1. Subscriber Agreement

This digital certificate Subscriber Agreement (“Agreement”) is between ZealiD AB, a Swedish Qualified Trust Service Provider, and you, the individual applying for and subscribing to a Certificate (“You”). By signing you enter into this agreement and accept the Terms & Conditions ZealiD QeID below under which you may apply for and subscribe to certificates and signatures.

You are asked to sign this agreement, by pressing the Sign button, to acknowledge that you have read this agreement, that you understand it, and that you agree to it. If you do not accept this agreement, do not continue. If you have any questions regarding this agreement please email ZealiD at support@zealid.com

2. Definitions and Acronyms

Authentication	Identification of a person by checking his/her alleged identity.
CA	Certificate Authority
Certificate	Public Key, together with additional information, laid down in the Certificate Profile, rendered unforgettable via encipherment using the Private Key of the Certificate Authority which issued it
Certificate Authority (CA)	A part of ZealiD AB’s (hereinafter “ZealiD”) structure responsible for issuing and verifying electronic Certificates and Certificate Revocation Lists with its electronic signature.
Coordinated Universal Time (UTC)	The time scale based on the second as defined in ITU-R Recommendation TF.460-6 (02/2002).
CP	See ZealiD QeID Service CPS for Certificate Policy references.
CPS	ZealiD QeID Service Certification Practice Statement.
Customer Support	Customer Support provides user support for solving problems related to ZealiD App usage.
Customer Support @ ZealiD TRA Service	Customer support is accessible via phone, email and app interaction. Customer Support accepts requests regarding ZealiD QeID Service Certificates from the Subscribers.
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.
ZealiD	A product brand name (consumer facing) of ZealiD AB, a Swedish limited liability company, registration number 556972-4288, a provider of the certification service.
ZealiD TRA Services	A part of ZealiD that is providing electronic authentication means and who is responsible for creating electronic identities which are used for issuing ZealiD QeID Service Certificates.

ZealiD QeID	ZealiD eID which contains one pair of Certificates consisting of the Authentication Certificate and the Qualified Electronic Signature Certificate and their corresponding Private Keys.
ZealiD QeID Service CPS	ZealiD's Trust Services Practice Statement.
ZealiD App	ZealiD App is an iOS/Android App based solution which combines registration remotely (ZealiD TRA Service) with providing a Subscriber with means for Electronic Authentication and Electronic Signature (ZealiD QeID Service).
ZealiD TRA Service	ZealiD TRA Service is an ZealiD function that based on manual and machine process manages all applications for ZealiD Qualified Certificates. ZealiD TRA Service also accepts applications for revocation of the Certificates.
Network Time Protocol (NTP)	Protocol to synchronize system clocks among a set of distributed time servers and clients as defined in RFC 5905.
OCSP	Online Certificate Status Protocol
OID	An identifier used to uniquely name an object.
PIN Code	Activation code for a Private Key.
Private Key	The key of a key pair that is assumed to be kept in secret by the holder 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. In the ZealiD QeID Service, the value of Private Key itself is never generated and the Private Key exists only in the form of its components.
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 Electronic Signature	Qualified Electronic Signature according to eIDAS Regulation.
Qualified Electronic Signature Certificate	Qualified Electronic Signature Certificate according to eIDAS Regulation.
Qualified Electronic Signature Creation Device	A Secure Signature Creation Device that meets the requirements laid down in eIDAS Regulation.
Relying Party	A third party, which uses services provided by the ZealiD System to enroll/register, authenticate and to allow Subscribers to electronically sign documents or transactions.
Relying Party	Relying Party Entity that relies on the information contained within a Certificate.
SLA	Service Level Agreement
Subscriber	A natural person to whom the ZealiD QeID Service Certificates are issued.
Terms and Conditions	Present document that describes the obligations and responsibilities of the Subscriber while using the Certificates.
Terms and Conditions TSA Service	ZealiD TSA Service Terms and Conditions for Subscribers
Time Stamp Authority (TSA)	The authority that issues Time Stamp Token.
Time Stamping Token (TST)	The data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed

	before that time.
TSAPS	ZealiD Time Stamping Authority Practice Statement.

3. General Terms

3.1. These Terms and Conditions describe the main policies and practices followed by ZealiD and provided in the ZealiD QeID CP and CPS, and TSAPS, as well as Terms and Conditions TSA Service.

3.2. For the purpose of these Terms & Conditions, ZealiD uses the term “Qualified” for certificates, signatures and time stamps that meet the corresponding technical requirements of eIDAS and ETSI standards.

3.3. The Terms and Conditions govern Subscribers' use of the Certificates and constitute a legally binding contract between Subscriber and ZealiD; for the TSA use - Terms and Conditions TSA Service are an integral part of the binding contract between Subscriber and ZealiD.

