.1. Qualifications, experience, and clearance requirements 48
5.3.2. Background check procedures 49
5.3.3. Training requirements 50
5.3.4. Retraining frequency and requirements 50
5.3.5. Job rotation frequency and sequence 51
5.3.6. Sanctions for unauthorized actions 51
5.3.7. Independent contractor requirements 51
5.3.8. Documentation supplied to personnel 51
5.4. Audit logging procedures 51
5.4.1. Types of events recorded 51
5.4.2. Frequency of processing log 53
5.4.3. Retention period for audit log 54

5.4.4. Protection of audit log 54
5.4.5. Audit log backup procedures 54
5.4.6. Audit collection system (internal vs. external) 54
5.4.7. Notification to event-causing subject 55
5.4.8. Vulnerability assessments 55
5.5. Records archival 55
5.5.1. Types of records archived 55
5.5.2. Retention period for archive 55
5.5.3. Protection of archive 56
5.5.4. Archive backup procedures 56
5.5.5. Requirements for time-stamping of records 56
5.5.6. Archive collection system (internal or external) 56
5.5.7. Procedures to obtain and verify archive information 56
5.6. Key changeover 57
5.7. Compromise and disaster recovery 57
5.7.1. Incident and compromise handling procedures 57
5.7.2. Computing resources, software, and/or data are corrupted 59
5.7.3. Entity private key compromise procedures 59
5.7.4. Business continuity capabilities after a disaster 59
5.8. CA or RA termination 59
5.8.1. RA termination 59
5.8.2. CA termination 60
6. TECHNICAL SECURITY CONTROLS 61
6.1. Key pair generation and installation 61
6.1.1. Key pair generation 62
6.1.1.1. ZealiD QeID Infrastructure Keys 62
6.1.1.2. ZealiD Subscriber Key pair 63
6.1.2. Private key delivery to Subscriber 63
6.1.3. Public key delivery to certificate issuer 64
6.1.4. CA public key delivery to relying parties 64
6.1.5. Key sizes 64
6.1.6. Public key parameters generation and quality checking 64
6.1.7. Key usage purposes (as per X.509 v3 key usage field) 65
6.2. Private Key Protection and Cryptographic Module Engineering Controls 65
6.2.1. Cryptographic module standards and controls 65
6.2.2. Private key (n out of m) multi-person control 66

6.2.3. Private key escrow 66
6.2.4. Private key backup 66
6.2.5. Key Restoration 66
6.2.6. Private key archival 67
6.2.7. Private key transfer into or from a cryptographic module 67
6.2.8. Private key storage on cryptographic module 67
6.2.9. Method of activating private key 67
6.2.9.1. Method of activating service private key 67
6.2.9.2. Method of activating subscriber private key 67
6.2.10. Method of deactivating private key 68
6.2.11. Method of destroying private key 69
6.2.12. Cryptographic Module Rating 69
6.3. Other aspects of key pair management 69
6.3.1. Public key archival 69
6.3.2. Certificate operational periods and key pair usage periods 69
6.4. Activation data 70
6.4.1. Activation data generation and installation 70
6.4.2. Activation data protection 70
6.4.3. Other aspects of activation data 70
6.5. Computer security controls 70
6.5.1. Specific computer security technical requirements 70
6.5.2. Computer security rating 72
6.6. Life cycle technical controls 73
6.6.1. System development controls 73
6.6.2. Security management controls 73
6.6.3. Life cycle security controls 73
6.7. Network security controls 74
6.8. Time-stamping 75
7. CERTIFICATE, CRL, AND OCSP PROFILES 76
7.1. Certificate profile 76
7.2. CRL profile 77
7.3. OCSP profile 77
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 77
8.1. Frequency or circumstances of assessment 77
8.2. Identity/qualifications of assessor 77
8.3. Assessor's relationship to assessed entity 77

8.4. Topics covered by assessment 78
8.5. Actions taken as a result of deficiency 78
8.6. Communication of results 78
9. OTHER BUSINESS AND LEGAL MATTERS 79
9.1. Fees 79
9.1.1. Certificate issuance or renewal fees 79
9.1.2. Certificate access fees 79
9.1.3. Revocation or status information access fees 79
9.1.4. Fees for other services 79
9.1.5. Refund policy 79
9.2. Financial responsibility 79
9.2.1. Insurance coverage 80
9.2.2. Other assets 80
9.2.3. Insurance or warranty coverage for end-entities 80
9.3. Confidentiality of business information 80
9.3.1. Scope of confidential information 80
9.3.2. Information not within the scope of confidential information 80
9.3.3. Responsibility to protect confidential information 80
9.4. Privacy of personal information 80
9.4.1. Privacy plan 80
9.4.2. Personal data processed 81
9.4.3. Information not deemed private 81
9.4.4. Responsibility to protect personal data 81
9.4.5. Notice and consent to use personal data 81
9.4.6. Disclosure pursuant to judicial or administrative process 81
9.4.7. Other information disclosure circumstances 81
9.5. Intellectual property rights 81
9.6. Representations and warranties 81
9.6.1. CA representations and warranties 81
9.6.2. RA representations and warranties 84
9.6.3. Subscriber representations and warranties 84
9.6.4. Relying party representations and warranties 85
9.6.5. Representations and warranties of other participants 85
9.7. Disclaimers of warranties 85
9.8. Limitations of liability 86
9.9. Indemnities 86

9.10. Term and termination 86
9.10.1. Term 86
9.10.2. Termination 86
9.10.3. Effect of termination and survival 86
9.11. Individual notices and communications with participants 87
9.12. Amendments 87
9.12.1. Procedure for amendment 87
9.12.2. Notification mechanism and period 87
9.12.3. Circumstances under which OID must be changed 87
9.13. Dispute resolution provisions 87
9.14. Governing law 87
9.15. Compliance with applicable law 87
9.16. Miscellaneous provisions 89
9.16.1. Entire contract 89
9.16.2. Assignment 89
9.16.3. Severability 89
9.16.4. Enforcement 89
9.16.5. Force Majeure 90

Revision History

Date	Revision	Comment	Contributor
2019-06-21	01	Re Formatting from document	Philip Hallenborg
2019-06-21	02	Published	Philip Hallenborg
2019-06-27	03	Chapters 4.1, 4.2, 4.4, 4.6, 4.7, 4.8	Tomas Zuoza
2019-06-27	04	Wording, adding 4,5,6 parts	Philip Hallenborg
2019-07-03	05	Wording Chapter 4	Philip Hallenborg/Jenny Dybedahl
2019-07-03	06	Chapters 5.4, 5.5	Tomas Zuoza/Ignas Karpiejus
2019-07-15	07	Input	May-Lis Farnes
2019-07-17	08	Review and chapters 6, 7	Tomas Zuoza
2019-07-17	09	Review naming, links	Philip Hallenborg
2019-07-23	10	Review, links, 2.2 update	May-Lis Farnes /Philip Hallenborg
2019-07-24	11	Name change	Philip Hallenborg
2019-07-25	12	Update CRL information	Ignas Karpiejus
2019-09-03	13	Update Certificate Policy Scope	Philip Hallenborg
2019-11-09	14	Update from TSPS TRA	Philip Hallenborg
2019-11-11	15	Updates Compliance Table	Tomas Zuoza/Philip Hallenborg
2020-05-28	16	Multiple updates	Tomas Zuoza/ Ignas Karpiejus/ Philip Hallenborg
2021-08-12	17	1.4.1 chapter changed to include batch signing option; 4.5.1 chapter updated to reflect that there are multiple signature formats support for Subscriber signing	Tomas Zuoza
2022-06-01	18	Multiple updates	Tomas Zuoza
2023-02-15	19	Chapter 9.6.2 update	Enrika Masalskiene
2023-06-05	20	Chapter 4.9.5, 5.2.1, 5.3.4 update	Enrika Masalskiene, Tomas Zuoza

2024-04-22	21	5.4.1 updated list of General RA events 5.8.2 updated with more detailed description of CA termination 6.2.9.3 minor update on description of mobile device-native biometrics 6.6.3 HSM clearance statement added 7.1 updated with the reference to ETSI TS 119 312	Enrika Masalskiene, Tomas Zuoza, Robert Hoffmann

1. INTRODUCTION

ZealiD AB, SE556972-4288, (ZealiD) was founded in 2014. It is a Swedish limited liability company (Aktiebolag) held 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 Authority for Privacy Protection (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

ZealiD is a Certificate Authority (CA) and issues qualified certificates and electronic signatures to subscribers.

