COMMERZBANK
The bank at your side

Terms and Conditions for Remote Data Transmission

(As amended on 14 September 2019)

1. Scope of services

(1) The Bank is available to its Customer (account holder) for remote transmission of data by electronic means, hereinafter referred to as "remote data transmission". Remote data transmission comprises submitting and downloading files (in particular, transmission of orders and downloading information).
(2) The Bank will notify the Customer of the types of services which the Customer may use within the framework of remote data transmission. The use of the remote data transmission is subject to the disposal limits agreed with the Bank.
(3) Remote data transmission is possible via the EBICS interface (Annexes 1a to 1c).
(4) The structure of the data records and files for transmission of orders and download of information is described in the data format specification (Annex 3) or agreed upon separately.

2. Users and subscribers, identification and security media

(1) Orders may only be placed via the EBICS interface by the Customer or the Customer's authorised account representatives. The Customer and the authorised account representatives are hereinafter collectively named "Users". To authorise order data transmitted by remote data transmission with an electronic signature, each User requires individual identification media which must be activated by the Bank. The requirements for the identification media are defined in Annex 1a. If agreed with the Bank, orders transmitted by remote data transmission can be authorised with a signed accompanying document/collective order.
(2) For data exchange via EBICS, the Customer may designate "technical subscribers" in addition to the authorised signatories, who must be natural persons and who are only authorised to carry out data exchanges. Users and technical subscribers are hereinafter collectively named "Subscribers". To protect the data exchange, each Subscriber requires individual security media which must be activated by the Bank. The requirements for the security media are described in Annex 1a.

3. Procedural provisions

(1) The requirements described in Annex 1a, in the technical interface documentation (Annex 1b) and in the data format specification (Annex 3) shall apply to the transmission method agreed upon between the Customer and the Bank.
(2) The Customer is obliged to ensure that all Subscribers observe the remote data transmission procedure and the specifications.
(3) The assignment of data fields is governed by the completion and control guidelines applicable to the specific format used (Annex 3).
(4) The User shall supply the payee's or payer's correct unique identifier as per the applicable special conditions. The payment service providers engaged in processing a payment order are authorised to process the payment solely on the basis of the unique identifier. Incorrect details may result in an order being misdirected. Any losses and disadvantages this causes shall be borne by the Customer. ~~This provision shall apply accordingly if any other orders (not payment orders) are transmitted by remote data transmission.~~
(5) Prior to the transmission of the order data to the Bank, a record of the full contents of the files to be transmitted and of the data transmitted for the verification of identification must be prepared. The Customer has to keep this record for a minimum period of 30 calendar days from the date of execution given in the file (for transfers) or due date (direct debits), or if there are several dates, the latest date, in such a form that it can be made available to the Bank again at short notice on request, unless otherwise agreed.
(6) In addition, the Customer must generate an electronic protocol for every submission of files and every file download according to section 10 of the specification for the EBICS interface (Annex 1b), keep the protocol on file and make it available to the Bank on request.
(7) To the extent that the Bank provides the Customer with data on payment transactions which are not yet finally processed, such data shall be deemed to be only nonbinding information. Such data will be specially marked.
(8) The order data submitted via remote data transmission shall be authorised either by an electronic signature or by a signed accompanying document/collective order as agreed with the Bank. Such order data shall be effective as an order
a) for data submitted with an electronic signature:
- if all necessary electronic signatures of the Users have been received by remote data transmission within the agreed period, and
- if the electronic signatures can be successfully checked against the agreed keys;
b) for data submitted with an accompanying document/collective order:
- if the Bank receives the accompanying document/collective order in the agreed period, and

– if the accompanying document/collective order has been signed in accordance with the account mandate.

4. Duties of conduct and care with respect to the identification media for the authorisation of orders

(1) Depending on the transmission procedure agreed with the Bank, the Customer is obliged to ensure that all Users comply with the obligations arising from these conditions and the identification procedures described in Annex 1a.