3.4. The Subscriber has to be familiar with and accept the Terms and Conditions.

3.5. ZealiD has the right to amend the Terms and Conditions at any time should ZealiD have a justified need for such amendments. Information on the amendments will be published on the website https://www.zealid.com/repository.

3.6. The Subscriber can apply for ZealiD QeID only personally, except for minors (under 18 who are not accepted). The ZealiD QeID cannot be issued to a representative.

3.7. ZealiD will retain a copy of all Terms and Conditions versions and Subscriber Agreements for twelve (12) years after the underlying certificate ceases to be valid. These will be published on the website https://www.zealid.com/repository.

4. Certificate Acceptance

4.1. After ZealiD has issued the Certificates, the Subscriber verifies correctness of the data in the Certificates. If the Subscriber has verified that the data in the Certificates is correct, the Subscriber confirms correctness of the information. Corresponding confirmation is deemed Certificate acceptance.

4.2. Subscriber data in the Certificates includes a unique personal identifier such as personal code, social security number, number of ID document, etc. For example, Swedish personal number (“personnummer”), Lithuanian personal code (“asmens kodas”), Duthch ID document number (“documentnummer”).

5. Certificate Type, Validation Procedures and Usage

	Usage	**Certification Policy Applied and Published**	**OID**
ZealiD QeID Certificates	Qualified Electronic Signature Certificate is intended for: creating Qualified Electronic Signatures compliant with eIDAS.	ZealiD AB - ZealiD QeID CPS - https://www.zealid.com/repository	See CPS

5.1. The use of the Subscriber´s Certificates is prohibited for any of the following purposes:

5.1.1. unlawful activity (including cyber attacks and attempt to infringe the Certificates of ZealiD QeID Services);
5.1.2. issuance of new Certificates and information regarding Certificate validity;
5.1.3. enabling other parties to use the Subscriber's Private Key;
5.1.4. enabling the Certificate issued for electronic signing to be used in an automated way;
5.1.5. using the Certificate issued for electronic signing for signing documents which can bring about unwanted consequences (including signing such documents for testing purposes).

5.2. The Subscriber Authentication Certificate can not be used to create Qualified Electronic Signatures compliant with eIDAS.
5.3. ZealiD Certificate subject DN is limited to 500 characters.

6. Reliance Limits

6.1. Certificates become valid as of the date specified in the Certificate.
6.2. The validity of the Certificate expires on the date of expiry indicated in the Certificate or if the Certificate is revoked.
6.3. ZealiD ensures that its clock is synchronized with UTC within the declared accuracy of 1 second using the NTP.
6.4. ZealiD monitors its clock synchronization and ensures that, if the time that would be indicated in a TST drifts or jumps out of synchronization with UTC, this will be detected. In the case of a TST drift or jump out of synchronization with UTC, ZealiD stops issuing time-stamps until the issue is resolved.

6.5. Both local and remote NTP servers with GPS time sources are used for NTP reference. Monitoring of clock synchronization is done by comparing the time sources.

6.6. Audit logs are retained on-site for no less than 12 years after the expiry date of the Certificate. Physical or digital archive records regarding Certificate applications, registration information and requests or applications for revocation are retained for at least 12 years after the expiry of the relevant Certificate.

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

7. Subscriber's Rights and Obligations

7.1. The Subscriber has the right to submit an application via the ZealiD App (RA Service) for issuing the Certificate for ZealiD QeID

7.2. The Subscriber is obligated to:

7.2.1. accept these Terms and Conditions;

7.2.2. adhere to the requirements provided by ZealiD QeID and TSA Service;

7.2.3. use the his/ her Private Keys for cryptographic functions within the secure cryptographic device;

7.2.4. use his/her Private Keys solely for creating Qualified Electronic Signatures;

7.2.5. use his/her Private Key and Certificate in accordance with the Terms and Conditions and the laws of Sweden and the European Union;

7.2.6. accept that ZealiD makes Signing Certificate available for retrieval;

7.2.7. ensure that he/she no longer uses his/her Private Key, in the case of being informed that his/her Certificate has been revoked or that the issuing CA has been compromised;

7.2.8. ensure that Subscriber´s Private Authorization Key is used under his/her control;

7.2.9. present true and correct information including all Subscriber generated information, liveness checks and photos of documentation to ZealiD QeID via the Registration Authority service;

7.2.10. notify ZealiD QeID of the correct details within a reasonable time period of not more than five (5) working days, in case of a change in his/her personal details, and during that period abstain from using the Private key;

7.2.11. immediately inform ZealiD of a possibility of unauthorized use of his/her Private Key and revoke his/her Certificates;

7.2.12. immediately revoke his/her Certificates if his/her Private Key has gone out of his/her possession;

7.2.13. following a compromise of his/her Private Key, immediately and permanently discontinue the use of this key.

