COMMERZBANK

Terms and Conditions for Remote Data Transmission

(Status 31 October 2009)

1. Scope of services

(1) The Bank is available to its Customers (account holders) for remote transmission of data by electronic means, hereinafter referred to as "remote data transmission". Remote data transmission comprises placing orders and exchanging data (transmission of orders and download of information).

(2) The Bank will notify the Customer of the types of services which the Customer may use within the framework of remote data transmission. The use of the remote data transmission is subject to the disposal limits agreed with the Bank

(3) Remote data transmission is possible by various procedures, especially via the EBICS interface (Annexes 1a to 1c) and the FTAM interface (Annexes 2a and 2b). The applicable transmission procedure shall be agreed between the Customer and the Bank.

(4) The structure of the data records and files for transmission of orders and download of information is described in the specifications for the data formats (Annex 3).

2. Users and subscribers, identification and security media

(1) Orders may only be placed by the Customer or the Customer's authorised agents. The Customer and the authorised agents are hereinafter collectively named "Users". To place orders with the Bank, each User requires individual identification media which must be activated by the Bank. The requirements for the identification media are defined in Annex 1a and Annex 2a. If agreed with the Bank, orders transmitted by remote data transmission can be authorised with a signed accompanying note.

(2) For data exchange via EBICS, the Customer may designate "technical subscribers" in addition to the authorised signatories, who must be natural persons and who are only authorised to carry out data exchanges. Users and technical subscribers are hereinafter collectively named "Subscribers". To protect the data exchange, each Subscriber requires individual security media which must be activated by the Bank. The requirements for the security media are described in Annex 1a.

(3) For data exchange via FTAM, each User requires a password for remote data transmission, which is provided by the Bank. The requirements for the remote data transmission password are described in Annex 2a.

(4) Identification and security media are authentication instruments in the senses of Section 1 (5) of the Payment Services Regulation Act (Zahlungsdiensteaufsichtsgesetz/ZAG).

3. Procedural provisions

(1) The transmission procedure agreed between the Customer and the Bank shall be subject to the requirements described in Annexes 1a and 2a, the requirements described in the documentation of the technical interfaces (Annexes 1b and 2b) and the specifications for the data formats (Annex 3).

(2) The Customer is obliged to ensure that all Subscribers observe the procedures and specifications agreed with the Bank.

(3) The assignment of data fields is governed by the completion and control guidelines applicable to the specific format used. The details stated in the "reason for payment" field shall refer exclusively to the respective payment transaction of the data record. At the beginning of the data field "reason for payment", details which the beneficiary/payer intends to access automatically or which the transferor/payee requires if the payment is returned because its destination could not be located or it has remained unpaid, are to be entered left-justified. Furthermore, the space available under "reason for payment" may not be used by the User to achieve a desired print layout, unless the space available under the "reason for payment" field of the data record and, if applicable, subsequent extension areas for details as to reason for payment are fully used. "Reason for payment" details may not replace the transmission of a separate message unrelated to a payment transaction (for example invoice, salary statement, etc.). Advertising texts may not be contained in the "reason for payment" field.

(4) The User must correctly state the bank identification code (bank sort code or BIC) of the payment service provider of the payee or payer (paying agent) and the account identification code (account number or IBAN) of the payee or payer. The payment service providers involved in the settlement of the payment order are authorised to process the transaction exclusively on the basis of the bank and account identification codes. Incorrect details may lead to the payment order being misrouted and thus result in damage for the Customer. Any damages or losses which may arise therefrom shall be borne by the Customer. This provision shall apply accordingly if any other orders (not payment orders) are transmitted by remote data transmission.

(5) Prior to the transmission of the order data to the Bank, a record of the full contents of the files to be transmitted and of the data transmitted for the verification of identification must be prepared. Such record must be kept by the Customer for a minimum period of 15 calendar days from the date of execution for domestic payment orders and 30 calendar days for international payment orders in such a form that it can be made available to the Bank again at short notice on request, unless otherwise agreed.

(6) In addition, the Customer must generate an electronic protocol for each data exchange according to section 10 of the EBICS Specification (Annex 1b) or section 1.7 of the FTAM Specification (Annex 2b), keep the protocol on file and make it available to the Bank on request.

(7) To the extent that the Bank provides the Customer with data on payment transactions which are not yet finally processed, such data shall be deemed to be only non-binding information. Such data will be specially marked.