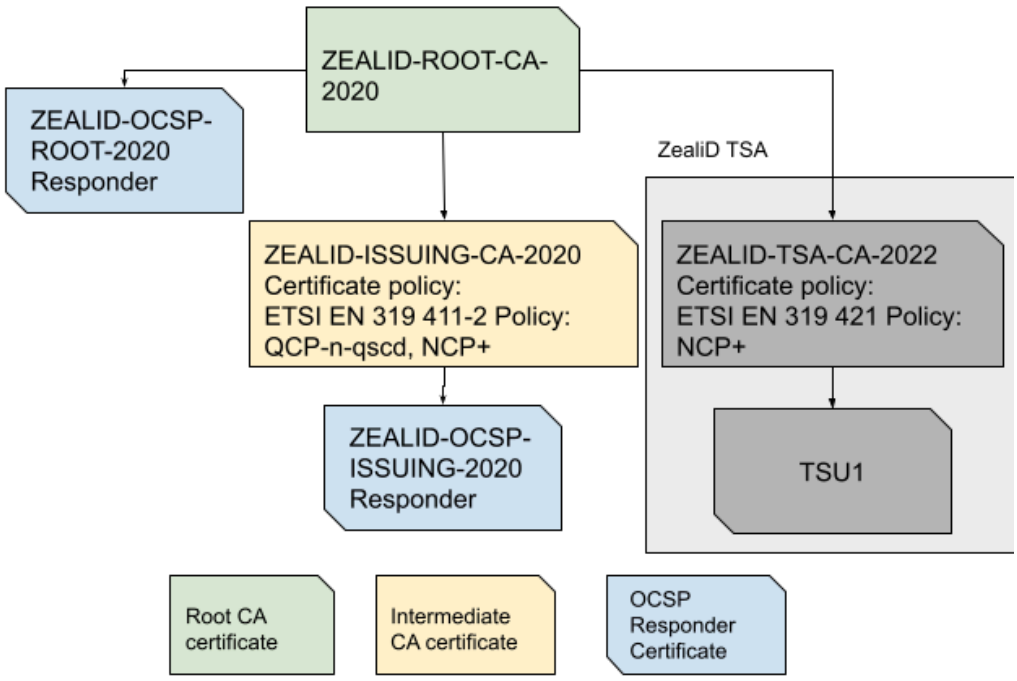
This Certificate Practice Statement (CPS) describes the practices for ZealiD's "ZealiD QeID Service".

It is based on the following applicable Certificate Policy (CP):

- QCP-n-qscd of ETSI EN 319 411-2
- NCP+

ZealiD currently uses this certificate chains:

- "ZealiD Root CA 2020", valid 2020-2050



Certificates issued by ZealiD QeID Service will be used for

- Providing software based electronic identities (electronic ID) in smartphone applications
- Subscriber non-repudiation electronic signing
- Subscriber authentication

This CPS is based on the structure suggested by Certification Practice Framework IETF RFC 3647. Section order and headings have been kept as close as possible to the suggested framework.

1.2. Document name and identification

This CPS is titled “ZealiD QeID Certificate Practice Statement”. The Issuing CPS has the object identifier: OID 1.2.752.251.1.5.51.1.21.

1.3. PKI participants

ZealiD QeID Service will issue certificates to subscribers in order to provide software based IDs, non-repudiation signing and subscriber strong authentication.

1.3.1. Certification authorities

ZealiD is the issuing CA. The name of the CA in the “Issuer” field of the CA certificate is “ZealiD Root CA 2020”.

1.3.2. Registration authorities

Registration authorities (RA) refer to the entities that establish identity proofing procedures for end-user certificate applicants, perform identification and authentication of certificate applicants, initiate or pass along revocation requests for certificates, and approve applications for renewal or re-keying of certificates on behalf of a CA.

RAs may be external to the CA.

Identified RAs for this CPS is:

- ZealiD TRA Service (Certified eIDAS RA)

1.3.3. Subscribers

The subscribers identified in this CPS are natural persons within the scope of their electronic identity. Certificates and signatures are issued to natural persons where the subscriber and the subject are identical.

1.3.4. Relying parties

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 QeID Service (CA).

1.3.5. Other participants

No stipulation.

1.4. Certificate usage

1.4.1. Appropriate certificate uses

Certificates under this CPS are issued to Subscribers for non-repudiation signing, strong authentication and issuance of electronic identities that will be issued to end-users.

Batch signing is enabled on a per customer basis. When signing multiple documents at the same time, the Subscribers are informed within the

ZealiD App of the number of documents and the party that is requesting the signatures.

1.4.2. Prohibited certificate uses

Applications using the certificates issued under this CPS must consider the key usage purpose stated in the “Key Usage” extension field in the certificate.

ZealiD CA Service Signing Keys used for generating subscriber certificates, and/or issuing revocation status information, shall not be used for any other purpose.

1.5. Policy administration

1.5.1. Organization administering the document

This CPS 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

1.5.2. Contact person

Compliance Manager
Email: legal@zealid.com

1.5.3. Person determining CPS suitability for the policy

Compliance Manager determines suitability. Compliance Manager is responsible to review and propose updates to the CPS such that it is reviewed regularly, updated at least once per year or more frequently should regulatory changes arise as per Chapter 2.3.

1.5.4. CPS approval procedures

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

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

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

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

The amended CPS 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.

1.6. Definitions and acronyms

1.6.1. Definitions

Term	Definition
Authentication	Unique identification of a person by checking his/her alleged identity.
Certificate	Public Key, together with additional information, laid down in the Certificate Profile.
Certificate Authority	A part of the trust service provider's structure responsible for issuing and verifying electronic Certificates and Certificate Revocation Lists with its electronic signature. ZealiD has created the

	ZealiD QeID Service that issues Certificates under this CPS.
Certificate Pair	A pair of Certificates consisting of one Authentication Certificate and one Qualified Electronic Signature Certificate.
Certificate Policy	A set of rules that indicates applicability of a specific Certificate to a particular community and/or PKI implementation with common security requirements.
Certification Practice Statement	One of the several documents that all together form the governance framework in which Certificates are created, issued, managed, and used.
Certificate Profile	Document that determines the information contained within a Certificate as well as the minimal requirements towards the Certificate.
Certificate Revocation List	A list of invalid (revoked or suspended) Certificates. A CRL contains suspended and revoked Certificates during their validity period, i.e. until they expire.
CA Service	Trust service related to issuing Certificates, managing suspension, termination of suspension, revocation, modification and re-key of the Certificates. In this CPS 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 CA Services
Directory Service	Trust service related to publication of Certificate validity information.

Distinguished name	Unique Subject name in the infrastructure of Certificates.
Encrypting	Information treatment method changing the information unreadable for those who do not have the necessary skills or rights.
ZealiD	ZealiD AB, the legal entity and provider behind the Trust Service and CA Service.
ZealiD App	The brand name is used facing consumers, Customers, Relying parties and the market in general.
ZealiD QeID Service	The specific name of the CA Service issuing qualified electronic signatures.
ZealiD TRA Service	Trust service related to the identification and authentication for ZealiD QeID Service.
Integrity	A characteristic of an array: information has not been changed since the array was created.
Object Identifier	An identifier used to uniquely name an object (OID).
PIN code	Activation code for the Authentication Certificate and for the Qualified Electronic Signature Certificate.
Private Key	The key of a key pair that is assumed to be kept secret by the subscriber of the key pair, and that is used to create electronic signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key	The key of a key pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by Relying Parties to verify electronic signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
Qualified Certificate	A certificate for electronic signatures that is issued by the qualified trust service provider and meets the requirements laid down in Annex I of the eIDAS Regulation.
Qualified Electronic Signature	Advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a Qualified Certificate for electronic signatures.
Qualified Electronic Signature Creation Device	A Secure Signature Creation Device that meets the requirements laid down in eIDAS Regulation.
Relying Party	Relying parties are defined as any Subscriber (as defined in Subscribers below) or any end-entity (also referred to as Customers) relying on the Certificate issued by the ZealiD QeID Service (CA).
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 Certificates. The Subscriber has to be familiar with the document and accept the Terms and Conditions upon submitting an application for the Certificate based services.