8. ZealiD's Rights and Obligations

8.1. ZealiD is obligated to:

8.1.1. supply certification service in accordance with these Terms and Conditions, CPS and agreements and legislation as stated under Chapter 13;
8.1.2. ensure that ZealiD QeID is using a Qualified Signature Creation Device (QSCD) by checking its certification status;
8.1.3. keep account of the certificates issued by it and of their validity;
8.1.4. provide security with its internal security procedures;
8.1.5. provide the possibility to check the validity of certificates 24 hours a day;
8.1.6. provide the CA and private Subscriber Signing and Auhtentication keys are protected by hardware security modules (i.e. HSM) and are under the sole control of ZealiD for CA keys and the Subscriber for Signing and Authentication Keys;
8.1.7. provide the Subscriber Signing and Authentication keys used in the supply of the certification service are activated on the basis of subscriber consent;
8.1.8. ensure that the subscriber's private key is used under the subscriber's sole control;
8.1.9. ensure that digital signatures are only created by a QSCD device;
8.1.10. ensure that private key shall be used for signing only within a QSCD.

9. Certificate Status Checking Obligations of Relying Parties

9.1. A Relying Party shall assess the risks and liabilities related to acceptance of the Certificate. The risks and liabilities have been set out in the ZealiD QeID Service CPS.
9.2. A Relying Party shall verify the validity of the Certificate on the basis of certificate validation services offered by ZealiD at the time of using the Certificate or affixing a Qualified Electronic Signature.
9.3. A Relying Party shall follow the limitations stated within the Certificate and make sure that the transaction to be accepted corresponds to the CPS and CP.
9.4. ZealiD ensures availability of Certificate Status Services 24 hours a day, 7 days a week with a minimum of 99.5% availability overall per year with a scheduled downtime that does not exceed 0.3% annually. This is ensured by ZealiD setting

up high availability systems, providing network redundancy (connection) and power.

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

9.6. ZealiD offers OCSP service for checking Certificate status. Service is accessible over HTTP protocol. A Relying Party shall verify the validity of the Certificate by checking Certificate validity against OCSP. ZealiD offers OCSP with following checking availability:

9.6.1. OCSP service is free of charge and publicly accessible at https://ocsp.zealid.com.

9.6.2. The URL of the OCSP service is included in the Certificate on the Authority Information Access (AIA) field in accordance with the Certificate Profile.

9.6.3. Archive Cut Off for ZealiD OCSP is set to 15 years.

9.6.4. Validation of the certificate chain must be carried out successfully up to the ZealiD trust anchor within the EU trusted list.

9.7. Revocation status information of the expired Certificate can be requested at the email address info@zealid.com

9.8. OCSP service contains Certificate status information until the Certificate expires. Status information is available from expired Certificates for 15 years.

10. Obligations of other participants

10.1. ZealiD QeID Provider ensures that:

10.1.1. It adheres to the key generation and storage procedures under its control and described in the CPS;

10.1.2. it adheres to provisions of fees described in the CPS;

10.1.3. it transfers the correct Certificate and correct Certificate status information.

11. Limited Warranty and Disclaimer/Limitation of Liability

11.1. The Subscriber is solely responsible for the maintenance of his/her Private Authentication Key.

11.2. The Subscriber is solely and fully responsible for any consequences of Authentication and Electronic Signature using their Certificates both during and after the validity of the Certificates.

11.3. The Subscriber is solely liable for any damage caused due to failure or undue performance of his/her obligations specified in the Terms and Conditions and/or the laws of Sweden.

11.4. The Subscriber is aware that no document shall be signed with a private key where the corresponding certificate is no longer valid.

11.5. ZealiD ensures that:

11.5.1. the certification service is provided in accordance with CPS, CP, TSAPS, Terms and Conditions TSA Service and the relevant legislation of Sweden and European Union;

11.5.2. the certification keys are protected by hardware security modules (i.e. HSM) and are under the sole control of ZealiD;

11.5.3. the certification keys used to provide the certification service are activated on the basis of shared control;

11.5.4. it has compulsory insurance contracts covering all ZealiD services to ensure compensation for damages caused by ZealiD breach of obligations;

11.5.5. it informs all Subscribers before ZealiD terminates service of Certificates and maintains the documentation related to the terminated service of Certificates and information needed according to the process set out in CPS and/or TSAPS.