(2) The User may place orders by an identification medium activated by the Bank. The Customer shall ensure that every User takes care that no third party obtains possession of the User's identification medium or gains knowledge of the password protecting it. This is because any third person who has obtained possession of the medium or a duplicate thereof can, in conjunction with the corresponding password, misuse the agreed services. The following shall be observed in particular to protect the identification media and the password secret:

- the identification medium must be protected against unauthorised access and stored securely;
- the password protecting the identification medium may not be written down on the identification medium or kept as a copy together with it or insecurely stored electronically;
- the identification medium must not be duplicated;
- when entering the password, care must be taken to ensure that no other persons can steal it.

5. Duties of conduct and care for dealing with the security media required for data exchange

With respect to connection via EBICS, the Customer is obliged to ensure that all Subscribers comply with the security procedures described in Annex 1a. The Subscriber shall secure the data exchange by means of the security media activated by the Bank. The Customer is obliged to request each User to ensure that no third party obtains possession of the security medium or is able to use it. In particular as regards storage in a technical system, the Subscriber's security medium must be stored in a technical environment which is protected against unauthorised access. This is because any third person who gains access to the security medium or a duplicate thereof may misuse the data exchange.

6. Security of the customer system

The Customer shall ensure that the systems used for the remote data transmission are adequately protected. The security requirements that are applicable to the EBICS procedure are described in Annex 1c.

7. Suspension of the identification and security media

(1) If the identification or security media are lost, become known to third parties or misuse of such media is suspected, the Subscriber must immediately request that the Bank suspend the remote data transmission access. Further details are stipulated in Annex 1a. The Subscriber can also request that the Bank suspend the access at any time via the separately notified contact data.

(2) Outside the remote data transmission procedure, the Customer may request suspension of a Subscriber's identification and security media or the entire remote data transmission access via the suspension facility notified by the Bank.

(3) If misuse is suspected, the Bank will suspend the entire remote data transmission access. It will inform the Customer of this suspension outside the remote data transmission process. Such a suspension cannot be cancelled via remote data transmission.

8. Treatment of incoming order data by the Bank

(1) The order data transmitted to the Bank by remote data transmission are processed during the normal course of work.

(2) On the basis of the signatures generated by the Subscribers with the security media, the Bank will verify whether the sender is authorised for the data exchange. If this verification reveals any discrepancies, the Bank will not process the affected order and will notify the Customer thereof immediately.

(3) The Bank will verify the identification of the User(s) and the authorisation of the order data transmitted by remote data transmission on the basis of the electronic signatures generated by the Users with the identification media or on the basis of the accompanying document/collective order provided and will check that the order data records comply with the provisions specified in Annex 3. If this verification reveals any discrepancies, the Bank will not process the affected order data and will notify the Customer thereof immediately. The Bank may delete order data not fully authorised after expiry of the time limit that is separately notified by the Bank.

(4) If errors are revealed by the Bank's verification, pursuant to Annex 3, of files or data records, the Bank will provide proof of the errors in the files or data records in a suitable form and notify the User thereof immediately. The Bank is authorised to exclude files or data records with errors from further processing if a proper execution of the order cannot be ensured.

(5) The Bank shall be obliged to document in the customer protocol the above procedures (cf. Annex 1a) and the forwarding of the orders for processing. The Customer in turn shall be obliged to call up the customer protocol without undue delay and to keep himself/herself informed of the processing of the order. In the event of any discrepancies, the Customer should contact the Bank.

9. Recall

(1) Before the authorisation of the order data, the Customer shall be entitled to recall the file. Individual order data can only be changed by recalling the whole file and placing the order again. The Bank can only accept a recall if it reaches the financial institution in good time so that it can be taken into account in the course of the normal working processes.

(2) The extent to which an order can be recalled shall be governed by the applicable special conditions (for example Terms and Conditions for Payment Services). Cancellation of orders can only take place outside the remote data transmission process or if agreed with the Customer pursuant to the regulations detailed in section 11 of Annex 3. To do this, the Customer must inform the Bank of the individual details given in the original order.

