



Registration of root certificate

please leave empty Root-ID:

Kontrolliert am/durch OSM:

Geprüft/freigegeben am:

Erfasst am/durch WES IT:

Send the completed and duly signed form and the root certificate to the address on the right.

SIX Interbank Clearing Ltd
SIC Operations
Hardturmstrasse 201
P.O. Box
8021 Zurich

Participants:

(name of the financial institution)

IID (BC no.):

Issuer of the root certificate (issuer):

Root certificate valid until:

(The certificate must still be valid for at least five years at the time of application)

Thumbprint of the root certificate:

(The thumbprint data shall be taken from the root certificate and entered in the table.)

With this application, we instruct SIX to use the root certificate on the data carrier enclosed with this letter as the basis for our means of authentication in accordance with the Terms and Conditions of Use. We accept the enclosed Terms and Conditions of Use and confirm the accuracy of the information provided.

Place and date

Legally binding signature(s) of the participant

Name(s)

Terms and Conditions of Use of SIX Interbank Clearing AG ("SIX Interbank Clearing") for access to the RTGS systems via the web portal

1. Terms

Participants: Financial institutions with a valid supplementary and service agreement (participant agreement) with SIX Interbank Clearing for use of the RTGS systems SIC and euroSIC.

User: A person authorized by a participant vis-à-vis SIX Interbank Clearing working for the participant who uses the web portal.

Third-party providers: Institutions offering electronic certificates that can be used for authentication vis-à-vis other parties. Third-party providers can be commercial providers, e.g. QuoVadis, but also participants with their own certificate infrastructure.

2. Access to the RTGS systems via the web portal

SIX Interbank Clearing shall grant the user access to the RTGS systems via the web portal either

- with a user certificate issued by SIX Interbank Clearing and a PIN or
- with a user certificate issued by a third-party provider approved by SIX Interbank Clearing and a PIN

(hereinafter "means of authentication"). The corresponding manuals or user instructions of SIX Interbank Clearing shall apply for the functionality of the web portal. The user has access to the participant's data in the RTGS systems, can use the modules released for him/her by the participant and carry out the corresponding application cases in the RTGS systems.

3. Interruption of service

SIX Interbank Clearing reserves the right to interrupt access to the RTGS systems via the web portal at its discretion to protect the participant and SIX Interbank Clearing at any time. SIX Interbank Clearing accepts no liability for any loss or damage arising from such interruptions.

4. Data protection

SIX Interbank Clearing undertakes to comply with the provisions of the Swiss Federal Data Protection Act; the data sent to SIX Interbank Clearing shall be treated as confidential. Any personal data that becomes known shall remain confidential and protected and shall only be used for the purpose for which it was disclosed to SIX Interbank Clearing. The participant acknowledges that data may be sent over an open network that is accessible to everyone (Internet). As such, data is regularly sent across international borders on an uncontrolled basis. This also applies to data that is transferred between two parties located in Switzerland.

5. Means of authentication of SIX Interbank Clearing

Means of authentication of SIX Interbank Clearing shall be used exclusively for authentication vis-à-vis the web portal within the scope of the contractually agreed services. The sole purpose of use is client authentication within the scope of the SSL protocol for accessing the web portal and authorization in the RTGS systems. SIX Interbank Clearing accepts no liability for the user certificates being used for other purposes.

6. Means of authentication of third-party providers

When certificates issued by third-party providers are used, SIX Interbank Clearing checks whether it authorizes them for access to the RTGS systems via the web portal. The decision regarding authorization is at the discretion of SIX Interbank Clearing. Certificates issued by third-party providers must fulfil at least the following requirements:

- The user certificate must be saved on a hardware-based security token;
- Validity of the user certificates: not expired, with new applications, still valid for at least nine months;
- Validity of the root certificates: not expired, with new applications, still valid for at least five years;
- Standard: X.509 V3;
- Signature algorithm: sha1RSA;
- Key length: at least 2048 bit;
- Key usage: Client authentication, digital signature;
- A minimum number of possible users for access to the web portal.

Recommended certificate:

- www.quovadisglobal.ch

Other solutions of equivalent quality may also possibly be accepted in respect of individual requirements. SIX Interbank Clearing reserves the right to change the requirements for the certificates issued by third-party providers and, if applicable, withdraw the authorization of individual certificates at its discretion for an important reason, also at short notice. SIX Interbank Clearing accepts no liability for any loss or damage arising from such procedures. The participant is responsible for delivering a root and user certificate to SIX Interbank Clearing; the participant shall deliver the root certificate SIX Interbank Clearing via data carrier.

The participant must ensure that root and user certificates are extended in good time before expiry, if required. SIX Interbank Clearing will not verify certificate block lists.

7. Security

The data transmitted between the user and the web portal is encrypted. As the data are transmitted via the Internet, absolute security cannot be guaranteed even with encrypted transmission. There is therefore a residual risk that unauthorized persons may gain access to the data transmitted or infiltrate the RTGS systems using the identity of the user. This residual risk is borne exclusively by the participant. Authentication vis-à-vis the web portal is carried out solely using the user's means of authentication. SIX Interbank Clearing cannot and does not check the actual identity of the user of the means of authentication.

8. Duty of care

The participant is responsible for the secure use and storage of the means of authentication by the user and shall request that he/she protects the means of authentication from misuse by unauthorized persons. The participant bears all risks that may arise in connection with the disclosure of the user's means of authentication or their use – even in the case of misuse. Changes or deletions in respect of the user (e.g. as a result of leaving the employment relationship) shall be reported to SIX Interbank Clearing immediately in writing.

9. Block

If there is reason to assume that the means of authentication have been misused or could be misused (e.g. in the event of loss, careless conduct, etc.), the user must immediately be blocked by the participant or the user. A block will be processed within a customary period of time. The participant bears the risk for the means of authentication being used prior to access being blocked. A written application from the participant is required to discontinue the block.

10. Exclusion of liability

SIX Interbank Clearing shall only be liable for any loss or damage caused intentionally or as a result of gross negligence. In particular, SIX Interbank Clearing shall not be liable for loss or damage incurred by the participant as a result of transmission faults, technical defects, overloading, interruptions (incl. system maintenance work), disruptions and illegal interference or due to any other defects on the part of telecommunications and network providers. Furthermore, in applying the usual level of due care and attention, SIX Interbank Clearing shall not be liable for the consequences of disruptions or interruptions to the web portal. It shall also not be liable for loss or damage incurred as a result of the use of inadequate or expired certificates issued by third-party providers or the misuse or incorrect use of certificates.

11. Notice of cancellation

The participant may terminate the user's access to the RTGS systems via the web portal subject to a notice period of one month to the end of a calendar month.

12. Prices

SIX Interbank Clearing shall charge the participant for access to the web portal in accordance with the current price list.

13. Amendments

SIX Interbank Clearing reserves the right to amend these Terms and Conditions of Use and all user instructions for the web portal at any time. Any amendments shall be announced in writing via a notification in the web portal or by any other suitable method.

14. German as the default language

In the event that any passages in the translations of these Terms and Conditions of Use are unclear or open to misinterpretation, the interpretation of the German version of these Terms and Conditions of Use shall take precedence.

15. Applicable law and place of jurisdiction

These provisions are subject to Swiss law; the place of jurisdiction is Zurich.