

TERMS AND CONDITIONS OF REMOTE DATA TRANSMISSION

I. Scope of services

1. The bank offers to its customers (account holders) data transmission by electronic means – hereinafter referred to as "remote data transmission (RDT)." Remote data transmission includes the placement of orders and the exchange of data (transmission of orders and retrieval of information).

2. The bank informs customers of the types of services they may use within the scope of remote data transmission. In case the bank intends to limit the amount of transactions that can be effected with remote data transmission, it will inform the customers thereof.

3. Remote data transmission is possible through two different procedures. The applicable transfer procedure shall be agreed between the customer and the bank.

4. The record and file format for the transmission of orders and retrieval of information is described in the Data Format Specification (Annex 3).

II. Users and subscribers, identity verification and security media

1. Orders may only be placed through the EBICS or FTAM connection by customers or their authorized account representatives. Customers and authorized account representatives shall be referred to collectively hereinafter as "users." For the placement of orders with the bank, each user requires individual identity verification media activated by the bank. The identity verification media requirements are defined in Annex 1a and 2a.

2. For the exchange of data over the EBICS connection, customers may, in addition to their authorized representatives, designate "technical subscribers" who are only authorized to conduct data exchanges. Users and technical subscribers shall be referred to collectively hereinafter as "subscribers." In order to ensure the secure exchange of data, each subscriber requires individual security media activated by the bank. The security media

requirements are described in Annex 1a.

3. For the exchange of data over the FTAM connection, each user requires a remote data transmission password issued by the bank. The data transmission password requirements are described in Annex 2a.

III. Procedural provisions

1. For the transfer procedure agreed between the customer and the bank the requirements set forth in Annex 1a "EBICS Connection" and Annex 2a "FTAM Connection" respectively, and the Technical Interface Documentation (Annex 1b "EBICS Specification," Annex 2b "FTAM Specification") and the Data Format Specification (Annex 3) shall apply respectively.

2. The customer shall ensure that all subscribers adhere to the procedure and specifications agreed with the bank.

3. Data field entries shall comply with the data entry and control instructions for the format used in each case. The data in the "reason for transfer" field shall relate exclusively to the relevant payment transaction in the data record. Left-justified at the start of the "reason for transfer" data field, data which the payee/payer intends to access electronically or which the remitter/payment recipient requires in the event that the payment is returned as undeliverable or unpaid shall be provided. In addition, users may not use the data field for the "reason for transfer" to specify a print image that they desire, unless the number of characters in this data field has been used in full in the data record or in any of the subsequent extensions with fields for entering the "reason for transfer." The "reason for transfer" data shall not replace the transmission of a separate message outside of the payment transaction (e.g. invoices, wage and payroll accounting). Advertising text may not be included in the reason for transfer data.

4. The user shall provide the appropriate bank identification code (bank sort code or BIC) of the payee's and paying agent's bank, respectively, and the account identification code (account number or IBAN) of the payee and the payer.

The banks involved in processing the

payment order shall be entitled to process the order exclusively through the use of bank and account identification codes. Incorrect data may lead to the payment order being misdirected. Any resulting damages or disadvantages shall be borne by the customer.

5. Prior to the transfer of data records to the bank, a record of the files to be transferred including their full content and the data provided for identity verification shall be produced. Unless otherwise agreed, this shall be retained by the customer for a minimum period of 14 calendar days and 30 calendar days from the implementation date for domestic and foreign payment orders, respectively, in such a format that the file may be provided to the bank again at short notice.

6. In addition, for each data transfer, the customer shall produce an electronic log, which corresponds to the provisions of section 10 of the Specification for the EBICS Connection (Annex 1b) and section 1.7 of the Specification for the FTAM Connection (Annex 2b) in terms of content, and to keep this in his/her records and, upon request, provide this to the bank.

7. Should the bank provide the customer with data about payment transactions that have not yet been fully processed, this data shall only represent non-binding information. The data shall be specially identified.