10. Execution of orders

(1) The Bank will carry out the orders if all of the following requirements for execution have been fulfilled:

- the order data submitted by remote data transmission must have been authorised in accordance with 3. (8) above;
- the defined data format must be complied with;
- the disposal limit must not be exceeded;
- the requirements for execution must be fulfilled in accordance with the special conditions applicable to the relevant order type.
- ~~the execution of the order must not violate any other legal provisions.~~

(2) If the conditions for execution outlined in 9. (1) above are not fulfilled, the Bank will not execute the order and will inform the Customer that the order has not been executed without undue delay through the agreed communication channel. As far as possible, the Bank will notify the Customer of the reasons and errors which caused the order not to be executed and the possible ways to correct these errors. ~~This shall not apply if giving reasons would violate any other legal provisions.~~

~~11. Security of the Customer's system~~

~~The Customer shall ensure that the systems used for the remote data transmission are adequately protected. The security requirements that are applicable to the EBICS procedure are described in Annex 1c.~~

11. Liability

11.1 Liability of the Bank in the event of an unauthorised remote order and a remote order not executed, executed incorrectly or delayed

The Bank's liability in the event of an authorised remote order and a remote order not executed, executed incorrectly or delayed, is based on the special conditions arranged for the order type in question (e.g. terms and conditions for payment services).

11.2 Liability of the Customer in the event of misuse of the identification or security media

11.2.1 Liability of the Customer in the event of unauthorised payment transactions prior to a blocking request

(1) Liability of the Customer that is not a consumer
If an unauthorised payment transaction prior to a blocking request is based on the misuse of their identification or security medium, the Customer shall be liable for the losses consequently incurred by the Bank if the Subscriber has negligently or wilfully breached his duties of conduct or care. Section 675v of the German Civil Code shall not apply.

(2) Liability of the Customer that is a consumer

a) If an unauthorised transaction prior to a blocking request relates to the use of a stolen or otherwise missing identification or security medium or to any form of misuse of the aforementioned, the Customer shall be liable for the losses consequently incurred by the Bank up to an amount of 50 euros, regardless of whether the Subscriber is culpable for this loss, theft or otherwise missing identification or security medium or any form of misuse of the aforementioned.

b) The Customer is not obliged to provide compensation for the loss pursuant to (2) a) above if

- the loss, theft or misappropriation of the identification or security medium was not detectable to him prior to the unauthorised payment transaction, or
- the loss of the identification or security medium was caused by an employee, agent or branch of the payment service provider or of an entity to which its activities were outsourced.

c) If an unauthorised payment transaction occurs before a blocking request is given and the Subscriber has acted fraudulently or has failed to comply with his/her notification duties or duties of conduct or care according to these conditions by deliberate intent or gross negligence, the Customer shall bear the resulting damage to the full extent. Gross negligence by the Subscriber can include, in particular, if he/she

- does not without undue delay notify the loss, theft or any other form of missing or misuse of the identification or security medium to the Bank after he/she has become aware of the same (see 7. (1) above),
- did not protect the data that identify him/her against unauthorised access and did not keep them securely,
- has noted or unsecurely stored electronically the password that serves to protect the identification medium.

(3) Liability for losses caused within the period applicable to the disposal limit is restricted to the agreed disposal limit in question.

(4) The Customer is not obliged to refund any losses pursuant to (1) and (2) a) and c) if the Subscriber pursuant to 6. (1) could not make the blocking request because the Bank had not ensured the means to receive the blocking request.

(5) (2) b), (3) and (4) shall not apply if the Subscriber acted with fraudulent intent.

11.2.2 Liability of the Customer in the event of other unauthorised transactions prior to a blocking request
If, prior to a blocking request, an unauthorised transaction which is not a payment transaction is based on the use of a lost, stolen, or otherwise missing identification or security medium or any other form of misuse of the aforementioned, and the Bank consequently incurs a loss, the Customer and the Bank shall be liable pursuant to the legal principles of contributory negligence.

11.2.3 Liability of the Bank subsequent to a blocking request
The Bank shall accept liability for all losses incurred due to unauthorised transactions effected after a blocking request has been received from a Subscriber. This does not apply if a Subscriber has acted with intent to defraud.

11.3 Preclusion of liability
Liability claims shall be precluded if the circumstances substantiating a claim are based upon an exceptional and unforeseeable event on which the party invoking this event has no influence and whose consequences could not be avoided even by exercising due diligence.

12. Final provisions

The annexes mentioned in these terms and conditions are part of the agreement made with the Customer.