(8) The submitted order data shall be authorised either by an electronic signature or by a signed accompanying note as agreed with the Bank. Such order data shall be effective as an order

a) for data submitted with an electronic signature:
- if all necessary electronic signatures of the Users have been received by remote data transmission within the agreed period, and
- if the electronic signatures can be successfully checked against the agreed keys;

b) for data submitted with an accompanying note:
- if the Bank receives the accompanying note in the agreed period, and
- if the accompanying note has been signed in accordance with the account mandate.

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

(1) Depending on the transmission procedure agreed with the Bank, the Customer is obliged to ensure that all Users comply with the identification procedures described in Annexes 1a and 2a.

(2) The User may place orders by means of the identification media activated by the Bank. The Customer shall cause every User to ensure that no third party obtains possession of the User's identification medium or gains knowledge of the password protecting it. This is because any third person who has obtained possession of the medium or a duplicate thereof can misuse the agreed services in conjunction with the corresponding password. The following shall be observed in particular to keep the identification media secret:
- the data identifying the User may not be stored outside the identification medium, for example on the computer's hard disk,
- the identification medium must be kept safely after the end of the remote data transmission procedure,
- the password protecting the identification medium may not be written down or stored electronically, and
- when entering the password, care must be taken to ensure that no other persons can steal it.

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

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

(2) With respect to connection via FTAM, the Customer is obliged to ensure that all Users comply with the security procedures described in Annex 2a. The Customer shall request that each User ensures that no third person gains knowledge of its password. Any third party who gains knowledge of the remote data transmission password can misuse data exchange with the Bank.

6. Suspension of the identification and security media

(1) If the identification or security media are lost, become known to third parties or misuse of such media is suspected, the Subscriber must imme-

diately request that the Bank suspend the remote data transmission access. Further details are stipulated in Annexes 1a and 2a. The Subscriber can also request that the Bank suspend the access at any time via the separately notified contact data.

(2) If three successive attempts are made to transmit an order to the Bank with an incorrect identification medium or to carry out the data exchange with an incorrect security medium, the Bank will suspend the respective Subscriber's remote data transmission access. Such a suspension cannot be cancelled via remote data transmission. The Customer must contact his/her bank in order to cancel the suspension.

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

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

7. Treatment of incoming order data by the Bank

(1) The order data transmitted to the Bank by remote data transmission are processed during the normal course of work. If the Bank is unable to execute a credit transfer initiated by a Customer on a paperless basis as a "SEPA Credit Transfer" in this format because the creditor's payment service provider named by the Customer does not support this format and the credit transfer is not rejected by the Bank, it will execute the credit transfer in a format supported by the creditor's payment service provider. In the event of such a change of format, the data elements or parts thereof listed in Annex 4 cannot be transmitted.

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

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

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

(5) The Bank shall be obliged to document the above procedures and the forwarding of the orders for processing in the Customer protocol (cf. Annexes 1a and 2a). The Customer in turn shall be obliged to call up the Customer protocol without undue delay and to keep himself/herself informed of the processing of the order. In the event of any discrepancies, the Customer should contact the Bank.

8. Recall

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

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

9. Execution of orders

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

- the order data submitted by remote data transmission must have been authorised in accordance with No. 3 sub-section 8,
- the defined data format must be complied with,
- the disposal limit must not be exceeded,
- the requirements for execution must be fulfilled in accordance with the special conditions applicable to the relevant service type, and
- the execution of the order must not violate any other legal provisions.

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

10. Security of the Customer's system

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

11. Liability

11.1 Liability of the Bank for unauthorised orders and orders not executed or incorrectly executed

The liability of the Bank for unauthorised orders and orders not executed or incorrectly executed shall be based on the special conditions agreed for the respective order (for example Corporate Customer Terms and Conditions for Payment Services).

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 suspend access

(1) If unauthorised payment transactions before the request to suspend access result from the use of a lost, stolen or otherwise missing identification or security medium or any other misuse of such media, the Customer shall be liable for the resulting loss to the Bank if the Subscriber is to blame for the loss, theft, other mislaying or other misuse of the identification or security medium. The Customer shall also be liable if he/she has not been careful in selecting any of his/her nominated Subscribers and/or has not regularly checked the Subscriber's compliance with the obligations under these terms and conditions. If the Bank has contributed to the occurrence of a loss through any fault of its own, the principles of contributory negligence shall determine the extent to which the Bank and the Customer must bear the loss.

