Zürcher Kantonalbank

User Manual for SecMail

Communicate with us by email in a simple and secure way

Table of contents

SecMail is an e-mail service of Zürcher Kantonalbank which enables secure e-mail communication using standardised S/MIME technology between your company and Zürcher Kantonalbank. SecMail requires a certain technical infrastructure on your part (see section 3.2).

SecMail is not suitable for payment, trading and other time-critical orders, as timely processing cannot be guaranteed. Please use our eBanking or eBanking Mobile for such orders.

SecMail's support for smartphones cannot be guaranteed. If you want to use a smartphone to send messages to your customer advisor, we recommend using our eBanking Mobile or WebMail.

1 Security

According to the current state of technology, both the content of the e-mail and attachments enjoy a high level of security against unauthorised access by third parties. However, the recipient's e-mail address(es), the date and the subject of the e-mail cannot be encrypted according to the Internet standard.

By using certificates, the authenticity on both sides can be verified.

If the e-mails are transmitted between your e-mail client and your S/MIME infrastructure via the Internet, e.g. if the S/MIME infrastructure is operated by third parties, then this transmission must be encrypted. If this is not the case, please contact your account manager for clarification of possible alternatives.

2 Infrastructure

2.1 Infrastructure used at Zürcher Kantonalbank

Zürcher Kantonalbank uses a "Mail Encryption Gateway" for the encryption of e-mails. This is responsible, among other things, for the encryption and decryption of the e-mails as well as for the exchange and management of the certificates required for this.

The "Mail Encryption Gateway" of the Zürcher Kantonalbank:

- obtains "X.509 user certificates" for its own employees from the company SwissSign AG
- protects the corresponding "private keys" from unauthorised access
- requests certificates from the e-mail recipient if technically necessary
- encrypts and signs the e-mails to be sent if requested by the sender

  Important: This is not a digital signature in the legal sense but merely an integrity check.
- decrypts and verifies the signature of the received e-mails
- transmits "X.509 user certificates" when requested

2.2 Necessary infrastructure on your side

The following infrastructure is necessary for the use of SecMail:

- Either your own e-mail domain (e.g. @musterag.ch), which is activated as a whole for SecMail, or one or more group mailboxes (e.g. buchhaltung@musterag.ch) and/or personal e-mail addresses (e.g. felix.meier@musterag.ch).
- S/MIME-compatible gateway solution or S/MIME-compatible mail client solution
- The key length of the CA as well as user certificates used must have a length of 2048 bits. SHA1 is considered an insecure hash algorithm and should therefore no longer be used.
- X.509 user certificates" from a recognised certificate issuer[1] for the e-mail addresses you use in communication with Zürcher Kantonalbank.

Notes:

a) The "X.509 user certificate" must have the intended use "signing and encrypting e-mail messages".
b) If domain encryption is used for communication with Zürcher Kantonalbank by means of a domain certificate, an "X.509 domain certificate" is also required for each e-mail domain to be connected.
c) If no domain certificate is used, then certificate requests from the Zürcher Kantonalbank e-mail gateway must be answered once either automatically by your e-mail gateway or manually by the recipient before e-mails from Zürcher Kantonalbank can be delivered in encrypted form.
d) The e-mail address of the user or the "RFC822 name" must be stored in the certificate field "Alternative applicant name".

3 Procedure

To use SecMail, you must proceed as follows:

1. Have the person responsible for your e-mail infrastructure (hereinafter referred to as the "technical contact") check whether the necessary infrastructure (see point 3.2) is already in place.
2. If the necessary infrastructure is in place on your side, then
   a) provide your account manager with either your e-mail domain or mailboxes and/or personal e-mail addresses,
   b) the details of the technical contact person (surname, first name, e-mail address, telephone number), and
   c) one or two authorised signatories[2], who will receive the agreement for communication via SecMail.
3. The IT department of Zürcher Kantonalbank will contact your technical contact person.
4. After receiving the signed agreement for communication via SecMail, our IT and the technical contact will exchange the domain certificates used, if applicable.
5. The technical contact person must check whether their SMIME software (e-mail gateway or client) already trusts the RSA SMIME LCP ICA 2021 – 2 certificate of the company SwissSign AG, see https://www.swisssign.com/support/ca-prod.html .
6. Tests are carried out by the technical contact person and our IT department.
7. If the tests are successful, the technical contact person and our IT agree on the time of commissioning SecMail.
8. After commissioning SecMail: If no domain certificate is used, certificate requests from the Zürcher Kantonalbank e-mail gateway must be answered once either automatically by your e-mail gateway or manually by the recipient before e-mails can be received from Zürcher Kantonalbank.

[1] Cf. the list of MS Internet Explorer, Firefox and Chrome certification authorities or the list of certification service providers recognised under the Federal Act on the Electronic Signature by the Swiss Federal Accreditation Service SAS, see https://www.sas.admin.ch/sas/de/home/akkreditiertestellen/akkrstellensuchesas/pki1.html .
[2] Depending on whether there is individual or collective signing authority

4 Usage

Depending on the solution, gateway or mail client you use, the e-mails are either automatically signed and encrypted or the user must manually select the "Sign" option as well as the "Encrypt" option in their mail client before sending an e-mail. Please consult the corresponding user manual of your mail client.

Whether a received e-mail has been signed and by which sender should be indicated in your mail client in the e-mail display screen by means of a seal icon and the sentence "Signed by: [sender's e-mail address]". This depends on the mail client you are using. Please consult the corresponding user manual of your mail client.

Note

Encrypted e-mails can only be viewed by persons / systems (e.g. archives) who have the corresponding certificate or private key. The private key must be taken care of accordingly. If there is any suspicion of misuse of the private key, the certificate issuer must be immediately blocked and Zürcher Kantonalbank must be notified without delay.

5 Administration

5.1 Deleting an account

If you no longer wish to communicate with Zürcher Kantonalbank via SecMail, the agreement for communication via SecMail must be terminated in accordance with the conditions described therein. To do this, please contact your client advisor.

5.2 Change of e-mail address

If you plan to change the name of the e-mail domain / group mailbox / personal e-mail address connected to SecMail or to connect an additional e-mail domain / group mailbox / personal e-mail address to SecMail, please inform us in good time. In this case, you must sign a new agreement for communication via SecMail. The procedure is as described in point 4 from step 2 onwards.

5.3 Certificate validity period

Please note that your certificates have a limited period of validity. You must make timely efforts to renew your certificates with your certificate issuer and send us the new certificates in good time. After the validity period has expired, e-mails signed and encrypted by outdated certificates will no longer be accepted by the "E-Mail Encryption Gateway" of Zürcher Kantonalbank.

6 Support and help

If you have any questions about the service or a concern, please contact your customer advisor.

For technical questions, please call **eBanking Support** at:

Phone	+41 44 293 99 15
Monday until Friday	08.00 - 17.30 Uhr