Conditions for remote data transmission

1 Scope of services

(1) The Bank is available to its customer (account holder), who is not a consumer, for remote data transmission by electronic means – referred to below as »remote data transmission« or »RDT«. Remote data transmission consists of submission and retrieval of data (in particular transmitting orders and calling-up information).

(2) The Bank informs the customer of the types of service available via remote data transmission. The limitations on sums (disposal limits) agreed with the Bank apply to the use of remote data transmission.

(3) Remote data transmission is possible by an EBICS connection (Appendices 1a to 1c).

(4) The structure of the data sets and files used for transmitting orders and for calling-up information is described in the specification of data formats (Appendix 3).

2 Users, participants, legitimisation and security media

(1) Orders can be issued via an EBICS connection only by the customer or its authorised account users. Customers and authorised account users are referred to below jointly as »users«. In order to authorise order data transmitted by remote data transmission using electronic signatures, each user requires individual legitimisation media, which must first be activated by the Bank. The requirements on the legitimisation media are defined in Appendix 1a. If agreed with the Bank, order data transmitted via RDT can be authorised with signed vouchers/collective orders.

(2) In addition to the authorised users, the customer can nominate »technical participants« who are only authorised to conduct data exchange via the EBICS connection. Users and technical participants are referred to jointly below as »participants«. Each participant requires individual security media to be activated by the Bank in order to ensure the security of exchanges of data. The requirements on the security media are described in Appendix 1a.

3 Provisions on the procedures

(1) The requirements described in Appendix 1a as well as those in the documentation of the technical interface (Appendix 1b) and the specification of data formats (Appendix 3) apply to the transmission procedure agreed between the customer and Bank.

(2) The customer is obliged to ensure that all participants observe the remote data transmission procedures and the specifications.

(3) The assignment of the data fields is governed by the assignment and control guidelines of the format used (Appendix 3).

(4) The user must accurately state the customer identification of the payee and/or payer in accordance with the relevant special conditions. The payment service providers involved in processing the payment order are entitled to do so solely on the basis of the customer identification. Erroneous details can result in a false routing of the payment transaction order. Losses and disadvantages incurred as a result are borne by the customer.

(5) Before data sets are transmitted to the Bank, a record must be compiled of the files to be transmitted, with their complete content and of the data transmitted to verify legitimization. Such records must be retained by the customer for a period of 30 calendar days from the date of execution specified in the file (for transfers) or due date (direct debits) or, in the case of several deadlines, the latest date. The form of these records must be such that the file can be submitted again at short notice at the request of the Bank, unless something is arranged to the contrary.

(6) Furthermore, the customer must compile a protocol by machine for each data submission and retrieval. The content of this must correspond to the provisions of Chapter 10 of the specification for an EBICS connection (Appendix 1b). These protocols must be filed and submitted to the Bank upon request.

(7) Insofar as the Bank provides the customer with data concerning payment processes, which are still to be conclusively processed, such solely represent non-binding information. The respective data are distinctly designated.

(8) The order data transmitted by RDT are to be authorised either by electronic signature or signed voucher/collective order as agreed with the Bank. The order data constitutes a valid order:

a) by submission with electronic signature, if
- all necessary electronic signatures of the user have been received via remote data transmission within the period agreed and
- the electronic signatures can be positively verified with the agreed keys or

b) by submission with voucher/collective order, if
- the voucher/collective order was received by the Bank within the period agreed and
- the voucher/collective order of the control authorization was correctly signed.

4 Obligations for conduct and care in handling legitimisation media for issuing orders

(1) The customer is obliged to ensure that all users observe the obligations in these conditions and the legitimisation process described in Appendix 1a, depending on the transmission process agreed with the Bank.

(2) The user can issue orders with the help of one of the legitimisation media activated by the Bank. The customer shall ensure that each user sees to it that nobody else obtains possession of their legitimisation medium, nor learns the password serving its protection. This is because any person who obtains possession of the medium or a duplicate of the same can misuse the agreed services in connection with the associated password. Compliance, in particular, with the following instructions is necessary to maintain

BeGo 2019-09
Form SB-29 EN

the secrecy of the legitimisation medium and password:

- The data legitimation medium must be protected against unauthorised access and stored securely;
- The password serving to protect the legitimisation medium may not be recorded on the legitimation medium or kept as a copy together with it or stored unsecured electronically;
- The password is only to be entered in a manner that assures that it may not be detected by anyone else.