(2) The Customer shall not be obliged to bear the loss under sub-sections 1 and 2 if the Subscriber was not able to issue the request to suspend access under No. 6.1 because the Bank had not taken steps to guarantee its ability to receive such requests and the loss arose as a result of his/her omission.

(3) The liability for losses caused in the period for which the disposal limit applies shall be limited to the agreed disposal limit.

11.2.2 Liability of the Customer for other unauthorised transactions before a request to suspend access

If unauthorised transactions other than payment transactions before the request to suspend access result from the use of a lost, stolen or otherwise missing identification or security medium or any other misuse of such media, the Customer shall be liable for the resulting loss to the Bank if the Subscriber is to blame for the loss, theft, other mislaying or other misuse of the identification or security medium. The Customer shall also be liable if he/she has not been careful in selecting any of his/her nominated Subscribers and/or has not regularly checked the Subscriber's compliance with the obligations under these terms and conditions. If the Bank has contributed to the occurrence of a loss through any fault of its own, the principles of contributory negligence shall determine the extent to which the Bank and the Customer must bear the loss.

11.2.3 Liability of the Bank after the request to suspend access

As soon as the Bank has received a request to suspend access from a Subscriber, it shall accept all losses which arise thereafter as a result of any unauthorised orders. This shall not apply if a Subscriber has acted with fraudulent intent.

12. Final provisions

The Annexes mentioned in these terms and conditions are part of the Agreement made with the Customer.

Annexes:

Annex 1a: EBICS Specification
Annex 1b: EBICS Specification
Annex 1c: Security requirements for the EBICS system
Annex 2a: FTAM interface
Annex 2b: FTAM Specification
Annex 3: Specifications for the data formats
Annex 4: Transmission of data in the event of a format change

Annex 1a: EBICS interface

1. Identification and security procedures

The Customer (account holder) shall disclose the Subscribers and their authorisations with respect to remote data transmission to the credit institution. The following identification and security procedures are used for EBICS:
Electronic signatures
Authentication signature
Encryption

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

1.1 Electronic signatures

1.1.1 Electronic signatures of the Subscribers

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

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

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

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

1.2 Authentication signature

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

1.3 Encryption

To ensure the secrecy of banking data on the application level, the order data must be encrypted in accordance with the EBICS Specification (see Annex "EBICS Specification") by the Customer, who must also take into account the current validity and authenticity of the credit institution's saved public keys.

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

2. Initialisation of the EBICS interface

2.1 Installation of the communication interface

Communication is initialised by utilising a URL (Uniform Resource Locator). Alternatively, an IP address for the respective credit institution may be used. The URL or IP address is disclosed to the Customer on conclusion of the agreement. For initialising EBICS, the credit institution shall provide the Subscribers designated by the Customer with the following data:
– URL or IP address of the credit institution
– Name of the credit institution
– Host ID
– Permitted version(s) of the EBICS protocol and the security procedures
– Partner ID (Customer ID)
– User ID
– System ID (for technical subscribers)
– Further specific details on Customer and Subscriber authorisations

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

2.2 Initialisation of the keys

2.2.1 First initialisation of the Subscriber keys

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

(1) The key pairs must be assigned exclusively and unambiguously to the Subscriber.

(2) If the Subscriber generates the keys, the private keys must be generated by means which the Subscriber can keep under his/her sole control.

(3) If the keys are made available by a third party, it must be ensured that the Subscriber is the sole recipient of the private keys.

(4) With respect to the private keys used for identification, each User shall define a password for each key which protects access to the respective private key.

(5) With respect to the private keys used to protect the data exchange, each Subscriber shall define a password for each key which will protect access to the respective private key. This password may be dispensed with if the Subscriber's security medium is stored in a technical environment which is protected against unauthorised access.

Transmission of the Subscriber's public keys to the bank system is necessary for the Subscriber's initialisation by the credit institution. For this purpose, the Subscriber shall transmit its public keys to the credit institution via two independent communication channels:
– via EBICS by means of the order types provided by the system for this procedure, and
– via an initialisation letter signed by the account holder or an authorised signatory.

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

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

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

2.2.2 Migration from FTAM to EBICS

If the Subscriber has already received a valid banking key that has been activated by the credit institution under a previously existing access to remote data transmission for FTAM, the banking keys may be retained in the course of a separately agreed migration from FTAM to EBICS, provided that they correspond at least to Version A004 and retention has been agreed to with the credit institution.