Annexes:

Annex 1a: EBICS interface
Annex 1b: Specification for the EBICS interface
Annex 1c: Security requirements for the EBICS customer system
Annex 2: Not currently in use
Annex 3: Data format specification

Annex 1a: EBICS interface

1. Identification and security procedures

The Customer (account holder) shall disclose the Subscribers and their authorisations with respect to remote data transmission to the Bank.

The following identification and security procedures are used for the EBICS interface:
- Electronic signatures
- Authentication signature
- Encryption

For each identification and security process, the Subscriber has an individual key pair which consists of a private and a public key. The public subscriber keys shall be disclosed to the Bank in accordance with the procedure described in 2. of this annex. The public bank keys must be protected against unauthorised alteration in accordance with the procedure described in 2. of this annex. The Subscriber's key pairs may also be used for communication with other banks.

1.1 Electronic signatures

1.1.1 Electronic signatures of the Subscribers

The following signature classes are defined for the electronic signatures (ESs) of the Subscribers:
- Single signature (type "E")
- First signature (type "A")
- Second signature (type "B")
- Transport signature (type "T")

The typical electronic signatures for use in banking are ESs of types "E", "A" or "B". Banking ESs are used for the authorisation of orders. Orders may require several banking ESs to be applied by different Users (account holders and their authorised account representatives). For each order type supported, a minimum number of banking ESs shall be agreed on between the Bank and the Customer.

ESs of type "T" are designated transport signatures and cannot be used for banking authorisation of orders, but only for transmission of orders to the bank system. Technical subscribers (see 2.2 in this annex) may only be assigned an ES of type "T".

The program used by the Customer can generate different messages (for example domestic and international payment orders, but also messages concerning initialisation, protocol download and retrieval of account and turnover information). The Bank shall inform the Customer what message types can be used and which ES type must be applied in the specific case.

1.1.2 Authentication signature

In contrast to the ES, which is used to sign order data, the authentication signature is used for an individual EBICS message and is configured via the control and login data and the ESs contained therein. With the exception of a few system-related order types defined in the specification for the EBICS interface specification, authentication signatures must be supplied by both the customer system and the bank system in every transaction step. The Customer must ensure that software is used which, in accordance with the specification for the EBICS interface (cf. Annex 1b), verifies the authentication signature of each EBICS message transmitted by the Bank and which takes into account the current validity and authenticity of the Bank's saved public keys.

1.2 Encryption

To ensure the secrecy of banking data on the application level, the order data must be encrypted in accordance with the specification for the EBICS interface (cf. Annex 1b) by the Customer, who must also take into account the current validity and authenticity of the Bank's saved public keys.

In addition, transport encryption must be utilised for the external transmission paths between the systems of the Customer and the Bank. The Customer must ensure the use of software that verifies, in accordance with the specification for the EBICS interface (cf. Annex 1b), the current validity and authenticity of the server certificates applied by the Bank.

2. Initialisation of the EBICS interface

2.1 Installation of the communication interface

Communication is initialised by utilising a URL (Uniform Resource Locator). Alternatively, an IP address for the respective Bank may be used. The URL or IP address is disclosed to the Customer on conclusion of the agreement with the Bank.

For initialising EBICS, the Bank shall provide the Subscribers designated by the Customer with the following data:
- URL or IP address of the Bank
- Name of the Bank
- Host ID
- Permitted version(s) of the EBICS protocol and the security procedures
- Partner ID (Customer ID)
- User ID
- System ID (for technical subscribers)
- Further specific details on Customer and Subscriber authorisations

For the Subscribers assigned to the Customer, the Bank will assign one user ID which clearly identifies the Subscriber. Insofar as one or more technical subscribers are assigned to the Customer (multi-user system), the Bank will assign a system ID in addition to the user ID. If no technical subscriber is defined, the system ID and user ID are identical.

