COMMERZBANK
Die Bank an Ihrer Seite

Corporate Banking

Terms and Conditions for Placing Orders with Electronic Signatures

Status 12 January 2018

1. Scope of validity

The following provisions shall apply to electronically signed orders that are submitted via the SWIFT FileAct communication channels or transmission processes agreed individually between the customer and the Bank (contractual parties). They shall not apply to remote data transmission with the EBICS standard communication procedure.

2. Scope of services

The Bank shall be available to the customer for electronic order placement. Data transfer shall comprise order placement in the specially agreed scope and in the agreed format. Orders shall be authorised by the customer or an authorised representative with an electronic signature.

3. User

The customer and the authorised representative shall hereinafter be uniformly referred to as the User.

4. Accepted signature media, authentication tool, signature medium

The Bank shall accept electronic signatures that were created with the signature certificates and procedures listed in Annex 1.

The electronic signature of the User shall be created with the help of a private key and personal password, together with the certificate assigned to the signature. It is the authentication tool as defined by article 1367, paragraph 2 of the French Civil Code, the French Décret No. 2017-1416 of 28 September 2017 which refers to articles 26, 28 and 29 of the European Regulation No. 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.
In order to check the electronic signature, the User must attach its certificate with the public key to every order.

The User shall ensure that the private key is further secured by means of a password and that the private key is stored together with the certificate and public key on a secure signature medium that is protected from third-party access (e.g. token, USB stick).

5. Provisions for the use of digital certificates

A certificate is an electronic certificate from a provider agreed upon by the contractual parties with which a person's signature verification data are assigned and the identity of this person is confirmed, in connection with an agreement between the contractual parties if applicable.

Only those certificates may be used which are issued by the certification authority directly for the purpose of confirming the electronic signature of the User and without the use of intermediate certificates.

The certification authorities agreed upon by the contractual parties can be found in Annex 1. Insofar as the Bank has no access to the certification authority's certificate revocation lists, the customer shall ensure that the Bank receives access at the Bank's request.

The User shall notify the Bank separately of a restriction on the scope of use or the revocation of the certificate. The customer shall ensure that the certificate does not create a conflict between the use of the electronic signature to authorise orders and the regulations for placing orders. The certificate may not contain any attributes that restrict its use in the authorization of orders except in view of the certificate's validity. Restrictions on the intended use of the electronic signature must be agreed separately between the User and the Bank. If a different scope of use or deviating entitlement to authorization is arranged between the attribute and the agreed options for order placement, the agreed provisions for placing orders shall be decisive in case of doubt.

6. Identification of the User in the use of certificates

Before placing the first order with an electronic signature, the User shall provide the Bank the details of his certificate and agree with the Bank the definitive assignment of the certificate to the User.

The person placing the order shall be identified by the Bank using the "Distinguished Name" provided in the certificate. The customer shall undertake to ensure that certificates with the same "Distinguished Name" issued by the certification authority are only accessible by the User that the customer or authorised representative agrees with the Bank to be the holder of the certificate.

7. Technical requirements of the electronic signature

Signed orders sent to the Bank must be created in accordance with the agreed signature formats in Annex 1 and with the signature procedures listed therein.

Insofar there is an order for which the order details and the signature are submitted separately, these must be transmitted in a container format supported pursuant to Annex 1. The container may only contain a user data file and a file containing the signatures and public keys.

8. Procedural provisions

The submitted order details must be authorised by electronic signature as agreed with the Bank. The order details shall become an effective order when all required electronic User signatures - pursuant to a separate agreement - have been received by remote data transmission, the agreed formats are observed and the electronic signatures can be successfully checked using the agreed keys.

9. Rules of conduct/due diligence for handling the signature medium for authorizing orders

Insofar as the User creates his own keys, private keys must be generated using a medium that the User has under his sole control. Insofar as the keys are provided by a third party, it must be ensured that the User has sole possession of the private keys.

For private keys used for signature, each User shall create a password only known to the User, which protects access to the private key.

The User may place orders with the help of the authentication tool agreed with the Bank. The customer shall ensure that every User sees to it that no other person obtains his signature medium or learns the personal password intended to protect the private key. Any other person who obtains the medium or a corresponding duplicate can make improper use of the agreed services in connection with the relevant password. The following should be noted in particular with regard to confidentiality:

- The data identifying the User may not be stored anywhere but the signature medium, e.g. on the computer's hard drive.
- When remote data transmission is concluded, the signature medium must be removed from the reading device and stored in a safe place.
- The password for protecting the signature medium or the personal key may not be written down or stored electronically.
- It should be ensured that no other persons are watching when a password is entered.