1.6.2. Acronyms

Acronym	**Definition**
CA	Certificate Authority
CAB	Conformity Assessment Body (eIDAS)
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
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”)
NCP+	Normalised Certificate Policy requiring a Secure Cryptographic Device from ETSI EN 319 411-1
OCSP	Online Certificate Status Protocol
OID	Object Identifier, a unique object identification code
PKI	Public Key Infrastructure
PTS	Swedish Post & Telecoms Authority
QSCD	Qualified Electronic Signature Creation Device
QCP-n-qscd	Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD from ETSI EN 319 411-2 [5]
RA	Registration Authority
SB	Supervisory Body (eIDAS) - see PTS
TRA Service	Trusted Registration Authority Service provided by ZealiD under the brand name ZealiD

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

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), available at https://zealid.com/repository, the following documents:

- ZealiD QeID CPS (this document)
- ZealiD QeID Service Description
- QeiD Terms and Conditions
- Audit results
- Insurance policies
- Certificates (rootCA, issuingCA and OCSP)
- Test Certificates (rootCA, issuingCA, Subscriber Authentication, Subscriber Signing and OCSP)
- Profiles

ZealiD has a User Portal for Subscribers, it is available 24/7 with 99% annual availability, which is contractually guaranteed by the hosting provider and provisions are made to be able to host via a secondary provider in case of emergency. The Portal can be reached at: https://my.zealid.com.

In the User Portal the Subscriber can find the following information:

- Personal data processed by ZealiD
- Signed Subscriber Agreement with Terms and Conditions
- Subscriber Certificates for retrieval

2.2. Publication of certification information

ZealiD makes the following documents publicly available:

- QeID Practice Statement (this CPS)
- Audit results
- Insurance policies

- Certificates, including root certificates and CA certificates under which certificates for subscribers are issued
- Test Certificates
- Profiles
- Terms and Conditions ZealiD QeID
- Online Certificate Status Protocol

A published Online Certificate Status Protocol (OCSP) will contain all processed revocation information at the time of publication. Publication of revocation information is according to the provisions found in section 4.9. Publication of information will be within the limitations stipulated in sections 9.3 and 9.4.

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

ZealiD provides the capability to allow third parties to check and test certificates it issues. Test Certificates clearly indicate that they are for testing purposes.

2.3. Time or frequency of publication

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

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

Upcoming changes will be made public minimum 14 days in advance.

Subscribers and Relying parties will be notified via the ZealiD public repository and further according to the ZealiD Routine External Comunication 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. The CEO and CPO are the only ones who can edit the CPS prior approval. All CPS versions are subject to final confirmation and approval by the ZealiD Management Board before publication. Publishing into ZealiD's repository is restricted to the CEO and CPO of ZealiD with multi-factor authentication access.

ZealiD User Portal can be accessed only by logging in with ZealiD App.

3. IDENTIFICATION AND AUTHENTICATION (I&A)

3.1. Naming

3.1.1. Types of names

3.1.1.1. Subscriber

Type of names assigned to the Subscriber is described in the Certificate Profile.

3.1.1.2. Issuing CA

Attribute	Value
Common Name	ZealiD Issuing CA 2020
Organization	ZealiD AB
Organisation Identifier	SE556972-4288
Country	SE
Address	Box 3437, Stockholm

Postcode	11156
Email	support@zealid.com

3.1.2. Need for names to be meaningful

All the values in the Subscriber information section of a Certificate are meaningful. Meaning of names in different fields of the Certificates is described in the Certificate Profile.

3.1.3. Anonymity or pseudonymity of Subscribers

Anonymity or pseudonymity of Subscribers is not allowed.

3.1.4. Rules for interpreting various name forms

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 the names

Subscriber's distinguished name is compiled according to the profile described in the Certificate Profile. ZealiD does not issue Certificates with an identical Common Name (CN), Serial Number (S) for different subjects.

3.1.6. Recognition, authentication, and role of trademarks
Trademarks are not allowed.

3.2. Initial identity validation

3.2.1. Method to prove possession of private key

Registration processes are conducted by certified eIDAS RAs. Once a registration is completed, the Subscriber's key pair is linked to the mobile device. For more information see section 6.1.2 of this CPS.

3.2.2. Authentication of organization identity
No stipulation.

3.2.3. Authentication of individual identity

A certified eIDAS RA collects the data necessary for identity proofing and verification of the Subscriber. This data is submitted to ZealiD QeID Service.

At present the certified RA is ZealiD TRA Service. Registration is made according to the ZealiD Trusted Registration Authority Practice Statement chapter 3.

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 collected.

The TRA service performs the identification of individual identity according to ETSI TS 119 461.

Where physical ID documents are used for the applicant identification, the TRA service fulfills 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).

The RA service verifies the identification of the individual identity and submits the data listed under section 5.4 “RA Events” in this CPS to ZealiD QeID Service.

3.2.4. Non-verified Subscriber information
Non-verified Subscriber information is not allowed in the Certificate.

3.2.5. Validation of authority
Representation of the Subscriber is not allowed.

3.2.6. Criteria for interoperation
No stipulation.

3.3. Identification and authentication for re-key requests

No stipulation.

3.3.1. Identification and authentication for routine re-key
No stipulation.

3.3.2. Identification and authentication for re-key after revocation
No stipulation.

3.4. Identification and authentication for revocation request

Please refer to section 4.9.3 of this CPS.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

4.1.1. Who can submit a certificate application

Any natural person can submit a certificate application to ZealiD via a contracted RA service.

The current RAs for ZealiD QeID service is the video identification RA service of ZealiD TRA Service.

The Subscriber submits an application for two certificates (signing and authentication) via the RA Service.

ZealiD accepts Certificate requests only from contracted external RA Services or its own ZealiD TRA Service.

The RAs are responsible for prevention of not acceptable applicants (e.g. minors) as part of identification processes.

4.1.2. Enrollment process and responsibilities

The registration and setup of subscribing applicants is done remotely (self-service) by the Subscriber in a process provided by the RA service. The RA Service needs to be certified to meet the requirements on Authentication of Subscribers by:

- Identifying Subscribers according to eIDAS article 24, 1d and
- being conformant with security level and level of assurance recognized in EU member state national law.

Subscriber applicants need to submit sufficient information to allow Issuing CAs and RAs to successfully perform the required verification. Issuing CAs and RAs shall protect communications and store information presented by the Applicant during the application process according to their practice statements.

QeID Service ensures Subscriber acceptance of the Terms and Conditions, and makes Subscriber aware of recommended security precautions in the registration process related to:

- the ZealiD App,
- mobile device,
- authentication process,
- usage of the authorization key usage,
- processing of personal data,
- and duties related to loss or compromise of the private key.

This is done by requiring the Subscriber to actively accept Subscriber agreement and its related Terms and Conditions by marking a checkbox.

4.1.3. QSCD and Annual Control

ZealiD QeID Service operates its HSM in combination with a SAM that is certified according to EAL4 + in accordance with ISO / IEC 15408.

ZealiD monitors certification status of QSCDs in use and quarterly checks that QSCD is recognised by verifying the validity of eIDAS Certificate issued for the QSCD or that it is continuously valid
in the European Commission's list of Secure Signature Creation Devices and Qualified Signature Creation Devices notified by the EU member states.

