

Application for the Issuance of a Code Signing Certificate

Please note that we can only accept forms that have been filled out electronically. If it is not practical for you to fill out the form electronically, please contact us. Guidelines and general conditions are attached on the following pages.

Certificate Holder Details

Company/Organisation (according to commercial register)

Commercial register number

Organisational Unit optional

Validity

3 Years (Standard)

2 Years

1 Year

Device (secure signature creation device)

USB Token

HSM*

* The HSM used for certificate issuance must be FIPS 140-2 Level 3 compliant and FIPS mode must be enabled. QuoVadis is also obliged to monitor and document the key generation ceremony at the HSM via remote maintenance.

Additional Details

Company Address (Street + No., Zip Code, City, Country)

Delivery address for USB Token/HSM (if different)

Billing Address (if different)

Phone/Mail Administrative Contact (for queries)

Phone/Mail Technical Contact (for queries)

Applicant

Signature Applicant

Telephone (for queries)

Position, Department

Applicant First and Last Name (block letters)

E-Mail Address

- ▶ The applicant confirms with his signature, that
- ▶ he agrees with submitting all relevant documents (Page 2)
- ▶ all declarations made in relation to the information contained in the certificate have been authorized by an Authorised Signatory
- ▶ he accepts and will conform with the conditions of use (Page 3)

Authorised Signatory

Signature Authorised Signatory

Signature Authorised Signatory

Last Name, First Name (block letters)

Last Name, First Name (block letters)

QuoVadis Trustlink Schweiz AG (for internal use)

Place, Date

Signature Registration Agent

QuoVadis Trustlink Schweiz AG

Poststrasse 17, Postfach, 9001 St. Gallen, Schweiz

Telefon + 41 71 272 60 60, E-Mail info.ch@quovadisglobal.com

www.quovadis.ch

Necessary official identity and registration documents

In addition to the signed application form (page 1), the following documents are required:

- ▶ copy of passport or ID of the applicant
- ▶ copy of passport or ID of every authorised signatory
- ▶ copy of current company registration document

Important:

- ▶ An easily readable colour copy of the official Passport or identity card (both sides) shall be made
 - ▶ The passport/ ID-card must be valid at the date of issuing a certificate
-

Send Documents to QuoVadis

Please send all required documents to QuoVadis:

QuoVadis Trustlink Schweiz AG
Poststrasse 17
Postfach
9001 St. Gallen

General Conditions for the Use of QuoVadis Certificates

General Naming Conventions

The name must clearly identify the certificate holder in humanly understandable form. Certificates may only be issued in the correct (registered) name of the certificate holder. Anonymous certificates are not allowed. The name of the certificate holder must be conclusive. A name may only be used multiple times if the certificate holder has multiple certificates with different key usages. Allowed characters are: a-z A-Z 0-9 / space.

Certificate Acceptance

Incorrectly issued certificates must be reported to QuoVadis without delay. A certificate is accepted by the certificate holder if the certificate is used, or no report is made to QuoVadis within 10 days after issuance.

Obligations of the Certificate Holder

The user agrees to:

- a.) to secure and protect the private key (including password, token or smartcard, and activation data) from theft, manipulation, endangerment, loss, damage, defect, release, changes, or unauthorised use
- b.) to exercise sole and complete control over the use of the private key
- c.) to inform QuoVadis without delay about situations where the holder believes or suspects a violation of the conditions in point a)
- d.) to use the certificate only according to all applicable laws and regulations
- e.) to immediately cease the use of the certificate upon revocation or expiry of the user contract
- f.) to take all necessary measures to not compromise the security or integrity of the QuoVadis PKI
- g.) to immediately request revocation upon loss or misuse of the private key
- h.) to inform QuoVadis in writing or via signed E-Mail within one month after changes of certificate holder data, in particular the name of the company/organisation, home or email address
- i.) to pay agreed fees in a timely fashion

If the certificate holder is in violation of the above-mentioned responsibilities, QuoVadis has the right to revoke the certificate at the client's cost.

Liability of the Certificate Holder according to CO

Swiss Code of Obligations art. 59a F

¹ The owner of a cryptographic key used to generate electronic signatures or seals is liable to third parties for any loss or damage they have suffered as a result of relying on a valid certificate...

² The owner is absolved of liability if he can satisfy the court that he took all the security precautions that could reasonably be expected in the circumstances to prevent misuse of the cryptographic key.

Revocation

Certificates may be revoked via E-Mail, telephone, or in handwriting to QuoVadis. Suspensions are not allowed. Once declared invalid, certificates cannot be renewed or extended.

Certificate Renewal with a new Key

The certificate holder confirms upon certificate renewal that the certificate information remains unchanged and that the photo ID produced upon initial application is still valid. The old certificate will not be revoked after issuance of the new certificate and remains valid until its expiration.

Contract Duration

This contract starts with issuance of the certificate and ends with the expiration of the certificate. Before the certificate expires, QuoVadis informs the certificate holder about the possibility of certificate renewal.

Retention period

The retention period of documents and certificates at QuoVadis is based on legal requirements.

Privacy Notice

The privacy notice can be found at https://www.quovadis-global.com/~media/Files/Repository/WISeKey_QuoVadis_Privacy_Notice_-_Certs_and_Signing.ashx

In order to process digital certificates, certificate content information is transferred outside Switzerland and EU to where our back-end certificate processing systems are located. This data is restricted to the data that will be included in the digital certificate and certain Trust/Link user data for the purposes of authentication and audit logging. The transfer takes place over an encrypted connection.

Additional Information

The website www.quovadisglobal.com/repository provides additional information and documents relating to users' rights and obligations. Changes to these documents are published to the website.

Contact, further Assistance, Revocation Service (7x24x365), Support (office hours)

QuoVadis Trustlink Schweiz AG, Poststrasse 17, 9001 St. Gallen
Tel. +41 71 272 60 60, info.ch@quovadisglobal.com,
www.quovadis.ch

Revocation service: www.quovadis.ch/revocation
Support: support.ch@quovadisglobal.com

Impressum

QuoVadis, a WISeKey company, is an internationally accredited certification service provider (CSP Certification Service Provider) with worldwide recognition (WebTrust). We offer electronic certificates according to Swiss legislation (ZertES) and European standard (ETSI).