10. Blocking of an electronic signature

If a signature medium is lost, other persons obtain the private key or there is suspicion of improper use, the User must immediately block his electronic signature or have it blocked by the Bank. The block must be applied to all Bank systems that use the compromised key. This shall apply even if the revocation of the public key or certificate was entered in a public barred list or in the barred list of the certification authority. If the Bank cannot access one of the aforementioned barred lists through no fault of its own, in case of doubt it shall be entitled to execute the order.

The User may have his electronic signature blocked vis a vis the Bank using the blocking facility disclosed by the Bank. The User may also issue the Bank a blocking notification at any time using the separately provided contact details.

11. Handling of order details by the Bank

The order details provided to the Bank by electronic data transmission shall be processed within the normal course of business.

When validating the electronic signature, the Bank shall in particular check that a temporarily valid key has not expired and that the signature for the check sum in the order details is correct. When using certificates, the Bank shall also check that the certificate used was issued by an agreed certification authority.

If a properly signed order contains additional electronic signatures that are invalid or for which there is no power of attorney for the signatory, the Bank shall be entitled to reject the order.

12. Order execution

The Bank shall carry out orders if all of the following execution conditions are on hand or have been fulfilled:

- The order details delivered by electronic data transmission were authorised in accordance with the agreement.
- The agreed data format has been observed.
- The execution conditions according to the special conditions applicable to the respective order type have been fulfilled.
- Execution of the order may not breach any other statutory provisions.

If the execution conditions pursuant to paragraph 1 have not been met, the Bank shall not execute the order and shall inform the customer of non-execution of the order immediately and in the agreed manner. If possible, the Bank shall notify the customer of the reasons and errors that resulted in non-execution of the order and how these errors can be rectified. This shall not apply if the statement of reasons is in breach of other statutory provisions.

13. Revocation

The ability to revoke an order shall be determined based on the applicable special conditions (e.g. the General Terms of Business of Commerzbank’s Paris Branch). Orders may only be revoked by means other than electronic data transmission. To this end, the customer must notify the Bank of the particulars of the original order.

14. Liability

14.1. Liability of the Bank for unauthorised, non-executed and improperly executed orders

The Bank's liability for unauthorised, non-executed and improperly executed orders shall be governed by the special conditions agreed for the respective order type (e.g General Terms of Business of Commerzbank’s Paris Branch) and to this respect, it is reminded that by virtue of Article L.133-2 of the French Monetary and Financial Code, the User and the Bank expressly agree not to apply the provisions of Articles L. 133-19, L. 133-20, L. 133-22, L. 133-23 and L. 133-25 of the French Monetary and Financial Code.

14.2 Liability of the customer for improper use of the electronic signature or signature medium

14.2.1. Liability of the customer for unauthorised orders prior to the blocking notification

If unauthorised orders executed prior to the blocking notification being sent to the Bank are based on the use of a lost, stolen or otherwise missing electronic signature or any other improper use of the electronic signature or signature medium, the customer shall be liable for losses incurred by the Bank as a result if the User is at fault for the loss, theft, other misplacement or other improper use. The customer shall also be liable if he has not carefully selected an appointed User and/or if he has not regularly checked the User's compliance with his obligations pursuant to these conditions. If the Bank has negligently contributed to the occurrence of a loss, the extent to which the customer and the Bank are to bear the loss shall be determined pursuant to the principles of contributory negligence.

If the order concerns a payment transaction, the customer shall not be obliged to compensate the loss pursuant to paragraph 1 if the User was not able to issue the blocking notification pursuant to section 10 because the Bank did not ensure the ability to receive the blocking notification and the loss occurred as a result.

The liability for losses that are incurred within the time frame for which a transaction limit applies shall be limited to the respective agreed transaction limit.

14.2.2 Liability of the Bank from the time of the blocking notification

As soon as the Bank receives a blocking notification from a participant, it shall subsequently assume all losses arising from unauthorised orders. This shall not apply if a participant has acted fraudulently.

15. Change in participant keys

If the certificates agreed with the participant are temporary, the User must notify the Bank of the new public keys in good time prior to the expiry date. When renewing certificates, the Bank must only be informed if the User's identification features agreed in section 6 change.

Commerzbank AG

Annex 1

Approved certificates	• x.509v3 certificates (pursuant to the specifications of the Internet Engineering Task Force, RFC 5280 www.ietf.org)
Approved certification authorities	• SWIFT (3skey)
Approved signature formats	• "Cryptographic Message Syntax" (CMS, pursuant to the specifications of the Internet Engineering Task Force, RFC 5652)
Accepted signature procedures	• SHA256 with RSA signature
Container formats for the submission of separate signatures	• Currently not supported

Commerzbank AG