5 Obligations for conduct and care in handling security media for data exchange

Within the framework of the EBICS connection, the customer is obliged to ensure that all participants observe the security procedures described in Appendix 1a. The participant secures the exchange of data with the aid of the security media activated by the Bank. The customer is obliged to ensure that each participant sees to it that nobody else obtains possession of their security medium or can use this. Particularly when filing on a technical system, the participant's security medium must be stored in a technical environment protected from unauthorised access. This is because anybody who has access to the security medium or a duplicate of the same can misuse the data exchange process.

6 Security of the customer system

The customer must arrange for adequate protection of the systems it deploys for remote data transmission. The security requirements applicable to the EBICS process are described in Appendix 1c.

7 Blocking legitimisation and security media

(1) If the legitimisation or security media are lost, become known to other persons or if there is a suspicion that they are being misused, the participant must block his RDT access with the Bank or arrange for it to be blocked immediately. More detailed regulations are given in Appendix 1a. The participant can issue a blocking notice to the Bank at any time, also by means of separately provided contact data.

(2) The customer can arrange for a participant's legitimisation and security media or the complete RDT access to be blocked outside the RDT process by means of the blocking facility announced by the Bank.

(3) The Bank will block the complete RDT access if there is suspicion that the RDT access is being misused. The Bank will inform the customer outside the RDT process. This block cannot be rescinded by means of RDT.

8 Handling of incoming orders by the Bank

(1) The orders issued to the Bank by RDT are processed within the framework of regular working procedures.

(2) The Bank reviews the signatures compiled by the participants by means of the security media to check whether the sender is authorised to exchange data. If irregularities are detected by review, the Bank will not process the order in question, but will inform the customer of this without delay.

(3) The Bank checks the legitimisation of the user or users on the basis of the electronic signatures compiled by the users by means of the legitimisation media or the transmitted voucher/collective order, and ensures that the order data sets comply with the provisions in Appendix 3. If irregularities are detected by review, the Bank will not process the orders in question, but will inform the customer of this without delay. The Bank is entitled to delete orders not fully authorised after expiration of the time limit separately announced by the Bank.

(4) If irregularities are detected by the checks on the files or data sets performed by the Bank in accordance with Appendix 3, the Bank will substantiate the incorrect files or data sets in a suitable form and notify the user of this without delay. The Bank is entitled to remove the incorrect files or data sets from further processing, if proper execution of the order cannot be guaranteed.

(5) The Bank is obliged to document the procedures (see Appendix 1a) and the forwarding of orders for processing in the customer protocol. The customer is likewise obliged to retrieve the customer protocol timeously and inform himself as to the status of order processing. He is to contact the Bank in the event of inconsistencies.

9 Recall

(1) A file cannot be recalled once the Bank has started to process it. Changes to individual order data are only possible by recalling the entire file and issuing the order new. However, the Bank can only comply with a recall if it is received in time sufficient to process within the framework of regular working procedures.

(2) The recall of an order is governed by the respective special conditions applicable (e.g. Conditions for credit transfers). Orders can be recalled outside the RDT process or, if agreed with the customer, in accordance with the provisions of Chapter 11 of Appendix 3. The customer is required to inform the Bank of the details of the original order for a recall to be executed.

10 Execution of orders

(1) The Bank will execute the orders if all of the following conditions of execution are satisfied:

- the order data delivered by RDT have been authorised pursuant to No. 3 para. 8;
- the order complies with the stipulated data format;
- the disposal limit has not been exceeded;

- the requirements for execution in accordance with the respectively applicable special conditions (e.g. sufficient funds on account pursuant to the Conditions for credit transfers) are satisfied.

(2) If the execution conditions pursuant to para. 1 are not satisfied the Bank will not execute the order and will notify the customer without delay that such order has not been executed by the means agreed. If possible the Bank will inform the customer of the reasons and error that caused the order not to be executed and of the means available to remedy such errors.

11 Liability

11.1 Liability of the Bank for an unauthorised RDT order and an RDT order unexecuted or defectively executed or executed with delay.

The Bank's liability for an unauthorised RDT order or an RDT order unexecuted or defectively executed or executed with delay is governed by the special conditions agreed for the respective type of order (e.g. Conditions for credit transfers).

11.2 Customer liability for misuse of legitimisation and security media

11.2.1 Customer liability for unauthorised payment transactions prior to blocking notice

(1) If an unauthorised payment transaction due to misuse of legitimisation or security media occurs prior to blocking notice, then the customer is liable to the Bank for damages, if the participant negligently or intentionally violated his/her duties of conduct and due diligence. Section 675v of the German Civil Code (»Bürgerliches Gesetzbuch«, BGB) does not apply.