If the validity in the European Commission's list of Secure Signature Creation Devices and Qualified Signature Creation Devices notified by the EU member states is expired due to the modification, then ZealiD will investigate the cause of the modification from the responsible member state or/and designated certification body. If the QSCD certificate is expired or invalidated, then ZealiD will take the following actions:

- notify immediately its supervisory body and conformity assessment body (CAB)
- revoke any affected certificates;
- inform all affected Subscribers and Relying parties.

4.2. Certificate application processing

4.2.1. Performing identification and authentication functions

The RA Service validates the Subscriber's identity as described in the RA TSPS. RA Service sends the Certificate requests to ZealiD QeID Service. Application for a Subscriber will be generated automatically via the RA Service. All communications shall be securely stored 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.

4.2.2. Approval or rejection of certificate applications

Applications are done by the Subscriber registering in the RA service using the ZealiD smartphone app. The acceptance or rejection of a Subscriber application is determined by the RA Service.

Subscriber applications will be approved if they meet the requirements in this CPS and those set forth in the RA Service TSPS. And where there is no other reason for rejection.

In case of rejection, a Subscriber will be informed as part of the RA Service as to the reason for the rejection decision, and provided details as to how to proceed for an approval.

ZealiD shall reject applications for Certificates where validation of all items cannot successfully be completed.

4.2.3. Time to process certificate applications

Applications are processed automatically by ZealiD QeID Service immediately after the application is submitted from the RA Service.

4.3. Certificate issuance

4.3.1. CA actions during certificate issuance

After verifying that the Subscriber's identification data in the Certificate request matches with the identification data in the data set, ZealiD QeID Service automatically issues the corresponding Certificates.

4.3.2. Notification to Subscribers by the CA of issuance of certificate

The Subscriber will be notified of issuance of certificate with a message within the ZealiD smartphone app immediately and a separate text message sent to the mobile number provided during registration.

4.4. Certificate acceptance

4.4.1. Conduct constituting certificate acceptance

ZealiD QeID Service shall inform the Subscriber that s/he may not use the Certificates until the Subscriber has reviewed and verified the accuracy of the data incorporated into the Certificates. To avoid this being an open-ended stipulation, the issuing service may set a time limit by when the Certificates shall be accepted, otherwise the Subscriber will have to start the process from the beginning.

Terms and Conditions are made available to the Subscriber via the ZealiD App prior acceptance.

The Subscriber after a successful identification process is presented with a screen in the ZealiD App which requests the Subscriber to verify the data in the authentication and signing certificates and accept Terms and Conditions with a subscriber agreement prior to signing a Subscriber Agreement with a copy of their identity documents inside. In order to do that, the Subscriber is presented with the details of certificates on screen and a link to the Subscriber agreement. When the Subscriber verifies the details and selects a checkbox to indicate acceptance of terms and conditions, it is then possible to click the “Sign Documents” button. The Subscriber sees on that screen the data from a CSR for the Certificates which they shall verify prior accepting terms and conditions and clicking sign, ZealiD processes the certification request and then asks the Subscriber by displaying a signing authorisation screen (with a signing request that includes data from the certificates) to use the signing keys generated to sign the Subscriber Agreement.

Once the Subscriber verifies accuracy of data and confirms the Subscriber Agreement with the Terms and Conditions, the Certificates are deemed as accepted. The consent and acceptance is logged.

After the Subscriber Agreement was signed, they are available and downloadable within the ZealiD application, User Portal. A public version can be downloaded from ZealiD Repository.

4.4.2. Publication of the certificate by the CA

ZealiD QeID Service does not publish Subscriber Certificates. Certificate validity can be checked through OCSP service.

4.4.3. Notification of certificate issuance by the CA to other entities

ZealiD QeID service will by means of secure data communication inform the RA Service responsible for the application processing of the certificate issuance.

4.5. Key pair and certificate usage

4.5.1. Subscriber private key and Certificate usage

The Subscriber is required to use the Certificate and Private Key lawfully and in accordance with:

- this CPS;
- the Subscriber Terms and Conditions ZealiD QeID;
- the RA Service Terms and Conditions;
- the TSPS of the RA Service.

Subscriber can use the signing key pair for signing using various signature formats.

Subscriber can use an authentication key pair for hash signing with sha256 hashing algorithm.

Signature padding in both cases is PKCS#1v1.5.

4.5.2. Relying party public key and Certificate usage

The Relying Party is required to use the Public Key and Certificate lawfully and in accordance with:

- this CPS;
- the ZealiD QeID Terms and Conditions.

4.6. Certificate renewal

Renewal of Certificates is not allowed.

4.6.1. Circumstance for certificate renewal

No stipulation.

4.6.2. Who may request renewal

No stipulation.

4.6.3. Processing certificate renewal requests

No stipulation.

4.6.4. Notification of new certificate issuance to subscriber

No stipulation.

4.6.5. Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6. Publication of the renewal certificate by the CA

No stipulation.

4.6.7. Notification of certificate issuance by the CA to other entities

No stipulation.

4.7. Certificate re-key

Certificate Re-Key initiated by the Subscriber is considered to be a new application and processed accordingly. Certificate re-key is not allowed.

4.7.1. Circumstance for certificate re-key

No stipulation.

4.7.2. Who may request certification of a new public key

No stipulation.

4.7.3. Processing certificate re-keying requests

No stipulation.

4.7.4. Notification of new certificate issuance to subscriber

No stipulation.

4.7.5. Conduct constituting acceptance of a re-keyed certificate

No stipulation.

4.7.6. Publication of the rekeyed certificate by the CA

No stipulation.

4.7.7. Notification of certificate issuance by the CA to other entities

No stipulation.

4.8. Certificate modification

Modification is processed as a new application and not allowed.

4.8.1. Circumstance for certificate modification

No stipulation.

4.8.2. Who may request certificate modification

No stipulation.

4.8.3. Processing certificate modification requests

No stipulation.

4.8.4. Notification of new certificate issuance to subscriber

No stipulation.

4.8.5. Conduct constituting acceptance of modified certificate

No stipulation.

4.8.6. Publication of the modified certificate by the CA

No stipulation.

4.8.7. Notification of certificate issuance by the CA to other entities

No stipulation.

4.9. Certificate revocation and suspension

4.9.1. Circumstances for revocation

If the Subscriber loses control over his/her Private key or mobile device, the Subscriber shall apply for Certificate revocation immediately.

ZealiD QeID Service revokes Subscriber's or CA's Certificates and Private keys if one or more of the following circumstances occurs:

- the Subscriber requests revocation using the ZealiD App or Site;
- the Subscriber has blocked the device PIN code;

- ZealiD obtains a report that the Subscriber has lost control over Private Keys or mobile device;
- the Subscriber notifies that the original Certificate request was not authorised and does not retroactively grant authorisation;
- ZealiD obtains a report that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a key compromise or no longer complies with the requirements;
- ZealiD obtains a report that the Certificate was misused; the service is made aware that the Subscriber has violated one or more of its obligations under the Terms and Conditions;
- ZealiD is made aware of any change (e.g. surname change) in the information contained in the Certificate;
- ZealiD is made aware that the Certificate was not issued in accordance with the CPS and/or CP;
- ZealiD obtains a report that a Certificate is no longer compliant with CP under which it has been issued;
- ZealiD determines that any of the information appearing in the Certificate is inaccurate or misleading;
- ZealiD QeID Service's right to issue Certificates is revoked or terminated;
- ZealiD obtains a report of a possible compromise of the Private Key of the CA used for issuing the Certificate;
- revocation is required by the CPS;
- the technical content or format of the Certificate presents an unacceptable risk to Relying Parties;
- ZealiD is made aware that CA Certificates has been compromised;
- ZealiD receives a report if cryptographic suites used in CA Certificates have been deemed non secure.

In case the RA has withdrawn Identity Provider status, the ZealiD QeID Service has the right to revoke all the Certificates which were issued for identities provided by this Identity Provider.

4.9.2. Who can request revocation

The Subscriber can request revocation of the Subscriber's Certificates at any time.

RA may request revocation of the Subscriber's certificates or submit a report of an event related to revocation based on Subscriber's application and RA TSPS.

CA may request revocation for any of the reasons listed in the Section 4.9.1 of this CPS.

