Terms and Conditions for Remote Data Transmission

The following translation is provided for your convenience only. The original German text "Bedingungen für Datenfernübertragung" is binding in all respects. In the event of any divergence between the English and German texts, constructions, meanings or interpretations, those of the German original shall govern exclusively.

1 Scope of services

(1) The Bank shall be at the disposal of customers (account holders) who are not consumers for remote data transmission by electronic means, referred to hereinafter as "remote data transmission" or "RDT". Remote data transmission comprises the presentation and retrieval of files (particularly transmitting orders and calling up information).

(2) The Bank shall inform customers of the types of services they may use within the scope of remote data transmission. The use of remote data transmission shall be subject to the transaction limits agreed with the Bank.

(3) Remote data transmission shall be possible via the EBICS connection (Annexes 1a – 1c).

(4) The structure of the data sets and files used for transmitting orders and calling up information is described in the Data Format Specification (Annex 3).

2 Users and subscribers, identification and security media

(1) Orders can be placed via the EBICS connection only by the customer or the customer's authorised representatives. The customer and the authorised representatives are referred to collectively hereinafter as "users" (Nutzer). In order to authorise order data sent by remote data transmission by means of an electronic signature, each user shall require individual identification media activated by the Bank. The identification media requirements are specified in Annex 1a. If agreed with the Bank, order data sent by remote data transmission may be authorised by means of a signed note accompanying it (Begleitzettel)/batch order (Sammelauftrag).

(2) In addition to authorised representatives, the customer can name "technical subscribers" (technische Teilnehmer) for the exchange of data via the EBICS connection. Such technical subscribers shall only be authorised to exchange data. Users and technical subscribers are referred to collectively hereinafter as "subscribers" (Teilnehmer). To protect the exchange of data, each subscriber shall require individual security media activated by the Bank. The security media requirements are set out in Annex 1a.

3 Procedural provisions

(1) The data transmission procedure agreed between the customer and the Bank shall be subject to the requirements set out in Annex 1a and in the technical interface documentation (Annex 1b) and the Data Format Specification (Annex 3).

(2) The customer shall be obligated to ensure that all subscribers comply with the RDT procedure and the specifications.

(3) Data field entries shall be governed by the data field entry and control guidelines for the format used in each case (Annex 3).

(4) The user must correctly state the unique identifier of the payee or payer in accordance with the relevant special terms and conditions. The payment service providers involved in handling the payment order shall be entitled to process it solely on the basis of the unique identifier. Incorrect details may result in the payment order being misrouted. Any loss or damage incurred as a result thereof shall be borne by the customer.

(5) Before 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 verification of identification must be made. This record must be kept by the customer for a minimum period of 30 calendar days from the date of execution (for credit transfers) or due date (direct debits) indicated in the file or, where several dates are indicated, from the latest such date. Unless otherwise agreed, it must be demonstrably kept in such a way that it can be made available to the Bank again at short notice on request.

(6) In addition, the customer must produce for each presentation and each retrieval of files an electronic protocol which complies with the provisions of Section 10 of the EBICS Connection Specification (Annex 1b). The customer must hold this protocol on file and make it available to the Bank on request.

(7) If the Bank provides the customer with data concerning payment transactions which have not yet been finally processed, this data shall merely constitute non-binding information. It shall be specifically marked as such in each case.

(8) The order data submitted by remote data transmission must, as agreed with the Bank, be authorised either by an electronic signature or by a signed note accompanying the data (Begleitzettel)/batch order (Sammelauftrag). This order data shall become legally effective as an order

a) when submitted with an electronic signature:
   - if all necessary user electronic signatures have been received by remote data transmission within the agreed period of time and
   - if the electronic signatures can be successfully verified with the agreed keys

oder

b) when submitted with an accompanying note (Begleitzettel)/batch order (Sammelauftrag):
   - if the accompanying note/batch order has been received by the Bank within the agreed period of time and
   - if the accompanying note/batch order has been signed in accordance with the account mandate.

4 Obligation to exercise due diligence when handling the identification media for authorising orders

(1) Depending on the transmission procedure agreed with the Bank, the customer shall be obligated to ensure that all users comply with the obligations resulting from these terms and conditions and the identification procedures set out in Annex 1a.