(2) The customer is not obliged to compensate the damage according to paragraph 1 if the participant was unable to submit the blocking notice in accordance with No. 7 (1) due to failure of the Bank to enable receipt of the blocking notice and if the damage could have thereby been avoided.

(3) The liability for damage caused during the period for which the disposal limit applies, is restricted respectively to the disposal limit agreed.

(4) Paragraphs 2 and 3 shall not apply if the participant has acted fraudulently.

11.2.2 Customer liability for other unauthorised transactions prior to blocking notice

If the unauthorised transactions, not pertaining to payments, are caused by use of a lost or stolen legitimisation or security medium or other misuse of the legitimisation or security medium prior to blocking notice, and the Bank incurs damage thereby, the customer and the Bank bear liability in accordance with the legal principles of contributory negligence.

11.2.3 Bank liability after the blocking notice

As soon as the Bank has received the blocking notice from a participant, it assumes liability for all damage incurred through subsequent unauthorised RDT orders. This does not apply where the participant has acted with fraudulent intent.

11.3 Indemnification

Liability claims are precluded where the circumstances giving rise a claim are due to events that are unusual and unpredictable, and where the party referring to this event has no influence and the consequences of which could not have been prevented despite all due diligence.

12 Concluding provisions

The Appendices mentioned in these conditions constitute components of the agreement concluded with the customer.

Appendix 1a: EBICS connection

Appendix 1b: Specification of EBICS connection

Appendix 1c: Security requirements of the EBICS customer system

Appendix 2: not filled at present

Appendix 3: Specification of data formats

Appendix 1a: EBICS connection

1 Legitimisation and security procedures

The customer (account holder) names the participants and their rights within the framework of remote data transmissions to the Bank. The following legitimisation and security procedures are deployed for an EBICS connection:

- electronic signatures
- authentication signature
- encryption.

The participant has an individual pair of keys for each transaction and security procedure at his disposal, consisting of a private and a public key. The Bank is to be notified of the public participant keys in accordance with the procedure described in No. 2. The public Bank keys must be protected from unauthorised change in accordance with the procedure described in No. 2. The participant's pair of keys can also be deployed for communication with other Banks.

1.1 Electronic signatures

1.1.1 Electronic signatures of participants

The following signature classes are defined for the electronic signatures (ES) of participants:

- individual signature (type »E«)
- first signature (type »A«)
- second signature (type »B«)
- transport signature (type »T«).

ES of type »E«, »A« or »B« are referred to as Bank-related ES. Bank-related ES serve to authorise orders. Orders can require several Bank-related ES, which must be provided by different users (account holder and its authorised users). The minimum number if Bank-related ES required is agreed between the Bank and customer for each type of order supported.

ES of type »T«, which are designated as transport signatures, are not used for a Bank-related release of orders, but rather solely for transmitting these to the Bank systems. »Technical participants« (see No. 2.2) can only be assigned an ES of type »T«.

The program used by the customer enables various messages to be compiled (e.g. orders for domestic and foreign payment transactions, although also for initialisation, calling-up protocols and collecting account and turnover information, etc.). The Bank informs the customer of the type of messages which can be used and which ES type is necessary for this purpose.

1.1.2 Authentication signature

In contrast to ES, which sign the order data, the authentication signature is composed of the individual message, including control and registration data and the ES contained therein. With the exception of a few system-related types of orders defined in the EBICS specification, the authentication signature is provided for each transaction stage both by the customer and by the Bank system. The customer must ensure that a software application is deployed which verifies the authentication signature of each EBICS message transmitted by the Bank with respect to currency and authenticity of the Bank's public key stored in accordance with the stipulations of the EBICS specification (see Appendix 1b).

1.2 Encryption

In order to guarantee the secrecy of the Bank-related data at application level, the customer must encrypt the order data in consideration of the currency and authenticity of the Bank's public key stored in accordance with the stipulations of the EBICS specification (see Appendix 1b).

Moreover a transport encryption is additionally required on the external transmission routes between the customer and Bank system. The customer must ensure that a software application is deployed that checks the currency and authenticity of the Bank's server certificates used for this purpose in accordance with the stipulations of the EBICS specification (see Appendix 1b).