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

4.9.3. Procedure for revocation request

The Subscriber can request revocation in the following way:

- By deleting profile by using ZealiD App via the settings interface; and confirming by using a biometric authentication;
- By filling out a Revocation Form on the ZealiD website;
- By sending an email to support@zealid.com;
- By deleting profile by using My ZealiD Portal (requires log in with ZealiD App);
- By calling the support desk during working hours Mo-Fri 0800-1800.

If a Subscriber requests revocation via methods other than the application or the User Portal, the identity is verified by the ZealiD support agent. This is done by asking the Subscriber to submit the following information: first name, last name, email, date of birth, mobile phone number, address and reason for revocation. The support agent verifies the Subscriber by using the identification data in the Subscriber's application. After the Subscriber's identity and legality is verified, the agent requests a Revocation Officer to revoke the Certificate. The Subscriber is notified about the Certificate revocation via an email and a text message to a phone number provided during the time of registration. The Subscriber also has a possibility to verify from the ZealiD System that the Certificate has been revoked.

The RA can request revocation of Subscriber Certificate or submit a report of events related to revocation in the following ways:

- Sending an email to the contact person they have listed in the agreement.

Information received via an email is verified by callback to the phone number ZealiD has listed as a contact to verify the validity of the email.

The Supervisory Body can request revocation or submit a report of events related to revocation in the following way:

- Sending in an official letterhead letter.

The letterhead received from a Supervisory Body is verified by a callback to the Supervisory Body in order to ensure that the letterhead letter is official.

If a request or a report of events for revocation of a CA Certificate is received, ZealiD Management Board is processing it.

The revocation of the Certificate is recorded in the certificate database of ZealiD QeID Service, which has it's time stamping synchronized with UTC at least once per 24 hours using NTP Server Pool Stratum 1.

Revoked Certificate can not be reinstated.

4.9.4. Revocation request grace period

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

4.9.5. Time within which CA must process the revocation request

ZealiD QeID Service immediately processes a request for revocation or a report of events of Subscriber's Certificate, after the submission.

Upon receiving a revocation request or a report of events for any of the CA Certificates from the Supervisory Body, ZealiD Management Board assembls within 4 hours to process the revocation request or the report.

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

minutes. The maximum delay between receipt of a certificate revocation request and the actual change of the certificate status information being available to all relying parties shall be at most 24 hours.

4.9.6. Revocation checking requirement for Relying parties

Please see Terms & Conditions ZealiD QeID Service.

4.9.7. CRL issuance frequency (if applicable)

The CRLs are not issued regularly. OCSP is used instead.

A final CRL is issued upon termination of the service and transferred to the Supervisory Body or a Custodian.

4.9.8. Maximum latency for CRLs (if applicable)

No stipulation.

4.9.9. On-line revocation/status checking availability

The service is free of charge and publically available 24/7 at https://ocsp.zealid.com

4.9.10. On-line revocation checking requirements

The mechanisms available to the Relying Party for checking the status of the Certificate on which it wishes to rely are established in the Terms and Conditions ZealiD QeID.

4.9.11. Other forms of revocation advertisements available

Revocation status information of expired Certificates can be requested at support@zealid.com.

4.9.12. Special requirements re key compromise

No stipulation.

4.9.13. Circumstances for suspension

No stipulation.

4.9.14. Who can request suspension

No stipulation.

4.9.15. Procedure for suspension request

No stipulation.

4.9.16. Limits on suspension period

No stipulation.

4.10. Certificate status services

ZealiD QeID Service offers OCSP certificate status request services accessible over HTTPS.

The URL of the OCSP service is included in the certificate.

OCSP Responses are signed with the same size signature as the underlying private key.

4.10.1. Operational characteristics

ZealiD OCSP is synchronized with an NTP Pool Server Stratum 1 for UTC time every 24 hours.

OCSP responses are signed with OCSP keys and a sha384 hashing algorithm is used for status responses of Issuing CA certificate, and sha256 hashing algorithm is used to sign status responses of Subscriber signing or authentication certificates.

4.10.2. Service availability

ZealiD QeID Service 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.

Last OCSP response shall be computed prior to expiring of the CA's certificate.

4.10.3. Optional features

No stipulation.

4.11. End of subscription

The validity period of the Certificate is described in appropriate ZealiD Certificate Profile documents.

4.12. Key escrow and recovery

The ZealiD QeID Service does not offer the Subscriber key escrow and recovery services.

4.13. Key escrow and recovery policy and practices

No stipulation.

4.14. Session key encapsulation and recovery policy and practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

ZealiD has implemented a Policy Information Security with a supporting Policy ICT 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.

The ZealiD Management Board defines and approves policies and practices related to information security, for its trust services. Changes that impact on the level of security provided shall be implemented only after approval of the ZealiD Management Board.

ZealiD performs risk assessment regularly in order to evaluate business risks, IT risks and risks related to the Registration Authority as well as Certification 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 retains overall responsibility for conformance with the procedures prescribed in internal information security policies, even when the TSP's functionality is undertaken by outsourcing partners.

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.

ZealiD QeID 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 QeID Services are managed in Sweden.

ZealiD sites are physically protected with different layers, and implement suitable physical security measures. Data centres used by ZealiD are ISO 27000 (or equivalent) certified.

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.

5.1.2. Physical access

ZealiD contracted data centre for the ZealiD QeID 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 QeID Services only as authorised resources notified on an approved list.

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

Common areas are outside the ZealiD QeID Service racks.

5.1.3. 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.

5.1.4. Water exposures

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

5.1.5. 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.

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. Data media containing sensitive information is stored only in a special fireproof safe designed for storing data media.

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 QeID 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.

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.

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.

5.2.1. Trusted roles

ZealiD has established and documented necessary Trusted roles to run the QeID 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.
Revocation Officers: Personnel accessing the QeID Service (CA) and ensuring revocation of certificates.
Compliance Manager: Manages Compliance, Information Security including Risk Management and some aspects of Quality.

ZealiD has several System Administrators with internal regulation.

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 QeID 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.

5.2.2. 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.

The assignment is made person by person by the Management Board.

The following activities require three System Operators, the Security Officer and an external trusted party:

- HSM initialization and generation of Master Backup Keys

The following activities require a minimum of two (out of three) System Operators, the Security Officer and an external trusted party:

- Generation of certification keys for Root CA

The following activities require a minimum of two System Operators and the Security Officer:

- Generation of certification keys for Issuing CA

The following activities require a minimum of Security Officer and Backup/Restore Approval User:

- Backup of the certification keys for Root and Issuing CAs

The following activities requires a Security Officer, Backup/Restore Approval User:

- Restoration of the certification keys for Root and Issuing CAs

The following activities require two System Administrators:

- User Management
- User Permission Management
- System Configuration and installation

ZealiD does not have any deputies who are authorized to assume duties of a Trusted Role that has been assigned to a specific employee.

5.2.3. 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.

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.

5.3. Personnel controls

5.3.1. 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:

- Not participate in any activity regarding the issuing of certificates in his/her name or legal representative of him/her;
- 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.

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 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. The role duties and access is not granted and suspended until the necessary checks are completed.

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.

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.

All personnel receive ongoing training on all ISMS topics. Line manager determines the need for an Individual Development Plan and associated training. Role specific training is provided.

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

5.3.8. 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.

5.4. Audit logging procedures

5.4.1. Types of events recorded

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
General RA events	• Result • Agent Name (not applicable during fully automated decision) • Identification timestamp • Transaction Number • ID number • Fraud reason • Facemap generated after liveness check • Identification changes (whether data was edited by the agent in hybrid verification) • Review of changes (whether the data change was reviewed by another agent in dual review cases)

- 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
- Pictures of person

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

Trust Service certificates
- All events relating to the life cycle of keys and Certificates managed by ZealiD, including CA keys and Certificates and Subscriber key pairs;
- Subscriber signing events (including associate certificate);
- Signed Subscriber Agreement with Terms and Conditions;
- Subscriber authentication during Signature Activation Protocol;
- Signature Activation Data management by the Signature Activation Module;
- 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.