IV. Conduct and care obligations in handling the identity verification media for the placement of orders

1. Depending on the transfer procedure agreed with the bank, the customer shall be obliged to ensure that all users adhere to the identity verification procedure described in Annex 1a and/or Annex 2a.

2. By using the identity verification media activated by the bank, the user will be able to place orders. The customer shall ensure that each user takes care that no other person may have access of his/her identity verification medium or acquires knowledge of the password protecting this identity verification medium. Any other person who has access to the identity verification medium or a corresponding duplicate may, along with the relevant password, make improper use of the agreed services. In

particular, the following is to be taken into account with regard to keeping the identity verification media secret:

- The data verifying the user's identity shall not be stored outside the identity verification medium, e.g. on a computer hard drive;
- After completion of the remote data transmission, the identity verification medium is to be removed from the reader and stored securely;
- The password protecting the identity verification medium shall not be recorded in writing or stored electronically;
- When entering the password, it is to be ensured that no other person is able to view it.

V. Conduct and care obligations in handling security media for the exchange of data

1. With regard to the EBICS connection, the customer is obliged to ensure that all subscribers adhere to the security procedure described in Annex 1a.

By using the security media activated by the bank, the subscriber secures the exchange of data. The customer is obliged to ensure that all subscribers take care that no other person comes into possession of their security medium or is able to use it. In particular, in the event of storage on an IT system, the subscriber's security medium must be stored in a technical environment that is protected against unauthorized access. Any other person who has access to the security medium or a corresponding duplicate may conduct improper data exchanges.

2. With regard to the FTAM connection, the customer is obliged to ensure that all users adhere to the security procedure described in Annex 2a. The customer shall ensure that each user takes care that no other person acquires knowledge of his/her data transmission password since any other person who knows the data transmission password may exchange data with the bank.

VI. Suspension of the identity verification and security media

1. Should the identity verification or security media be lost, become known to other persons or suspicion of improper use arise, the subscriber shall immediately instruct the bank to suspend his/her remote data

transmission access. This is stipulated in greater detail in Annex 1a and Annex 2a.

2. If a subscriber has issued the bank with a suspension request, from the time this notification is received, the bank shall be liable for any damages arising as a result of its failure to take this into account.

3. Should three consecutive attempts be made to place an order with the bank using an incorrect identity verification medium or to conduct a data exchange using an incorrect security medium, the bank shall suspend the data transmission access of the subscriber in question. This suspension cannot be removed by means of remote data transmission. In order for this suspension to be lifted, the customer must contact his/her bank.

4. Outside of the data transmission procedure, the customer can have the use of the identity verification and security media of a subscriber or all data transmission access suspended through the suspension facility notified by the bank.

5. The bank shall suspend all remote data transmission access if suspicion of improper use of the remote data transmission access arises. The customer shall be informed of this outside of the remote data transmission procedure. This suspension cannot be lifted through remote data transmission.

VII. Processing of incoming orders by the bank

1. Orders placed with the bank through the remote data transmission procedure shall be processed as part of the normal workflow.

2. Should the bank be unable to perform a transfer order given to it by the customer as a paperless "SEPA transfer" in such format because the bank of the payee specified by the customer does not support this format and the bank does not reject the transfer, it shall carry out the transfer in a format supported by the payee's bank. With this change of format, the data elements mentioned in Annex 4 or parts thereof cannot be transmitted.

3. The bank shall verify whether the sender is entitled to conduct the data exchange by means of the signatures provided by the subscribers through the security media. Should the verification reveal any discrepancies, the bank shall not process the

order in question and immediately provide information in this regard to the customer.

4. The bank shall verify the identity of the user and/or the users by means of the signatures provided by the users through the identity verification media and the conformity of the order data records with the provisions according to Annex 3. Should the verification reveal any discrepancies, the bank will not process the orders in question and immediately provide information in this regard to the customer. The bank shall be entitled to cancel any orders that have not been fully authorized within the time limits separately specified by the bank.