(2) The user may place orders using an identification medium activated by the Bank. The customer shall ensure that each user takes care that no other person obtains possession of their identification medium or gains knowledge of the password protecting it. This is because any other person who is in possession of the medium or a duplicate thereof and knows the corresponding password can misuse the agreed services. In order to protect the identification medium and the password, the following must be observed in particular:

- The identification medium must be protected against unauthorised access and kept in a safe place.
- The password protecting the identification medium must not be noted on the identification medium or kept together with it as a copy or stored unsecured electronically.
- The identification medium must not be duplicated.
- When entering the password, care must be taken to ensure that no other persons can view it.

5 Obligation to exercise due diligence when handling the security media for data exchange

When using the EBICS connection, the customer shall be obligated to ensure that all subscribers comply with the security procedures set out in Annex 1a.
The subscriber shall secure the data exchange using the security media activated by the Bank. The customer shall be obligated to ensure that each subscriber takes care that no other person obtains possession of, or can use, their security medium. Particularly if it is filed 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 other person who has 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 they use for remote data transmission are adequately protected. The EBICS security requirements are set out in Annex 1c.

7 Blocking of the identification and security media

(1) If the identification or security media are lost, become known to other persons or misuse of these media is suspected, the subscriber must immediately block their RDT access or arrange for the Bank to block it. Further details are contained in Annex 1a. The subscriber may also send the Bank a blocking request at any time via the separately notified contact data.

(2) Outside the RDT procedure, the customer can arrange for the use of a subscriber's identification and security media or the entire RDT access to be blocked via the blocking facility specified by the Bank.

(3) The Bank shall block the entire RDT access if misuse is suspected. It shall notify the customer thereof outside the RDT procedure. Such blocking cannot be lifted via remote data transmission.

8 Handling of incoming order data by the Bank

(1) The order data delivered to the Bank by remote data transmission shall be processed in the regular course of business.

(2) The Bank shall verify by means of the signatures generated by the subscribers with the security media whether the sender is authorised to exchange data. If this verification reveals any discrepancies, the Bank shall not process the order data concerned and shall notify the customer thereof without delay.

(3) The Bank shall verify the identification of the user(s) and authorisation of the order data delivered by remote data transmission on the basis of either the electronic signatures generated by the users with the identification media or the accompanying note (Begleitzettel)/batch order (Sammelauftrag) and whether the order data sets comply with the provisions of Annex 3. If this verification reveals any discrepancies, the Bank shall not process the order data in question and shall notify the customer thereof without delay. The Bank may delete any order data that has not been fully authorised after expiry of the time limit separately notified by the Bank.

(4) If the verification of the files or data sets performed by the Bank in accordance with Annex 3 reveals errors, the Bank shall indicate the files or data sets containing errors in appropriate form and notify the user thereof without delay. The Bank may exclude the files or data sets containing errors from further processing if proper execution of the order cannot be ensured.

(5) The Bank shall be obligated to document the procedures (see Annex 1a) and the forwarding of orders for processing in the customer protocol. The customer shall be obligated to call up the protocol promptly and ascertain the status of order processing. In the event of any discrepancies, the customer shall contact the Bank.

9 Recall/revocation

(1) The customer may recall a file before the order data has been authorised. Individual order data can only be changed by recalling the entire file and placing the order again. The Bank can only accept a recall if the recall reaches it early enough to be taken into account in the regular course of business.

(2) The extent to which an order can be revoked shall be governed by the relevant special terms and conditions (e.g. Terms and Conditions for Credit Transfers). Orders can be revoked outside the RDT procedure or, where agreed with the customer, in accordance with the provisions of Section 11 of Annex 3. For this purpose, the customer must provide the Bank with the individual details of the original orders.

10 Execution of orders

(1) The Bank shall execute orders if all the following conditions for execution have been fulfilled:

- The order data delivered by remote data transmission has been authorised in accordance with Section 3 (8).
- The specified data format has been complied with.
- The transaction limit has not been exceeded.
- The requirements for execution set out in the special terms and conditions governing the respective order type (e.g. a sufficient credit balance in an account under the Terms and Conditions for Credit Transfers) have been met.

(2) If the conditions for execution under paragraph 1 are not fulfilled, the Bank shall not execute the order and shall notify the customer of the non-execution without delay through the agreed communication channel. Where possible, the Bank shall explain why the order was not executed and indicate how any errors that caused the nonexecution can be rectified.