5.4.2. Frequency of processing log

Processing 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 14 years.

When a certificate ceases to be valid, associated logs and Terms and Conditions and Subscriber agreements are kept for 12 years.

In case of ZealiD termination audit logs are retained and accessible until abovementioned term for retention in accordance with section 5.8.2. of this ZealiD QeID CPS.

5.4.4. Protection of audit log

Audit log is stored encrypted in a dedicated storage within ZealiD infrastructure. Logs are signed and the signature is validated when auditing logs. The access to the audit log is given to a person who does not have administrative or operational access to ZealiD QeID 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 into a dedicated backup server.

On a quarterly basis a physical backup is taken by recording that logs into an encrypted USB drive. The backup is verified for restoration immediately after it has been taken.

Every 6 months an older backup is verified for restoration at the time when a physical backup is being taken.

The hashes of the backups are recorded during the time of backup in order to compare whether the full log has been backed up.

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.

Audit collection system is running on a dedicated virtual machine on ZealiD Backend infrastructure. The startup and shutdown of the logging virtual machine or a logging function causes an alarm to System Auditor. ZealiD QeID Service does not have a possibility to switch off a logging function.

Logging function of the ZealiD QeID System cannot be switched off.

5.4.7. Notification to event-causing subject

No Stipulation

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

5.5.1. Types of records archived

Physical or digital archive records about certificate applications, signed Subscriber agreements, registration information (including evidence of Subscriber identity verification), certificates with retention information, certificate status information with retention period and requests or applications for revocation are retained.

5.5.2. Retention period for archive

Physical or digital archive records about certificate applications, signed Subscriber agreements, registration information (including evidence of Subscriber identity verification), certificates with retention information, certificate status information with retention period and requests or

applications for revocation are retained for at least 12 years after validity of relevant certificate.

OCSP Responder has a 15 year archive cutoff in order to provide status information past the expiration of the certificate.

In case of termination ZealiD archive records are retained and accessible until abovementioned term for retention in accordance with section 5.8 of this ZealiD QeID CPS.

5.5.3. Protection of archive

The archive is stored encrypted in a dedicated storage within ZealiD infrastructure. Encryption of the log generates an HMAC verification hash to ensure integrity.

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

5.5.4. Archive backup procedures

The archive is backed up to an encrypted offline media and stored in a secure safe.

5.5.5. Requirements for time-stamping of records

Database entries contain accurate time and date information. The time-stamps are not cryptographically based.

5.5.6. Archive collection system (internal or external)

ZealiD uses an internal archive collection system.

5.5.7. Procedures to obtain and verify archive information

Only authorised personnel in Trusted Roles are allowed access to the archive.

Should the records concerning the operation of services be required for the purposes of providing evidence of the correct operation of the services and for the purpose of legal proceedings, they are made available to legal authorities and/or persons whose right of access to them arises from the law.

The integrity of the information is verified during the recovery tests. The archive systems with built-in integrity controls are in use.

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 QeID 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, 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 QeID service.

Incident response actions shall uphold the original security requirements, and in particular, not break dual control, if originally required.

Incident response procedures are documented. Where it is determined that the incident requires remediation, a mitigation plan is documented and followed up regularly.

In case of private CA key compromise ZealiD will additionally:

- Indicate that ZealiD QeID Certificates and validity information issued using this CA may no longer be valid via information on the website and a press release;
- Inform the Supervisory Body regarding a certificate revocation so that the National Trusted List can also be updated accordingly;
- Inform all affected Subscribers and Relying parties.

In case of algorithm or associated parameters become insufficient for its remaining intended usage ZealiD will additionally:

- Schedule a revocation of any affected ZealiD QeID Certificates;
- Inform all affected Subscribers and Relying parties.

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 QeID 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.

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

ZealiD key compromise is handled according to internal Incident Management documentation and considered to be a disaster.

5.7.4. Business continuity capabilities after a disaster

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

5.8. CA or RA termination

5.8.1. RA termination

ZealiD is aware that its RA Service has a Termination Plan which describes the process of a service termination. Stakeholders affected by any termination will be informed according to it.

Should the RA Service be terminated, ZealiD can opt to introduce an alternative certified RA Service. Any additional RA, regardless of termination, may be introduced only following an updated CPS, communications to subscribers and relying parties, as well as information to CAB and necessary approval from SB.

5.8.2. CA termination

The ZealiD QeID 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.

In any case of termination, ZealiD concludes a detailed action plan with a timeframe for the execution of termination actions and considering the requirements and internal routines of ZealiD. 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 QeID Certificates for 12 years and
- audit logs are retained and accessible for 12 years.

Before ZealiD terminates a CA 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 destroys the CA private keys, including backup copies or keys withdrawn from use in such a manner that the private keys cannot be retrieved;
- ZealiD resets or destroys any hardware appliances related to this service depending on the security regulations;
- ZealiD terminates authorisation of all subcontractors to act on behalf of ZealiD in carrying out any functions relating to the process of issuing ZealiD QeID Certificates for this service.

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

In case of scheduled termination ZealiD maintains the logs and documentation related to the provision of the Trust Service and information needed to verify the Certificates.

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.

The requirements are applicable also in case of RA termination. ZealiD takes over the documentation and information related to the supply of the Trust Service and provides evidence of the operation for a time period defined in relevant service-based Policy and/or Practice Statement.

6. TECHNICAL SECURITY CONTROLS

6.1. Key pair generation and installation

ZealiD uses cryptographic keys for its Trust Services and follows industry best practices for key lifecycle management, key length and algorithms.

6.1.1. Key pair generation

6.1.1.1. ZealiD QeID Infrastructure Keys

The signing keys of ZealiD QeID Service are created in accordance with the internal regulation of ZealiD: Protocol CA Key Ceremony. For the key ceremony of ZealiD QeID Service key pair generation for all root CA, issuing CA, OCSP responders, 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. The commission has to include an external auditor independent of ZealiD, who confirms the correctness of the procedure and report of the key ceremony. The external auditor is not needed for Issuing CA generation. Procedure for ZealiD QeID Service key pair generation is carried out according to the detailed instructions created for the specific procedure. The creation of ZealiD QeID 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 QeID 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 QeID 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, including the external auditor. 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 QeID Service certificate, ZealiD generates a new QeID 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 QeID Service certificate always contains the number of the year in which it was created. The new QeID Service certificate is generated and distributed according to this practice statement.

6.1.1.2. ZealiD Subscriber Key pair

Subscriber key pair is generated in the HSM. The private key is encrypted with MBK and stored in the encrypted database of SAM Appliance and the public key is stored in an encrypted storage of a Signature Activation Module.

6.1.2. Private key delivery to Subscriber

The private key is not delivered to the Subscriber.

ZealiD App detects whether it is the first time the device is being used to register and asks the Subscriber to confirm the registration process. Upon approval from the subscriber the ZealiD App sends a registration request to ZealiD QeID backend. The backend generates two OTP messages that are sent via two different channels input by the user earlier in the registration process - mobile phone number and email address. If the Subscriber correctly inputs the OTP messages into the ZealiD App, the application then generates authorization key pairs, where the key pair is stored in the secure element of the device and protected by device-native biometrics. Afterwards ZealiD App creates a CSR against the key pair which is sent to the ZealiD backend to receive

mobile device authorisation certificate. Once certified the certificate is passed both to Signature Activation Module and the Subscriber's mobile device where it is linked with the key pair (the authorisation certificate will be used later in the process to verify the SAD once the authorisation request is authorised by the ZealiD App).

ZealiD Backend then requests a central high-trust signing and authentication key pairs to be generated within the HSM residing in QeID infrastructure which is a QSCD and then certified. During this process Subscriber's mobile device hardware identifier is recorded as an approved device to authorise the use of this authentication or signing key and certificate.

6.1.3. Public key delivery to certificate issuer

Subscriber's public key is stored in the encrypted storage of the Signature Activation Module.

6.1.4. CA public key delivery to relying parties

ZealiD rootCA, issuingCA and OCSP public keys are distributed in the form of X.509 certificates issued by ZealiD CA. The primary distribution is via the ZealiD Repository, https://www.zealid.com/repository.