2.2 Initialisation of the keys

2.2.1 First initialisation of the subscriber keys

The key pairs used by the Subscriber for the banking ESs, the encryption of the order data and the authentication signature shall, in addition to the general conditions described in 1. of this annex, comply with the following requirements:

(1) The key pairs must be assigned exclusively and unambiguously to the Subscriber.
(2) If the Subscriber generates the keys, the private keys must be generated by means which the Subscriber can keep under his/her sole control.
(3) If the keys are made available by a third party, it must be ensured that the Subscriber is the sole recipient of the private keys.
(4) With respect to the private keys used for identification, each User shall define a password for each key which protects access to the respective private key.
(5) With respect to the private keys used to protect the data exchange, each Subscriber shall define a password for each key which protects access to the respective private key. This password may be dispensed with if the Subscriber's security medium is stored in a technical environment which is protected against unauthorised access.

Transmission of the Subscriber's public keys to the bank system is necessary for the Subscriber's initialisation by the Bank. For this purpose, the Subscriber shall transmit their public keys to the Bank via two independent communication channels:
- via the EBICS interface by means of the order types provided by the system for this procedure; and
- via an initialisation letter signed by the account holder or an authorised account representative.

For the Subscriber's initialisation, the credit institution shall verify the authenticity of the public subscriber keys transmitted via EBICS on the basis of the initialisation letters signed by the account holder or an authorised account representative.

The initialisation letter shall contain the following data for each public subscriber key:
- Purpose of the public subscriber key
- Electronic signature
- Authentication signature
- Encryption
- The respective version supported for each key pair
- Specification of exponent length
- Hexadecimal representation of the public key's exponent
- Specification of modulus length
- Hexadecimal representation of the public key's modulus
- Hexadecimal representation of the public key's hash value

The Bank will verify the signature of the account holder or authorised account representative on the initialisation letter and also whether the hash values of the Subscriber's public key transmitted via EBICS are identical to those transmitted in writing. If the verification is positive, the Bank will activate the relevant Subscriber for the agreed order types.

2.3 Initialisation of the bank keys

The Subscriber will download the Bank's public key with an order type specifically provided by the system for this process.

The hash value of the public bank key shall additionally be made available by the Bank via a second communication channel separately agreed with the Customer.

Prior to the first data transmission via EBICS, the Subscriber shall verify the authenticity of the public bank keys sent by remote data transmission by comparing their hash values with the hash values notified by the Bank via the separately agreed communication channel.

The Customer shall ensure that software is used which verifies the validity of the server certificates used in connection with the transport encryption by means of the certification path separately notified by the Bank.

3. Special duties of care in the production of identification and backup media by the Customer

Insofar as the Customer generates his own identification and security media in accordance with the specifications of the EBICS specification and initialises them at his Bank, he must ensure the following:

In all phases of authentication, including display, transmission and storage, confidentiality and integrity of the identification medium must be guaranteed.

Private subscriber keys on the identification and security media must not be stored in plain text.

The identification medium will be blocked at the latest after five incorrect entries of the password.

The private and public subscriber keys must be generated in a secure environment.

The identification and security media are to be assigned and used exclusively and unambiguously to the Subscriber.

4. Placing orders with the Bank

The User shall verify the correctness of the order data and ensure that only the verified data are signed electronically. Upon initialisation of communication, the Bank first carries out Subscriber-related authorisation verifications, such as order type authorisation or verifications of possibly agreed limits. The results of additional banking verifications such as limit verifications or account authorisation verifications will later be notified to the Customer in the customer protocol.

Order data transmitted to the bank system may be authorised as follows:

(1) All necessary banking ESs are transmitted together with the order data.
(2) If the distributed ES ("verteilte elektronische Unterschrift – VEU") has been agreed with the Customer for the respective order type and the transmitted ESs are insufficient for banking authorisation, the order is stored in the bank system until all required ESs are applied.
(3) If the Customer and the Bank agree that order data submitted by means of remote data transmission may be authorised by means of a separately transmitted accompanying document/collective order, a transport signature (type "T") must be supplied for technical protection of the order data instead of the User's banking ES. To this end, the file must bear a special code indicating that there are no further ESs for this order other than the transport signature (type "T"). The order is authorised after the Bank successfully verifies the User's signature on the accompanying document/collective order.

4.1 Placing orders by means of the distributed electronic signature (VEU)
The manner in which the distributed electronic signature will be used by the Customer shall be agreed with the Bank.