5. Should any mistakes be revealed in the verification by the bank of the files or data records in accordance with Annex 3, the bank shall indicate which files or data records are incorrect in an appropriate form and immediately provide this information to the user. The bank shall be entitled to exclude the incorrect files or data records from further processing if the normal execution of the order cannot be ensured.

VIII. Recalls

1. Once the bank has started processing a file it may no longer be recalled. The bank may, however, only execute a request for a recall if notification is provided to it in such timely manner as necessary for its consideration during the normal workflow. Changes to the content of a file can only be made by recalling the file and placing a new order.

2. Recalling individual orders from files can only take place outside of the remote data transmission procedure, unless the bank provides for such a possibility within the process. To this end, the customer must provide the bank with the pertinent information on the original order relating to the bank identification code of the payee/paying agent's bank (bank sort code or BIC), the account identification code (account number or IBAN) and the name of the payee/payer, the text key/ text key extension, the amount, the bank sort code of the transferring bank/the first collection agency and the account number and name of the remitter/payment recipient, as well as the content of the data in the "reason for transfer" data field in the data record, in accordance with Annex 3.

IX. Security of the customer system

The customer shall ensure there is adequate protection for the system he/she has installed for remote data transmission. The security requirements that apply to the EBICS procedure are described in Annex 1c. Event of Format Change

X. Closing provisions

The annexes mentioned in these terms and conditions form part of the agreement concluded with the customer.

- Annex 1a:** EBICS Connection
- Annex 1b:** EBICS Connection Specification
- Annex 1c:** Security Requirements of the EBICS Customer System
- Annex 2a:** FTAM Connection
- Annex 2b:** FTAM Connection Specification
- Annex 3:** Data Format Specification
- Annex 4:** Transmission of Data in the

TERMS AND CONDITIONS OF REMOTE DATA TRANSMISSION

ANNEX 1a: EBICS Connection

1. Identity verification and security procedure

The customer (account holder) shall specify the subscribers and their rights in respect of remote data transmission to the bank.

The following identity verification and security procedures are incorporated in the EBICS connection:

- electronic signatures
- authentication signature
- encryption

For each identity verification and security procedure, the subscriber has an individual key pair, comprised of a private and a public key. The bank shall be notified of the public subscriber keys in accordance with the procedure described under number 2. The public bank keys must be protected against unauthorized changes in accordance with the procedure described under number 2. The subscriber's key pairs can also be used for communication with other banks.

1.1 Electronic signature

1.1.1 Electronic signature of the subscribers

For the electronic signature (ES) of the subscribers, the following signature classifications are defined:

- single signature (type "E")
- primary signature (type "A")
- secondary signature (type "B")
- transport signature (type "T")

Bank-specific ES refers to type "E," "A" or "B" electronic signatures. Bank-specific ES serve as authorization for orders. Orders may require several bank-specific ES that must be provided by different users (account holders and their authorized representatives). For each supported type of order between the bank and the customer, a minimum number of required bank-specific ES shall be agreed.

Type "T" ES, designated as transport signatures, are not used for bank-specific approval of orders, but merely for their transfer to the banking system. "Technical

subscribers" (see number 2.2) may only be assigned type "T" electronic signatures.

With the program used by the customer, various messages (e.g. orders for domestic and foreign payment transactions, as well as for initialization, log call-up and the collection of account and revenue information, etc.) can be generated. The bank shall inform the customer what type of messages can be used and what type of ES should be used for these.

1.2 Authentication signature

Unlike the ES, which signs the order data, the authentication signature is generated from the individual EBICS message including the control and registration data and the ES contained therein. With the exception of a few system-specific order types defined in the EBICS Specification, the authentication signature is provided at each transaction stage both by customers and the banking system. The customer must ensure that software is installed that verifies each EBICS message from the bank, taking into account the currentness and authenticity of the saved public bank key according to the provisions of the EBICS Specification (see Annex 1b).