11 Liability

11.1 Liability of the Bank for unauthorised RDT transactions and non-execution, incorrect execution or delayed execution of RDT transactions

The liability of the Bank for unauthorised RDT transactions and non-execution, incorrect execution or delayed execution of RDT transactions shall be governed by the special terms and conditions agreed for the respective order type (e.g. Terms and Conditions for Credit Transfers).

11.2 Liability of the customer for misuse of the identification or security media

11.2.1 Liability of the customer for unauthorised payment transactions before a request to block access

(1) If unauthorised payment transactions conducted before a request to block access are due to the misuse of identification or security media, the customer shall be liable vis-à-vis the Bank for the loss or damage incurred by the Bank if the subscriber has negligently or wilfully breached their obligations to exercise due diligence. Section 675y of the German Civil Code (Bürgerliches Gesetzbuch [BGB]) shall not apply.

(2) The customer shall not be obligated to provide compensation for loss or damage under paragraph 1 if the subscriber was unable to issue the request to block access under Section 7 (1) because the Bank failed to ensure that it had the means to receive such requests to block access and the loss or damage would in this way have been avoided.

(3) Liability for loss or damage caused within the period of time for which the transaction limit applies shall be limited in each case to the agreed transaction limit.

(4) Paragraphs 2 and 3 shall not apply if the subscriber acted with fraudulent intent.

11.2.2 Liability of the customer for other unauthorised transactions before a request to block access
If unauthorised transactions other than payment transactions conducted before a request to block access are due to the use of a lost or stolen identification or security medium or to any other misuse of the identification or security medium and if the Bank has incurred loss or damage as a result thereof, the customer and the Bank shall be liable in accordance with the statutory principles of contributory negligence.

11.2.3 Liability of the Bank after receipt of a request to block access
As soon as the Bank has received a request to block access from a subscriber, it shall bear any loss or damage incurred thereafter due to unauthorised RDT transactions. This shall not apply if a subscriber has acted with fraudulent intent.

11.3 Preclusion of liability
Claims for compensation shall be precluded if the circumstances substantiating a claim are based on an exceptional and unforeseeable event on which the party referring to this event has no influence and whose consequences could not have been avoided by it even by exercising the required due diligence.

12 Final provisions
The Annexes referred to in these terms and conditions shall form part of the agreement concluded with the customer.

Annex 1a	EBICS Connection
Annex 1b	EBICS Connection Specification
Annex 1c	Security Requirements for the EBICS Customer System
Annex 2	currently blank
Annex 3	Data Format Specification

Terms and Conditions for Remote Data Transmission

Annex 1a

EBICS Connection

1 Identification and security procedures
The customer (account holder) shall indicate the RDT subscribers and their authorisations to the Bank.
The following identification and security procedures shall be used for the EBICS connection:

- Electronic signatures
- Authentication signature
- Encryption

The subscriber shall possess an individual pair of keys, consisting of a private key and a public key, for each identification and security proce dure. The public subscriber keys must be disclosed to the Bank in accordance with the procedure set out in Section 2. The public bank keys must be protected against unauthorised alteration in accordance with the procedure set out in Section 2. The subscriber's key pairs may also be used for communication with other banks.

1.1 Electronic signatures

1.1.1 Electronic signatures of subscribers
The following signature classes shall be defined for the electronic signatures (ESs) of subscribers::

- Single signature (Type "E")
- First signature (Type "A")
- Second signature (Type "B")
- Transport signature (Type "T")

Type "E", "A" or "B" ESs are referred to as "banking ESs". Banking ESs are used to authorise orders. Orders may require several banking ESs which must be provided by different users (account holders and their authorised representatives). For each order type supported, aminimum number of required banking ESs shall be agreed between the Bank and the customer.
Type "T" ESs, which are called "transport signatures", are not used for banking authorisation of orders, but solely for transmitting orders to the bank system. "Technical subscribers" (see Section 2.2) may only be assigned a type "T" ES.
Type "T" ESs, which are called "transport signatures", are not used for banking authorisation of orders, but solely for transmitting orders to the bank system. "Technical subscribers" (see Section 2.2) may only be assigned a type "T" ES..

1.1.2 Authentication signature
In contrast to the ES, which is used to sign order data, the authentication signature is configured via the individual EBICS message including the control and log-in data and the ES contained therein. With the exception of a few system-determined order types defined in the EBICS Connection Specification, the authentication signature is provided by both the customer system and the bank system in every transaction step. The customer must ensure the use of software which, in accordance with the EBICS Connection Specification (see Annex 1b), verifies the authentication signature of each EBICS message transmitted by the Bank, taking into account the current validity and authenticity of the Bank's stored public keys.