6.1.5. Key sizes

Subscriber Signing Keys are 4096 RSA keys
Subscriber Authentication Keys are 4096 RSA keys
issuingCA keys are 4096 RSA keys
rootCA keys are 4096 RSA keys
OCSP key are 4096 RSA keys

6.1.6. Public key parameters generation and quality checking

Before issuing a Certificate, the key is checked for duplicates and some basic analytic checks are applied (e.g. e > 1 for RSA). More thorough checks are run over the database of issued Certificates regularly. Secure random number generators are further used to ensure the quality of public keys.

6.1.7. Key usage purposes (as per X.509 v3 key usage field)

Subscriber Authentication Key usage:

- digitalSignature

Subscriber Signing Key usage:

- nonRepudiation

Root CA Key usage:

- keyCertSign
- keyCrlSign

Issuing CA Key usage:

- keyCertSign
- KeyCrlSign

OCSP Key usage:

- digitalSignature
- nonRepudiation
- ocspSigning

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic module standards and controls

The HSMs used by ZealiD QeID 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 QeID Service verifies that HSM is not tampered physically after its installation, by checking the security seal.

ZealiD QeID Service verifies that HSM is functioning correctly during usage and retains its certification status.

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

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

The access to ZealiD QeID 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 in accordance with clause 5.2.2 of this CPS.

6.2.3. Private key escrow

No Stipulation.

6.2.4. Private key backup

The private keys of the CA 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.
The Backup/Restore Approval User is a temporary role during the backup 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.

Subscriber private keys are backed up in a dedicated backup database with the SAM Appliance.

6.2.5. 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.

6.2.6. Private key archival

ZealiD QeID Service will not archive Trust Service private keys after it has expired. All copies of ZealiD QeID Service Trust Service private keys are destroyed after their expiry or revocation so that further use or derivation thereof is impossible.

6.2.7. Private key transfer into or from a cryptographic module

All ZealiD QeID Trust Service keys must be generated by and in the cryptographic module. ZealiD QeID 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.

6.2.8. Private key storage on cryptographic module

ZealiD QeID Infrastructure Private Keys (rootCA, issuingCA, OCSP and MBK) held in the HSM.

6.2.9. Method of activating private key

6.2.9.1. Method of activating service private key

Each of the ZealiD QeID Control Keys for HSM is protected with a smart card with an individual PIN code held by System Administrators, System Operators and the Security Officer.

6.2.9.2. Method of activating subscriber private key

The Subscriber uses mobile device-native biometrics to approve an authorisation request originating from ZealiD QeID Service. If done correctly this releases the private authorisation key held in the secure element of the mobile device to digitally sign the Authorisation Response message (called SAD - Signature Activation Data). The message contains the same elements as in the request message above plus (a) Mobile Device hardware identifier and (b) the authorisation signature on the response.

The SAD is sent back to the ZealiD Backend for verification of the following items:

A. Data hash value is the same;
B. The UserID is the same;
C. The centrally held certificate alia is the same;
D. The salt information, if set, is the same;
E. The mobile device hardware identifier is for one of the subscriber's registered devices;
F. The signature on the response can be verified by the device's authorisation certificate which was set-up when the device was registered

If all checks are successful the signing key becomes available for signing.

6.2.10. Method of deactivating private key

ZealiD Service private keys are deactivated when an attempt is made to open the security module used for storage of the keys, when the configuration is changed, the power supply is disconnected or transferred or in other events endangering the security.

Deactivation of any component of the Subscriber's private key or change of security setting on the device will deactivate the private key held on a mobile device and the Subscriber will not be able to use it for signatures.

Due to incorrect authentication attempts the ZealiD Backend will automatically request revocation from a Revocation Officer:

a. A Subscriber makes 3 incorrect authentication attempts - signing is disabled for 20 minutes
b. A Subscriber makes 6 incorrect authentication attempts - signing is disabled for 12 hours
c. A Subscriber makes 9 incorrect authentication attempts - subscriber certificate is revoked.

6.2.11. Method of destroying private key

Method of destroying ZealiD QeID Service Trust Service private keys and internal control mechanisms depend on the options available to specific secure cryptographic modules.

6.2.12. Cryptographic Module Rating

See section 6.1.2 above.

6.3. Other aspects of key pair management

6.3.1. Public key archival

All certificates issued (including all expired or revoked certificates) are retained and archived as part of ZealiD QeID Service routine backup procedures. The retention period is 14 years.

6.3.2. Certificate operational periods and key pair usage periods

The operational period of a certificate ends upon revocation or expiration. The operational period for key pairs is the same as the operational period for the certificates, except that the public keys may continue to be used for signature verification. Private keys are not used beyond their life cycle.

In addition, ZealiD QeID Service stops issuing new certificates for Subscribers with an old Issuing CA when a new Issuing CA has been generated such that no Subscriber certificate expires after the expiration of the Trust Service certificate.

If an algorithm or the appropriate key length offers no sufficient security during the validity period of the certificate, the concerned certificate will be revoked and a new certificate application will be initiated. The applicability of cryptographic algorithms and parameters is constantly supervised by ZealiD's management.

The Subscribers' certificates are valid for 2 years.

6.4. Activation data

6.4.1. Activation data generation and installation

ZealiD QeID Service Trust Service private key activation data generation and installation is performed according to the user manual of HSM.

The initial activation data is chosen by Subscriber. PIN codes are not stored by ZealiD QeID Service nor by the ZealiD App.

6.4.2. Activation data protection

HSM is kept in a secure environment and access to it is given only to authorized personnel in Trusted Roles. At least two people in Trusted Roles need to be present physically to conduct any HSM operation.

The Subscriber shall use mobile device-native biometrics to secure the device and to authorise the use of certificates. If the device is not under the control of the Subscriber, Subscriber shall apply for Certificate revocation immediately.

6.4.3. Other aspects of activation data

No stipulation.

6.5. Computer security controls

6.5.1. 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 QeID 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.

Status information service is monitored for requests concerning non-issued certificates and such events are raised as an alert.

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.

6.5.2. Computer security rating

ZealiD uses 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

Measures are implemented In the information system of ZealiD QeID 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.

6.6.3. Life cycle security controls

ZealiD QeID Service policies, assets and practices (including ZealiD QeID Service CPS) 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 QeID Service systems are regularly checked for changes that violate ZealiD QeID 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 QeID 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 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.

The Hardware Security Modules (HSMs) will be cleared according to their supplier's documentation upon retirement from service.

6.7. Network security controls

ZealiD QeID Service network is divided into zones by security requirements. Communication between the zones is restricted. Only the protocols needed for ZealiD QeID 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. Administrative network access is separated from the operational access.

Production systems are separated from non-production systems such as testing and development.

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

The SAM Appliance, which contains the CA service (the SAM and the HSM), is in a high security zone and dedicated network. ZealiD QeID 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.

ZealiD performs a vulnerability scan once a quarter on public and private IP addresses identified by ZealiD.

ZealiD QeID Service and ZealiD assets undergo penetration testing on the certification systems annually, at the set up, and after the infrastructure or application upgrades or modifications determined significant by ZealiD.

ZealiD records evidence that each vulnerability scan and penetration test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

6.8. Time-stamping

All ZealiD QeID Service CA and ZealiD Backend components are synchronized at least daily with a Network Time Protocol (NTP) service Pool Server Stratum 1 for UTC time. Time derived from the time service shall be used for establishing the time of:

- Initial validity time of a CA Certificate;
- Revocation of a CA Certificate;

- Logging;
- Archiving;
- Issuance of Subscriber end entity Certificates.

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

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate profile

Refer to ZealiD rootCA, ZealiD issuingCA and ZealiD Subscriber Certificate Profiles.

ZealiD Certificate validity:

Certificates	Validity
Subscriber Certificates	2 years
IssuingCA Certificate	15 years
RootCA Certificate	30 years
TSACA Certificate	15 years
TSU Certificates	5 years
OCSP Certificates	5 years

ZealiD Certificates are compiled in accordance with the X.509 version 3, IETF RFC 5280, ETSI EN 319 412-2, ETSI EN 319 412-5, ETSI EN 319 411-2, and ETSI TS 119 312.