1.3 Encryption

In order to ensure the secrecy of the bank-specific data on an application level, the customer's order data is to be encrypted, taking into account the currentness and authenticity of the stored public bank key, in accordance with the provisions in the EBICS Specification (see Annex 1b).

In addition, for external transmission networks between customer and bank systems, transport encryption is also to be carried out. The customer must ensure that software is installed that, in accordance with the provisions in the EBICS Specification (see Annex 1b), verifies the currentness and authenticity of the bank server certificates installed for this purpose.

2. Initialization of the EBICS connection

2.1 Setting up the communication link

Communication is established by using a URL (Uniform Resource Locator). Alternatively, an IP address of the relevant bank can also be used. The URL or the IP address shall be provided to the customer when the contract is concluded with the bank.

The bank shall provide the subscribers designated by the customer with the following data for access to the EBICS connection:

- the bank's URL or IP address
- the name of the bank
- host ID
- supported version(s) for the EBICS protocol and the security procedure
- partner ID (customer ID)
- user ID
- system ID (for technical subscribers)
- other specific information relating to customer and subscriber permissions.

For each of the subscribers associated with the customer, the bank shall issue a user ID, which uniquely identifies the subscriber. If one or more technical subscribers are associated with the customer (multi-user system), the bank shall issue a system ID in addition to the user ID. If no technical subscribers have been designated, the system ID and user ID are identical.

2.2 Key initialization

2.2.1 New initialization of subscriber key

The key pairs used by the subscriber for the bank-specific ES, the encryption of the order data and the authentication signature must, in addition to the general conditions described under number 1, meet the following requirements:

1. The key pairs shall be exclusively and uniquely assigned to the subscriber.
2. If the subscriber generates his/her key pair independently, the private keys are to be generated using means that the subscriber can keep under his/her sole control.
3. If the keys are provided by a third party, it is to be ensured that the subscriber acquires sole possession of the private keys.
4. In order to authenticate the private keys used, each user shall set a password for each key, securing access to the private key in question.
5. For the private keys used to secure the exchange of data, each subscriber shall set a password for each key, securing access to the private key in question. This password can be avoided, if the security medium of the subscriber is stored in a technical environment that is protected against unauthorized access.

For a subscriber to be initialized at the bank, the subscriber's public key must be provided to the bank system. For this, the subscriber shall provide the bank with his/her public keys through two mutually independent communication channels:

- Through the EBICS connection by means of the system-specific order types provided for this purpose.
- By means of an initialization letter signed by the account holder or an authorized account representative.

In order for the subscriber to be activated, the bank shall verify the authenticity of the public subscriber key provided through EBICS on the basis of the initialization letter signed by the account holder or an authorized account representative.

The initialization letter shall include the following information about each public subscriber key:

- purpose of the public subscriber key:
- electronic signature
- authentication signature
- encryption
- the supported version for each key pair
- exponent length specification
- public key exponent represented in hexadecimal form
- modulus length specification
- public key modulus represented in hexadecimal form
- public key hash value represented in hexadecimal form

The bank shall verify the signature of the account holder or authorized account representative on the initialization letter and the conformity of the hash values of the subscriber's public key sent via the EBICS connection with those provided in written form. If the results of the verification are positive, the bank shall activate the subscriber in question for the agreed order types.

2.2.2 Migration from FTAM to EBICS

If, owing to his/her existing remote data transmission access, the subscriber already has a valid bank-specific key for FTAM that has been activated by the bank, in the course of the separately agreed migration from FTAM to EBICS, the existing bank-specific keys can be kept, provided they corresponds to at least version A004 and this has been agreed with the bank.

In this event, the public keys for authentication and encryption shall be provided to the bank with the designated order types. These messages are to be signed with the key for the bank-specific ES. Separate sending of a signed initialization letter is not necessary.