2 Initialisation of the EBICS connection

2.1 Establishing the communication connection

The participants nominated by the customer are to provide the following data by the Bank in order to establish an EBICS connection:

- URL or IB address of the Bank
- Designation of the Bank
- Host-ID
- Admissible version(s) of the EBICS protocol and security procedures
- Partner-ID (customer ID)
- User ID
- System ID (for technical participants)
- Other specific details concerning customer and participant rights

The Bank issues a user ID for each of the participants assigned to the customer which uniquely identifies the participant. If one or more technical participants are assigned to the customer (multiuser system), the Bank issues a system ID in addition to the user ID. Insofar as a technical participant has not been designated, the system ID and user ID are identical.

2.2 Initialisation of the participant keys

The pair of keys used by the participant for the Bank-related ES, encryption of order data and the authentication signature must satisfy the following requirements in addition to the general conditions described in No. 1:

(1) The pair of keys is assigned exclusively and uniquely to the participant.

(2) If the participant generates his keys himself, the private keys must be generated by means which the participant can keep under his exclusive control.
(3) If the keys are provided to a third party, it is necessary to ensure that the participant obtains sole possession of the private key.
(4) In order to deploy the private keys used for legitimisation, each user defines a password for each key which secures access to the respective private key.
(5) In order to deploy the private keys used to secure data exchanges, each participant defines a password which secures access to the respective private key. No password is necessary if the participant's security medium is stored in a technical environment which is protected from unauthorised access.
The participant's public key must be transmitted to the Bank system to enable the Bank to initialise the participant. For this purpose the participant transmits his public key to the Bank via two communication paths independent of each other:

- Via the EBICS connection by means of the order types determined by the system and foreseen for this purpose;
- By means of an initialisation letter signed by the account holder or a authorised account user.

When activating a participant, the Bank checks the authenticity of the public participant key transmitted via EBICS on the basis of the initialisation letters signed by the account holder or an authorised user. The initialisation letter contains the following data on each public participant key:

- Reference of the public participant key
- Electronic signature
- Authentication signature
- Encryption
- The respectively supported version per pair of keys
- Length of the exponent
- Exponent of the public key in hexadecimal form
- Length of the modulus
- Modulus of the public key in hexadecimal form
- Hash value of the public key in hexadecimal form

The Bank checks the signature of the account holder or of the authorised account user on the initialisation letter and verifies that the hash values of the participant's public key transmitted via the EBICS connection coincide with that submitted in writing. If the result of the check is positive, the Bank activates the participant concerned for the types of order agreed.

2.3 Initialisation of the Bank-specific key

The participant collects the Bank's public key by means of a dedicated type of order determined by the system and foreseen for this purpose. The hash value of the public Bank key is provided additionally by the Bank via a second communication path agreed separately with the customer.
Before first-time use of EBICS, the participant should verify the authenticity of the public Bank key sent to it by remote data transmission. This is done by comparing its hash values with the hash values provided by the Bank via the separately agreed communication path.
The customer must ensure that a software application is deployed which checks the validity of the server certificates used with the framework of transport encryption on the basis of the certification path provided separately by the Bank.

3 Special duties of care in the generation of legitimation and security media by the customer

Insofar as the customer generates his own legitimation and security media in accordance with the requirements of the EBICS specification and initiates them at his bank, he must ensure the following:

- In all phases of authentication, including display, transmission and storage, confidentiality and integrity of the legitimation medium must be guaranteed.
- Private participant keys on the legitimation and security media may not be stored in plain text.
- The legitimation medium will be blocked after a maximum of five incorrect entries of the password.
- The private and public participant keys must be generated in a secure environment.
- The legitimation and security media are to be clearly assigned to and exclusively used by the participant.

4 Issuing orders to the Bank

The user checks the correctness of the order data and ensures that precisely these data are signed electronically. When establishing the communication, the Bank first verifies the participant-related rights, such as order type authorisation or any limit checks agreed. The Bank notifies the customer of the results of further reviews made by the Bank, such as limit checks or reviews of account authorisation, in the customer protocol at a later date.
Orders transmitted to the Bank system can be authorised as follows:
(1) All the necessary Bank-related ES are transmitted together with the order data;
(2) If the distributed electronic signature (DES) has been agreed with the customer for the respective type of order and the ES transmitted are insufficient for release by the Bank, the order is filed in the Bank system until all the necessary ES have been submitted.
(3) Insofar as the customer and Bank agree that orders can be authorised by means of accompanying notes/collective orders transmitted separately, the user's Bank-related ES should be replaced by a transport signature (type »T«) to ensure the technical security of the order data. To this end the file should be given a special marking which states that

there are no other ES for this order apart from the transport signature (type »T«). The order is released once the Bank has successfully verified the user's signature on the accompanying note/collective order.