11.6. ZealiD is not liable for:

11.6.1. inadequate checks of the Certificates or for the wrong decisions of a Relying Party or any consequences due to error or omission in Certificate validation checks;

11.6.2. the non-performance of its obligations if such non-performance is due to faults or security problems of the supervisory body, the data protection supervision authority, Trusted List or any other public authority;

11.6.3. the failure to perform if such failure is occasioned by force majeure.

12. Termination of ZealiD QeID

To ensure sustainability and durability of the ZealiD QeID, and confidence of Subscribers and Relying parties on the continuity, ZealiD maintains an up-to-date termination plan, in case of a scheduled or unscheduled termination as referred to in Art.24.2(i) of the eIDAS regulation. ZealiDs objective is to secure that ZealiD QeID qualified signatures created before the termination will not lose trustworthiness or validity because of that termination and it should still be possible to validate them afterwards.

12.1. Preservation of Subscriber's Personal Data

In the case of termination, ZealiD will ensure that Subscriber's Personal Data, provided for the issuance of certificates and signatures, is securely preserved with a Custodian or Supervisory body for at least 12 years.

12.2. Preservation of Operational Data

In the case of termination, ZealiD will ensure that operational data such as archives, event logs etc are securely preserved with a Custodian or Supervisory body for at least 12 years.

12.3. Conditions on continuation of use of ZealiD QeID

ZealiD QeID service will in case of termination give three (3) months notice period after which issuance of ZealiD QeID certificates and signatures will be discontinued.

12.4. Status information

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

Final CRL will be generated before ZealiD QeID Service termination and transfer via physical media to the Supervisory Body or a Custodian. Revocation status information shall be retained for at least 12 years.

13. Applicable Agreements, CPS, CP

13.1. Relevant agreements, policies and practice statements related to Terms and Conditions for use of Certificates are:

13.1.1. ZealiD Certification Practice Statement, published at https://www.zealid.com/repository/. This also contains references to the legal acts that form the Certificate Policy.
13.1.2. ZealiD Trust Services Practice Statement, published at https://www.zealid.com/repository/.
13.1.3. ZealiD Time Stamping Authority Practice Statement, published at https://www.zealid.com/repository/.
13.1.4. Certificate and OCSP Profile for ZealiD QeID, published at https://www.zealid.com/repository/.
13.1.5. Terms and Conditions TSA Service, published at https://www.zealid.com/repository/.
13.1.6. Principles of Processing Personal Data, published at https://www.zealid.com/repository/.

13.2. Current versions of all applicable documents are publicly available in the ZealiD repository https://www.zealid.com/repository/.

14. Privacy Policy and Confidentiality

14.1. ZealiD follows the Principles of Processing Personal Data, provided in the ZealiD repository https://www.zealid.com/repository/, when processing personal information and logging information.

14.2. The Subscriber is aware and agrees to the fact that during the use of Certificate in Enrollment/registration, Authentication, the person conducting the identification is sent the Certificate that has been entered in the Subscriber's ZealiD ID and contains the Subscriber's name and personal identification code.

14.3. The Subscriber is aware and agrees to the fact that during the use of Certificate for Qualified Electronic Signature, the Certificate that has been entered in the Subscriber's ZealiD QeID and contains the Subscriber's name and serial number (which contains one of the following: personal number, document number, or tax identification number) is added to the document the Subscriber electronically signs.

14.4. All information that has become known while providing services and that is not intended for disclosure (e.g. information that had been known to ZealiD because of operating and providing Trust Services) is confidential.

14.5. The Subscriber has the right to obtain information from ZealiD about him/herself pursuant to the law. ZealiD secures confidential information and information intended for internal use from compromise and refrains from disclosing it to third parties by implementing different security controls.

14.6. The Subscriber, upon Subscriber strong authentication, has the right to request that the data ZealiD keeps from the registration be transmitted to a party designated by the Subscriber.

14.7. ZealiD has the right to disclose information about the Subscriber to a third party who pursuant to relevant laws and legal acts is entitled to receive such information.

14.8. Additionally, non-personalised statistical data about ZealiD's services is also considered public information. ZealiD may publish non-personalised statistical data about its services.

15. Contact Information

Trust Service Provider ZealiD, ZealiD AB, Registration number 556972-4288, Box 3437, 111 56 Stockholm, Sweden, Phone +46 (0)10-199 40 00, E-mail: info@zealid.com

Any complaints arising from the service or these Terms & Conditions shall be communicated to legal@zealid.com or using the online form "Report and Issue" on https://www.zealid.com.

The applications for revoking ZealiD QeID certificates are accepted 24/7 via the ZealiD App. The Customer Support may be contacted for revocation between 0800 - 1800 CET during working days at: support@zealid.com