2.3 Bank key initialization

The subscriber shall collect the bank's public key via a system-specific order type specifically designated for this purpose. The hash value of the public bank key shall also be provided by the bank through a second communication channel that has been separately agreed with the customer.

Prior to the first use of EBICS, the subscriber shall verify the authenticity of the public bank keys provided to him/her via data telecommunication by comparing the hash values of these with the hash values that have been provided by the bank through the separately agreed communication channel.

The customer must ensure that software is installed that verifies the validity of the server certificates used within the framework of the transport encryption using the certification path separately provided by the bank.

3. Placing orders with the bank

The user checks the correctness of the order data and ensures that precisely these data are electronically signed. Once communication has been established, the bank first carries out subscriber-specific authorization checks, including order type authorization or, where appropriate, agreed limit checks. The results of further bank-specific checks, such as limit checks or account authorization checks, for example, are provided to the customer in the customer log at a later date. An exception to this is the optionally agreed online check of the order data agreed with the customer by the bank.

Orders transmitted to the bank system can be authorized as follows:

1. All required bank-specific ES are transferred with the order data.
2. If the distributed electronic signature (DES) has been agreed with the customer for the relevant order type and the ES transmitted is insufficient for bank-specific approval, the order is stored in the bank

system until all required ES are provided.

3. If the customer and the bank agree that the authorization of orders may take place by means of separately submitted accompanying notes, instead of the user's bank-specific ES, a transport signature (type "T") is to be provided for the technical security of the order data. For this, the file is to be provided with a special identification that shows that apart from the transport signature (type "T") there are no further ES for this order. The approval of the order takes place after successful verification by the Bank of the user's signature on the accompanying note.

3.1 Placing orders through the distributed electronic signature (DES)

The manner in which the customer uses the distributed electronic signature must be agreed upon with the bank.

The distributed electronic signature (DES) is to be used if the authorization of orders is to take place independently of the transmission of the order data and, where necessary, also through several subscribers.

If all the bank-specific ES required for authorization are not yet available, the order may be cancelled by a user entitled to do so. If the order has been fully authorized, only a recall in accordance with paragraph VIII of the Terms and Conditions of Remote Data Transfer is possible.

The bank shall be entitled to cancel any orders that have not been fully authorized after the time limits separately specified by the bank have passed.

3.2 Identity verification by the bank

A received order file will only be executed by the bank if the required number of electronic signatures and the signed accompanying note have been received and successfully verified.

3.3 Customer logs

The bank documents the following procedures in customer logs:

- transfer of the order data to the bank system
- transfer of data files from the banking system to the customer system
- results of any identity verification checks of orders made by customers to the banking system

- further processing of orders, insofar as this relates to signature verification, notification of order data
- errors in decompression

The subscriber shall inform himself/herself about the results of the checks carried out by the banks by calling up the customer log.

The subscriber shall add this log, the content of which corresponds to the requirements of section 10 of Annex 1b, to his/her documents and provide it to the bank upon request.

4. Change of subscriber key with automatic activation

If the validity of the identity verification and security media used by the subscriber is limited in terms of time, the subscriber shall inform his/her bank of the new public subscriber key in good time before the expiry date is reached. After the expiry date for the old key is reached, a re-initialization is to be carried out.

If the subscriber generates his/her keys personally, he/she shall renew the subscriber keys using the system-specific order types agreed for this process at the time agreed with the bank and provide notification of this in good time before the expiry date of the old key is reached.

For automatic activation of the new keys without a further subscriber initialization, the following order types are to be used:

- updating the public bank-specific key (PUB) and
- updating the public authentication key and the public encryption key (HCA)

The PUB and HCA order types are to be provided with a valid user bank-specific ES. Following a successful update only the new keys are to be used.

Should the electronic signature not be successfully verified, the procedure specified under number VI(3) of the "Terms and Conditions of Data Telecommunication" shall be followed.

The change of key may only take place after all orders have been fully processed. Failing this, the orders not yet executed are to be resubmitted with the new key.