Note: ZealiD does not set the ArchiveCutOff date to the CA's certificate "notBefore" time and date value. Instead, the archiveCutOff date is set to an

archiving of 15 years so that revocation status information is made available via OCSP 15 years beyond the validity period of the certificate.

7.2. CRL profile

No stipulation.

7.3. OCSP profile

Refer to ZealiD OCSP Profile.

ZealiD OCSP is configured as defined RFC 6960 [11].

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 Section 1.1 and 9.15).

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.

8.2. 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.

8.3. 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.

8.4. 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 CPS 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).

8.5. 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 fulfil requirements within a time limit set by the Supervisory Body.

ZealiD makes efforts to stay compliant and fulfil 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.

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

9.1.1. Certificate issuance or renewal fees
Subscriber is not required to pay fees for Certificate Issuance.

9.1.2. Certificate access fees
Subscriber is not required to pay fees for Certificate access.

9.1.3. Revocation or status information access fees
Neither Subscribers nor Relying Parties are required to pay fees for accessing revocation or status information.

9.1.4. Fees for other services
Relying parties pay fees according to Master Service Agreements and Service specification signed with ZealiD.

9.1.5. Refund policy
ZealiD handles refund requests from Relying Parties on a case-by-case basis.

9.2. Financial responsibility

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 CPS and the requirements of eIDAS.

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

9.2.1. Insurance coverage
ZealiD has professional services insurances required by law and published on www.zealid.com/repository.

9.2.2. Other assets
No stipulation.

9.2.3. Insurance or warranty coverage for end-entities
See clause 9.2.1. above

9.3. Confidentiality of business information

9.3.1. Scope of confidential information
All personal data is considered confidential. All information not required to be public by law, regulation or applicable standards is considered confidential.

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 statistical data about its services.

9.3.3. Responsibility to protect confidential information
ZealiD safeguards confidential information and information intended for internal use from illicit access and use by third parties.

9.4. Privacy of personal information

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. Due to the nature of the Trust Service, ZealiD has a Privacy Policy and a Data Protection Officer (DPO) appointed and registered with the Swedish Authority for Privacy Protection.

9.4.2. Personal data processed
The scope of personal data processed by ZealiD is in the terms and conditions found in ZealiD QeID CPS (this document), RA TSPS. This can be found under www.zealid.com/repsository.

9.4.3. Information not deemed private
No stipulation.

9.4.4. Responsibility to protect personal data
ZealiD ensures protection of personal information by implementing security controls as described in chapter 5 of this CPS.

9.4.5. Notice and consent to use 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 Relying Parties 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 CPS.

9.6. Representations and warranties

9.6.1. CA representations and warranties

ZealiD is a TSP participant in a trust relationship between TSP, Subscribers, Customers and Relying Parties. This CPS 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 CPS and according to the policies under which this CPS is created.
- be responsible for the effective compliance with the procedures set forth in this CPS.
- 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 CPS.
- honour its part in Subscriber Terms and Conditions and secure Subscriber availability and access to the services set out in this CPS.
- retain overall responsibility for conformance with the procedures prescribed in internal information security policies, even when the TSP's functionality is undertaken by outsourcing partners.
- protect the integrity and confidentiality of personal data and information acquired as part of service provisioning and not subject to publication.
- maintain the integrity of Trust Service Access to Relying parties (e.g. Tokens) and offer effective services to check the validity of certificates.
- inform the Conformity Assessment Body and National Supervisory Body of any changes to a public key used for the provision Trust Services.
- 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 of security or loss of integrity without undue delay.
- preserve all the documentation, records and logs related to Trust Services according to the sections 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 CPS.
- 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 CPS, in specific contractually adhere to requirements set forth in sections:

- 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 QeID 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.

9.6.2. RA representations and warranties

Where ZealiD TRA service acts as an RA, ZealiD Service shall specifically:

- Perform its services according to the ZealiD TRA TSPS;
- Meet the level of assurance equivalent to physical presence in remote identification as set forth in German national state-of-the-art legislation conformant to eIDAS.

9.6.3. Subscriber representations and warranties

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 CPS;
- Note that intentionally presented false, incorrect or incomplete information will lead to denial of application and may lead to a police report;

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

  The Subscriber shall use his/her private key and certificates in accordance with this CPS and service Terms and Conditions.

9.6.4. Relying party representations and warranties

A Relying Party shall:

- Review and observe the documentation, risks and liabilities related to the acceptance of the certificates. The risks and liabilities have been set out in this CPS, 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.

9.6.5. Representations and warranties of other participants

No stipulation.

9.7. Disclaimers of warranties

ZealiD:

- is liable for the delivery of all its obligations specified in section 9.6.1 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 CPS by Force Majeure;
- Damages resulting from Subscriber private keys not being kept secret;
- Any errors in checking certificates on the part of Relying parties;

- 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.

9.8. Limitations of liability

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

9.9. Indemnities

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

9.10. Term and termination

9.10.1. Term

No stipulation.

9.10.2. Termination

This CPS 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

ZealiD communicates the status of this CPS on its public repository.

The communication specifies which provisions survive termination. In case of such termination, and to meet its obligations, ZealiD archives and logs personal and confidential information, as well as the public information present on the repository.

Subscriber contracts are in effect until the certificate is revoked or expired, even if this CPS terminates. Termination of this CPS cannot be done before termination actions described in section 5.8 of this CPS.

9.11. Individual notices and communications with participants

ZealiD uses its website www.zealid.com for all notifications and communications to subscribers and relying parties. In addition, smartphone applications (ZealiD app or app SDK) may be used for notifications and communications.

9.12. Amendments

9.12.1. Procedure for amendment
See 1.5.4 of this CPS.

9.12.2. Notification mechanism and period
See 2.2.1 of this CPS.

9.12.3. Circumstances under which OID must be changed
No stipulation.

9.13. Dispute resolution provisions

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.

The Subscriber or other party can submit their claim or complaint on the following email: legal@zealid.com.

9.14. Governing law

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

9.15. Compliance with applicable law

ZealiD ensures compliance with the legal requirements to meet all applicable statutory requirements for protecting records from loss, destruction and falsification, and the requirements of the following:

- 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;

Requirements for Trust Service Providers:

- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates Part 2: Policy requirements for certification authorities issuing qualified certificates
- CEN EN 419 241-1 Trustworthy Systems Supporting Server Signing (CEN)

Where physical ID documents are used for the applicant identification, the TRA Service fulfills 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).

As well as requirements:

- ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates Part 2: Policy requirements for certification authorities issuing qualified certificates

Where ID documents containing electronic chip are used for the applicant identification, the TRA Service fulfills the requirements:

- ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects;

- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates Part 2: Policy requirements for certification authorities issuing qualified certificates.

9.16. Miscellaneous provisions

9.16.1. Entire contract

ZealiD mandates each RA by way of contractual obligation to comply with this ZealiD QeID CPS. ZealiD also requires each party using its services to abide by its terms and conditions and in the case of Customers and Subscribers to sign a contract that outlines all terms of the service.

9.16.2. Assignment

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

9.16.3. Severability

ZealiD may claim indemnification and legal fees from a party for damages, losses, and expenses related to that party's conduct. ZealiD's failure to enforce a provision of this CPS does not waive ZealiD's right to enforce the same provision later or right to enforce any other provision of this CPS. To be effective, waivers must be in writing and signed by ZealiD.

9.16.4. Enforcement

ZealiD may claim indemnification and legal fees from a party for damages, losses, and expenses related to that party's conduct. ZealiD's failure to enforce a provision of this CPS does not waive ZealiD's right to enforce the same provision later or right to enforce any other provision of this CPS. To be effective, waivers must be in writing and signed by ZealiD.

9.16.5. Force Majeure

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

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

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

Non-fulfilment of the obligations arising from CPS 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 CPS and/or relevant service-related Policies and/or Practice Statements caused by Force Majeure.