4.1 Issuing orders by Distributed Electronic Signature (DES)

The manner in which the Distributed Electronic Signature is used by the customer must be agreed with the Bank.

The distributed electronic signature (DES) should be deployed if orders are to be authorised independent of the transport of the order data and, if applicable, also by several participants.

As long as not all of the Bank-related ES necessary for authorisation are available, the order can be deleted by the user entitled to do so. If the order has been fully authorised, it can only be recalled in accordance with Section 9 of the Conditions for Remote Data Transmission.

The Bank is entitled to delete orders not fully authorised after expiration of the time limit announced separately by the Bank.

4.2 Legitimacy check by the Bank

Incoming orders via RDT will not be executed by the Bank until the necessary Bank-related ES or the signed accompanying notes/collective orders have been received and positively verified.

4.3 Customer protocols

The Bank documents the following processes in customer protocols:

- Transmission of order data to the Bank system
- Transmission of information files from the Bank system to the customer system
- Result of each legitimacy check on the customer's orders sent to the Bank system
- Further processing of orders, insofar as this concerns signature verification and notification of order data

The participant is to inform himself on a timely basis of the results of Bank checks by retrieval of the customer protocol. This protocol, the content of which complies with the provisions of Chapter 10 of Appendix 1b, is to be retained by the participant and submitted to the Bank upon demand.

5 Changing participant keys with automatic activation

If the validity of the legitimisation and security media deployed by the participant is subject to limited duration, the participant must transmit in a timely manner the new public participant keys to the Bank prior to expiry. A new initialisation must be performed after the validity of the old keys has expired.

If the participant himself generates the keys he must renew the participant keys by the point in time agreed with the Bank and transmit these in a timely manner before the old keys expire, using the types of order determined by the system and foreseen for this purpose.

The following types of order are to be used to automatically activate new keys without a renewed participant initialisation:

- updating the public Bank-related key (PUB) and
- updating the public authentication key and the public encryption key (HCA).

or alternatively

- updating all three keys referred to above (HCS).

The order types PUB, HCA and HCS, respectively, need to be provided with a valid, Bank-related ES of the user for this purpose. After the change has been made, only the new keys should be used.

If the electronic signature cannot be successfully verified, the procedure described under No. 8 (3) of the »Conditions for remote data transmission« applies. The key may not be changed until all orders have been processed. Otherwise any orders not yet executed should be reissued with the new key.

6 Blocking participant keys

If there is suspicion that a participant key is being misused, the participant is obliged to have his access rights blocked to all Bank systems which use the compromised key(s).

If the participant has valid legitimisation and security media at his disposal, he can block his access rights via the EBICS connection. This is done by sending a message with the order type »SPR« which blocks the access for the participant under whose user ID the message was sent. After blocking, no more orders can be issued by this participant via the EBICS connection until the new initialisation described under No. 2 has been performed.

If the participant no longer has valid legitimisation and security media at his disposal, he can have his legitimisation and security media blocked outside the RDT process via the blocking facility provided separately by the Bank.

The customer can arrange to have a participant's legitimisation and security media or even the complete RDT access blocked outside the RDT process via the blocking facility provided by the Bank.

Apendix 1b: Specification of the EBICS connection

The technical specification of the EBICS connection is published at the website www.ebics.de.

Appendix 1c: Security Requirements for the EBICS customer system

In addition to the security measures described in Appendix 1a, No. 6, the customer must also observe the following requirements:

- The software deployed by the customer for the EBICS process must fulfil the requirements described in Appendix 1a.
- EBICS customer systems may not be deployed without a firewall. A firewall is an application which monitors all incoming and outgoing traffic and only allows recognised or authorised connections.
- An anti-virus scanner must be installed and regularly updated with the latest virus definition files.
- The EBICS customer system must be set-up in such a way that participants must log-on before use. They are to log-on as normal users and not as an administrator, e.g. someone who has the right to install programs.
- The internal IT communication paths for unencrypted, Bank-related data or for unencrypted EBICS messaged must be protected from interception and manipulation.
- If updates relevant to security are available for the operating system used or other software programs relevant to security which are installed, the EBICS customer systems are to be updated with these.

Implementation of the requirements is the sole responsibility of the customer.

Appendix 2:

not filled at present.

Appendix 3: Specification of data formats

The technical specification of the EBICS connection is published at the website www.ebics.de.