5. Suspension of the subscriber key

Should suspicion of misuse of the subscriber key arise, the subscriber shall suspend

his/her access rights to all bank systems that use the compromised key.

Provided the subscriber has a valid identity verification and security media, he/she can suspend his/her access rights via the EBICS connection. By sending a message with the "SPR" order type, access for the subscriber under whose user ID the message has been sent will be suspended. Following a suspension, no further orders can be sent by this subscriber via the EBICS connection until the re-initialization as described in number 2 has been carried out.

If the subscriber no longer has valid identity verification and security media, he/she can have his/her identity verification and security media suspended outside of the remote data transfer procedure via the suspension facility separately notified by the bank.

The customer can have the identity verification and security media of a subscriber or all remote data transfer access suspended outside of the remote data transfer process via the suspension facility separately notified by the bank.

ANNEX 1b: Specification of the EBICS Connection

The Technical Specification of the EBICS Connection can be found online at www.ebics.de for downloading. The bank can also provide the Specification on disc (e.g. CD) or in paper format, upon request.

ANNEX 1C: Security Requirements of the EBICS Customer System

In addition to the security measures described in Annex 1a, number 5, the following requirements are to be observed by customers:

- The software installed by the customer for the EBICS process must meet the requirements described in Annex 1a.
- EBICS customer systems may not be installed without firewalls. A firewall is a program that monitors all incoming and out-going data transfers and only permits known or authorized connections.
- A virus scanner shall be installed and

regularly updated with the most recent virus definition files.

- The EBICS customer system is to be set up in such a way that the subscriber must log in before using it. Subscribers must log in as normal users and not as administrators, who are entitled to install programs, for example.
- The internal IT communication channels for unencrypted bank-specific data or for unencrypted EBICS messages are to be protected from interception and manipulation.
- If security updates for the installed operating system and other installed software programs are available, the installed EBICS customer systems is to be updated with these.

The implementation of these requirements shall be the sole responsibility of the customer.

Annex 2 A: FTAM Connection

1. Identity verification and security procedure

The customer (account holder) shall specify the users and their rights in the context of remote data transmission to the bank.

The following identity verification and security procedures are included in the FTAM connection:

- electronic signature
- remote data transfer password

1.1 Electronic signature

For the FTAM connection, identity verification is carried out by means of electronic signatures (ES).

The program used by customers allows various messages (for example, orders for domestic and foreign payment transactions, as well as for initialization, calling up logs and collecting account and revenue data, etc.) to be generated. The bank shall inform the customer what type of messages can be

used and which ones are to be transmitted with electronic signatures.

For the electronic signature the user has a key pair, made up of a private and a public key. The private key is to be protected against unauthorized readout and changes. The public key is to be provided to the bank in accordance with the procedure described under number 2.2. The user's key pair can also be used for communication with other banks.

1.2 Remote data transfer password

With the FTAM connection, the exchange of data between the customer and the bank is protected with a remote data transfer password. Each user receives a separate password for this, which the bank provides to the user during the initialization of the FTAM connection (see number 2.1). The user is obliged to change this password during the initialization process.

The customer shall ensure that each user takes care that no other person acquires knowledge of his/her remote data transfer password. Any other person who knows the remote data transfer password may exchange data with the bank.

The user enters his/her remote data transfer password in order to exchange data.

2. Initialization of the FTAM connection

2.1 Setting up the communication link

The bank shall provide the users designated by the customer with the data necessary to initialize a connection via remote data transfer. This data consists of:

- customer ID
- host name
- Datex-P NUA or ISDN NUA
- host type
- user ID
- first remote data transfer password

The customer uses these data to produce a bank parameter file for the bank, unless this has already been provided to him/her by his/her bank. The customer specifies a minimum number of electronic signatures required for each order type.

Each participant has a function to change the remote data transfer password in his/her

program (»PWA«).