1.2 Encryption
In order to ensure the secrecy of the banking data at application level, the order data must be encrypted in accordance with the EBICS Connection Specification (see Annex 1b) by the customer, taking into account the current validity and authenticity of the Bank's stored public keys.
In addition, transport encryption is required on the external transmission routes between the customer and bank systems. The customer must ensure the use of software which, in accordance with the requirements of the EBICS Connection Specification (see Annex 1b), verifies the current validity and authenticity of the server certificates used by the Bank for this purpose.

2 Initialisation of the EBICS connection

2.1 Establishing the communication link
Communication is established using a URL (Uniform Resource Locator). Alternatively, an IP address for the respective Bank may be used.

The URL or IP address shall be disclosed to the customer on conclusion of the agreement with the Bank.
To initialise the EBICS connection, the Bank shall provide the following data to the subscribers named by the customer:

- URL or IP address of the Bank
- Name of the Bank
- Host ID
- Permitted version(s) of the EBICS protocol and security procedures
- Partner ID (customer ID)
- User ID
- System ID (for technical subscribers)
- Further specific details of customer and subscriber authorisations.

For the subscribers assigned to the customer, the Bank shall issue a user ID which clearly identifies the subscriber. If one or more technical subscribers are assigned to the customer (multi-user system), the Bank shall issue a system ID in addition to the user ID. If no technical subscriber is specified, the system ID and user ID are identical.

2.2 Initialisation of subscriber keys

The key pairs used by the subscriber for the banking ESs, encryption of the order data and the authentication signature shall, in addition to the general conditions set out in Section 1, comply with the following requirements::

1. The key pairs are assigned exclusively and unambiguously to the subscriber.
2. If the subscriber generates their keys independently, the private keys must be generated by means which the subscriber can keep under their sole control.
3. If the keys are made available by a third party, it must be ensured that the subscriber obtains sole possession of the private keys.
4. As regards the private keys used for identification, each user shall define a password for each key which protects access to the respective private key.
5. As regards 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.

   Initialisation of the subscriber by the Bank requires transmission of the subscriber's public keys to the bank system. For this purpose, the subscriber shall transmit their public keys to the Bank via two independent communication channels:

   - via EBICS by means of the system-determined order types provided for this purpose.
   - via an initialisation letter signed by the account holder or an authorised representative.

   For initialisation of the subscriber, the Bank 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 representative.

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

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

2.3 Initialisation of bank keys

The subscriber shall collect the Bank's public key using a systemdetermined order type specifically designated for this purpose.
The hash value of the public bank key shall additionally be made available by the Bank via a second communication channel agreed separately with the customer.

Before using EBICS for the first time, the subscriber shall verify the authenticity of the public bank keys sent to them by remote data trans mission by comparing their hash values with the hash values notified by the Bank via the separately agreed communication channel.

The customer must ensure use of software which verifies the validity of the server certificates used in transport encryption by means of the certification path notified separately by the Bank.

3 Special due diligence requirements where identification and security media are generated by the customer

Where the customer generates their identification and security media in accordance with the EBICS Connection Specification themself and initialises these with their Bank, they shall ensure the following:

- Confidentiality and integrity of the identification medium are maintained in all phases of authentication, including display, transmission and storage.
- Private subscriber keys on identification and security media are not stored in clear text.
- The identification medium is blocked as soon as the wrong password has been entered five times in succession.
- Private and public subscriber keys are generated in a secure environment.
- Identification and security media are clearly and uniquely assigned to the subscriber and used.

4 Placing orders with the Bank

The user shall verify the accuracy of the order data and ensure that only this data is signed electronically. When initialising communication, the Bank shall first conduct subscriber-related authorisation verifications, such as order type authorisation or, if applicable, agreed limit verifications. The results of further banking verifications such as limit verifications or account authorisation verifications shall be notified to the customer in the customer protocol at a later date. An exception shall be the online verification of order data by the Bank agreed with the customer on an optional basis.

Order data transmitted to the Bank system may be authorised a follows:

1. All necessary banking ESs are transmitted together with the order data.

2. If a Distributed Electronic Signature (Verteilte Elektronische Unterschrift [VEU]) has been agreed with the customer for the respective order type and the ESs transmitted are insufficient for banking authorisation, the order is stored in the bank system until all necessary ESs have been submitted.