The distributed electronic signature (VEU) shall be used where orders are to be authorised independently of the transport of the order data and, if applicable, by several Subscribers.

If all banking ESs necessary for authorisation have not been submitted, the order may be deleted by an authorised User.

If the order has been fully authorised, only a recall pursuant to section 9. of the Terms and Conditions for Remote Data Transmission can be made.

The Bank may delete orders that have not been fully authorised after expiry of the time limit separately notified by the Bank.

4.2 Verification of identification by the Bank
Order data submitted by data transmission are executed by the Bank only after the necessary banking ES or the signed accompanying document/collective order has been received and positively verified.

4.3 Customer protocols
The Bank will document the following transactions in customer protocols:
- Transmission of the order data to the bank system
- Transmission of information files from the bank system to the customer system
- Result of each verification of identification for orders from the Customer to the bank system
- Further processing of orders if they concern the verification of signatures and the display of order data

The Subscriber is obliged to keep himself/herself informed about the result of the verifications carried out by the Bank by downloading the customer protocol without undue delay.

The Subscriber shall include this protocol, the contents of which correspond to the provisions of section 10 of Annex 1b, in their files and submit it to the Bank when required.

5. Change of the subscriber keys with automatic activation

If the validity period of the identification and security media used by the Subscriber is limited, the Subscriber must transmit the new public keys to the Bank in good time prior to the expiry date of such validity period. After the expiry date of the old keys, a new initialisation must be made.

If the Subscriber generates keys himself/herself, the subscriber keys must be renewed using the order types provided by the system for this purpose on the date agreed to with the Bank. The keys must be transmitted in good time before expiration of the old keys.

The following order types shall be used for an automatic activation of the new keys without renewed Subscriber initialisation:
- update of the public banking key (PUB); and
- update of the public authentication key and the public encryption key (HCA); or alternatively
- update of all three above-mentioned keys (HCS).

The User must supply a valid banking ES for order types PUB, HCA and HCS. After the keys have been changed, only the new keys may be used.

If the electronic signature could not be positively verified, the provisions described in section 8. (3) of the Conditions for Remote Data Transmission shall be applicable.

The keys may be changed only after all orders have been completely processed, otherwise orders still unprocessed will have to be placed again using the new key.

6. Suspension of the subscriber keys

If misuse of the subscriber keys is suspected, the Subscriber must suspend the access authorisation for all bank systems using the compromised key(s).

If the Subscriber is in possession of valid identification and security media, the Subscriber can suspend access authorisation via the EBICS interface. If a message with order type "SPR" is sent, access will be suspended for the relevant Subscriber whose user ID was used to send the message. After suspension, the Subscriber can place no further orders via the EBICS interface until the access has been initialised again as described in 2. of this annex.

If the Subscriber is no longer in possession of valid identification and security media, the Subscriber can request suspension of the identification and security media outside the remote data transmission procedure via the suspension facility separately notified by the Bank.

Outside the remote data transmission process, the Customer may request suspension of a Subscriber's identification and security media or of the entire remote data transmission access via the suspension facility notified by the Bank.

Annex 1b: Specification for the EBICS interface

The specification is published on the website http://www.ebics.de

Annex 1c: Security requirements for the EBICS customer system

In addition to the security measures described in Annex 1a section 6, the Customer must observe the following requirements:

- The software used by the Customer for the EBICS procedure shall comply with the requirements described in Annex 1a.
- A firewall is an application which supervises all incoming and outgoing messages and only allows known or authorised connections to pass through. EBICS customer systems may not be used without a firewall.
- A virus scanner must be installed and must be updated regularly with the newest virus definition files.
- The EBICS customer system must be configured in such a manner that the Subscriber has to log in before the system can be used. The Customer must log in as a normal User and not as an administrator who is authorised, for instance, to carry out program installations.
- The internal IT communication channels for unencrypted banking data or for unencrypted EBICS messages must be protected against interception and manipulation.
- If security-relevant updates are available for the operating system in use or for other security-relevant software programs which may have been installed, such updates shall be applied to the EBICS customer systems.

The Customer is exclusively responsible for the implementation of these requirements.

Annex 2: Not currently in use

Annex 3: Data format specification

The specification is published on the website http://www.ebics.de