2.2 Key initialization

The key pair used by the user must, in addition to the general conditions described under number 1, meet the following requirements:

1. The key pair shall be exclusively and uniquely assigned to the user.
2. If the user generates his/her key pair independently, the private key is to be generated using means that the user can keep under his/her sole control.
3. If the key pair is provided by a third party, it is to be ensured that the user acquires sole possession of the private key.
4. Each user shall set a password for use of the private key, securing access to the private key.

For the user to be initialized with the bank, the user's public key must be provided to the bank system. For this, the user shall provide the bank with his/her public key through two mutually independent communication channels:

- Through the FTAM connection by means of the system-specific order types provided for this purpose.
- By means of an initialization letter signed by the account holder or an authorized account representative.

In order for the user to be activated, the bank shall verify the authenticity of the public key provided through FTAM on the basis of the initialization letter signed by hand by the account holder or an authorized account representative.

The initialization letter shall include the following data regarding the public key:

- purpose, "electronic signature" of the public key
- the supported version for each key pair
- exponent length specification
- public key exponent represented in hexadecimal form
- modulus length specification
- public key exponent modulus represented in hexadecimal form
- public key hash value represented in hexadecimal form

The bank shall verify the personal signature of the account holder or authorized account representative on the initialization letter and the conformity of the hash value of the user's public key sent via the FTAM connection provided in written form. If the results of the verification are positive, the bank shall activate the user in question for the agreed order types.

3. Placing orders with the bank

3.1 Placing orders with an electronic signature

The user checks the correctness of the files to be signed and ensures that precisely these data are electronically signed. For each file containing orders, one or more electronic signatures are generated, according to the agreement made with the bank.

Orders and the associated electronic signature(s) are contained in any file that can be transferred to the bank either collectively or separately.

Orders are only placed with the bank when, in addition to the file containing the order data (e.g. payment transaction order), a corresponding signature file has been transferred (at a different time from the transmission of the order file, if applicable).

The customer and the bank can agree that the authorization of orders may take place through separately provided accompanying notes. In this case, the activation of the order takes place after the bank has successfully verified of the user's signature on the accompanying note.

In order to retrieve information from the bank, the desired retrieval orders are to be prepared and provided to the bank. For this purpose, the user's corresponding remote data transfer password is to be entered. A bank-specific ES is not required for information requests.

3.2 Identity verification by the bank

A received order file will only be executed by the bank if the required number of electronic signatures or the signed accompanying note have been received and successfully verified.

The bank shall be entitled to cancel any orders that have not been fully authorized after the time limits separately specified by the bank have passed.

3.3 Customer logs

The bank documents the following procedures in customer logs:

- transfer of the order data to the bank system
- transfer of data files from the bank system to the customer system
- results of any identity verification checks of orders made by the customer to the bank system
- the further processing of orders, insofar as this relates to signature verification, notification of order data.
- errors in decompression

The user shall inform himself/herself about the results of the checks carried out by the banks by calling up the customer log.

The participant shall add this protocol, the content of which corresponds to the requirements of section 1.7 of Annex 2b, to his/her documents and provide it to the bank at the request of this latter.

4. Change of user key

4.1 Change of keys with automatic activation

If the validity of the identity verification media used by the user is time limited, the user shall inform his/her bank of the new public key in good time before the expiry date is reached. After the expiry date for the old key is reached, a re-initialization is to be carried out in accordance with number 2.2.

If the user generates his/her key personally, he/she shall renew the key using the system-specific order types agreed for this process with the bank and provide notification of this in good time before the expiry date of the old key is reached.

For automatic activation of the new key without a further participant initialization, the following order type is to be used:

- updating the public key (PUB)

For this, the PUB order is to be provided with a valid electronic signature of the user. Following successful verification of the electronic signature, only the new key is to be used.

Should the electronic signature not be successfully verified, the procedure specified

under number VI (3) of the Terms and Conditions of Remote Data Transfer shall be followed.

The change of key may only take place after all orders have been fully processed. Failing this, the orders not yet executed are to be resubmitted with the new key.