3. If the customer and the Bank agree that order data delivered by RDT may be authorised by means of a separately transmitted accompanying note (Begleitzettel)/batch order (Sammelauftrag), a transport signature (type "T") must be provided for the technical protection of the order data instead of the user's banking ES. To this end, the file must bear a special tag indicating that there are no further ESs for this order other than the transport signature (type "T"). The order is authorised once the Bank has successfully verified the user's signature on the accompanying note (Begleitzettel)/batch order (Sammelauftrag)

4.1 Issuing orders by means of the Distributed Electronic Signature (VEU)

The manner in which the Distributed Electronic Signature will be used by the customer must be agreed with the Bank.
The Distributed Electronic Signature shall be used if orders are to be authorised independently of the transport of the order data and, if applicable, by several subscribers.
Until all banking ESs necessary for authorisation are available, the order can be deleted by an authorised user. If the order has been fully authorised, it can only be recalled/revoked in accordance with Section 9 of the Terms and Conditions for Remote Data Transmission.
The Bank may delete orders that have not been fully authorised after expiry of the time limit notified separately by the Bank.

4.2 Verification of identification by the Bank

Order data delivered by remote data transmission shall be executed as an order by the Bank only after the necessary banking ESs or the signed accompanying note (Begleitzettel)/batch order (Sammelauftrag) have been received and positively verified.

4.3 Customer protocols

The Bank shall document the following 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 where these concern signature verification and the display of order data.

The subscriber shall consult the result of the verifications carried out by the Bank by promptly calling up the customer protocol.
The subscriber shall file this protocol, the contents of which shall comply with the provisions of Section 10 of Annex 1b, in its records and make it available to the Bank on request.

5 Change of subscriber keys with automatic activation

If the identification and security media used by the subscriber are valid for a limited period of time, the subscriber must transmit the new public subscriber keys to the Bank promptly before the expiry date. After the expiry date of the old keys has passed, a new initialisation must be performed.
If the subscriber generates their keys personally, they must renew the subscriber keys using the system–determined order types provided for this purpose and transmit them promptly before expiry of the old keys.
To automatically activate new keys without renewed subscriber initialisation, the following order types shall be used::

- 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 keys (HCS).

The order types PUB and HCA or HCS must be provided with a valid user banking ES for this purpose. After the keys have been successfully changed, only the new keys may be used.
If the electronic signature could not be positively verified, the procedure specified in Section 8 (3) of the Terms and Conditions for Remote Data Transmission shall apply.
The key may be changed only after all orders have been fully processed. Otherwise, any orders not yet executed must be placed again using the new key.

6 Blocking of subscriber keys

If misuse of the subscriber keys is suspected, the subscriber shall be obligated to block their access authorisation for all bank systems using the compromised key(s).
If the subscriber is in possession of valid identification and security media, they can block their access authorisation via EBICS. By sending a message with an "SPR" order type, access will be blocked for the subscriber whose user ID was used to send the message. After blocking, no further orders can be placed by this subscriber via EBICS until the re–initialisation referred to in Section 2 has been carried.
If the subscriber is no longer in possession of valid identification and security media, they can request blocking of the identification and security media outside the RDT procedure via the blocking facility notified separately by the Bank.
The customer may request blocking of a subscriber's identification and security media or the entire remote data transmission access outside the RDT procedure via the blocking facility notified by the.

Annex 1b

EBICS Connection Specification

The specification is available at www.ebics.de.

Annex 1c

Security Requirements for the EBICS Customer System

In addition to the security measures set out in Annex 1a (6), the customer must comply with the following requirements:

- The software used by the customer for the EBICS procedure must meet the requirements set out in Annex 1a.
- EBICS customer systems may not be used without a firewall. A firewall is an application which monitors all incoming and outgoing messages and allows only known or authorised connections.
- A virus scanner must be installed and regularly updated with the latest virus definition files.
- The EBICS customer system should be configured in such a way that subscribers must log in before using it. They should log in as a normal user and not as an administrator who is authorised, for example, to carry out programme installations.

- The internal IT communication channels for unencrypted banking data or for unencrypted EBICS messages must be protected against interception and manipulation.
- If security-related updates are available for the operating system in use and for other security-related software programmes that have been installed, they should be used to update the EBICS customer systems.

The customer shall be exclusively responsible for compliance with these requirements.

Annex 2

currently blank.

Annex 3

Data Format Specification
The specification is available at www.ebics.de.