4.2 Change of key with re-initialization

The user may replace his/her current key pair through remote data transfer by providing a new public key ("PUB" order type). The new key pair will only be activated by the bank after receipt of the corresponding initialization protocol produced for this purpose ("Ini-letter"). Only after this can the orders signed with the new key been processed.

For security purposes, after transmission of the new public key any orders signed with the old key and not yet processed by the bank will not be executed. The user shall be informed of this immediately, via the customer log, for example. The relates in particular to orders

- for which the bank has not yet completed verification of the electronic signature or
- which have not yet been transmitted to the bank at this time.

In order for these orders to be executed, they therefore need to be resubmitted in full.

For the period until the bank has received the associated initialization letter signed by hand and the new public key has been activated for use following verification by the bank, which may easily take several days taking into account postal times, an alternative identity verification process can be agreed with the bank for the authentication of orders (alternative procedure).

Following activation of the new public key by the bank, new orders that have not yet been transferred by the bank are to be newly authenticated with the new key pair and transmitted to the bank.

5. Suspension of a user key

Should suspicion of misuse of the key arise, the user shall suspend his/her access rights to all bank systems that use the compromised key.

Provided the user has valid identity verification media, he/she can suspend his/her access rights via the FTAM connection. By sending a message with the "SPR" order type, access, i.e. the public key and the remote data transfer password, for the user under whose user ID the message has been sent shall be suspended. Following a suspension, no further orders can be sent by this user via the FTAM connection until the re-initialization as described under number 2 has been carried out.

If the user no longer has valid identity verification media, he/she can have his/her identity verification media suspended outside of the remote data transfer process via the suspension facility separately notified by the bank.

The customer can have the identity verification and security media of a user or all remote data transfer access suspended outside of the remote data transfer process via the suspension facility separately notified by the bank.

ANNEX 2b: Specification of the FTAM Connection

The Technical Specification of the FTAM Connection can be found online at www.ebics.de for downloading. The bank can also provide the Specification on disc (e.g. CD) or in paper format, upon request.

ANNEX 3: Specification of Data Formats

The Specification of Data Formats can be found online at

www.ebics-zka.de/spec/spezifikation.htm

ready for downloading. The bank can also provide the Specification on disc (e.g. CD) or in paper format, upon request

Annex 4: Transmission of Data in the Event of Format Change

Should the bank be unable to perform a transfer order given to it by the customer as a paperless "SEPA transfer" in such format because the bank of the payee specified by the customer does not support this format and the bank does not reject the transfer, it shall carry out the transfer in a format supported by the payee's bank.

[The following lists only apply when using "Translation Rules MX pacs.008.001.01 to MT103" dated June 2007]

1. In the event of a format change, the following data elements cannot be transmitted:

- different payee (Payment Information » Credit Transfer Transaction Information » Ultimate Creditor)
- different remitter (Payment Information » Ultimate Debtor and Payment Information » Credit Transfer Transaction Information » Ultimate Debtor)
- payee identification (Payment Information » Credit Transfer Transaction Information » Ultimate Creditor)
- remitter identification (Payment Information » Debtor » Identification)

2. In the event of a format change the following data elements can only partially be transmitted:

- payee address [the first 66 of the 140 characters originally available are transmitted] (Payment Information » Credit Transfer Transaction Information » Creditor » Postal Address)
- remitter address [the first 66 of the 140 characters originally available are transmitted] (Payment Information » Debtor » Postal Address)
- payee name [the first 66 of the 70 characters originally available are transmitted] (Payment Information » Credit Transfer Transaction Information » Creditor » Name)
- remitter name [the first 66 of the 70

- characters originally available are transmitted] (Payment Information » Debtor » Name)
- purpose of transfer [the customer reference and purpose of transfer are transmitted together, but must not exceed 130 characters in total. The customer reference (End to End Identification) comes first and is always stated in full.] (Payment Information » Credit Transfer Transaction Information » Remittance Information)