In this event, the public keys for authentication and encryption will be transmitted to the credit institution via the order types intended for this purpose. These messages must be signed with the key for the banking ESs. The separate transmission of a signed initialisation letter may be omitted.

2.3 Initialisation of the Bank keys

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

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

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

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

3. Placing orders with the credit institution

The User shall verify the correctness of the order data and ensure that only the verified data are signed electronically. Upon initialisation of communication, the credit institution first carries out Subscriber-related authorisation verifications, such as order type authorisation or verifications of possibly agreed limits. The results of additional banking verifications such as limit verifications or account authorisation verifications will later be notified to the Customer in the Customer protocol. As an exception to this, the Customer may choose to agree to online verification of the order data by the credit institution.

Orders transmitted to the Bank system may be authorised as follows:

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

(2) If distributed ES ("verteilte elektronische Unterschrift – VEU") has been agreed with the Customer for the respective order type and the transmitted ESs are insufficient for banking authorisation, the order is stored in the Bank system until all required ESs are applied.

(3) If the Customer and the credit institution agree that orders may be authorised by means of separately transmitted accompanying notes, a transport signature (type "T") must be supplied for technical protection of the order data instead of the User's banking ES. To this end, the file must bear a special code indicating that there are no further ESs for this order other than the transport signature (type "T"). The order is authorised after the credit institution successfully verifies the User's signature on the accompanying note.

3.1 Placing orders by means of the distributed electronic signature (VEU)

The manner in which the distributed electronic signature will be used by the Customer shall be agreed with the credit institution.

The distributed electronic signature (VEU) shall be used where orders are to be authorised independently of the transport of the order data and, if applicable, by several Subscribers. Until all banking ESs necessary for authorisation have been applied, the order may be deleted by an authorised User. If the order has been fully authorised, only a recall pursuant to section VIII of the Conditions for Remote Data Transmission can be made.

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

3.2 Verification of identification by the credit institution

An incoming order is executed by the credit institution only after the necessary banking ES or the signed accompanying note has/have been received and positively verified.

3.3 Customer protocols

The credit institution will document the following transactions in Customer protocols:
– Transmission of the order data to the Bank system
– Transmission of information files from the Bank system to the Customer system
– Result of each verification of identification for orders from the Customer to the Bank system
– Further processing of orders if they concern the verification of signatures and the display of order data
– Decompression errors

The Subscriber is obliged to keep informed on the result of the verifications carried out by the credit institution by downloading the Customer protocol.

The Subscriber shall include this protocol, the contents of which correspond to the provisions of section 10 of the Annex "EBICS Specification", in its files and submit it to the credit institution on request.

4. Change of the Subscriber keys with automatic activation

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

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

The following order types shall be used for an automatic activation of the new keys without renewed Subscriber initialisation:
– update of the public banking key (PUB), and
– update of the public authentication key and the public encryption key (HCA).

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

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

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

5. Suspension of the Subscriber keys

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

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

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

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

Annex 1b: EBICS Specification

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

Annex 1c: Security requirements for the EBICS system

In addition to the security measures described in section 5 of the Annex "Conditions for remote data transmission – EBICS interface", the Customer must observe the following requirements:

The software used by the Customer for the EBICS procedure shall comply with the requirements described in the Annex "EBICS interface". EBICS customer systems may not be used without a firewall. A firewall is an application which supervises all incoming and outgoing messages and only allows known or authorised connections to pass through.

A virus scanner must be installed and must be updated regularly with the newest virus definition files. The EBICS customer system must be configured in such a manner that the Subscriber has to login before the system can be used. The Customer must login as a normal user and not as an administrator who is authorised, for instance, 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-relevant updates are available for the operating system in use or for other security-relevant software programs which may have been installed, such updates shall be applied to the EBICS customer systems.

The Customer is exclusively responsible for implementation of these requirements.

Annex 2a: FTAM interface

1. Identification and security procedures

The Customer (account holder) will disclose the Users and their authorisations in respect of remote data transmissions to the credit institution. The following identification and security procedures are used for FTAM:
– Electronic signature
– Remote data transmission password

1.1 Electronic signature

The identification procedure applied for FTAM connections is the electronic signature (ES).
By means of the program used by the Customer, different types of messages can be generated (for example domestic and international payment

orders, messages concerning initialisation, protocol downloads, collection of account and turnover information, etc.). The credit institution will inform the Customer what message types can be used and which of these must be transmitted with an electronic signature.

The User has a key pair consisting of a private and a public key for the electronic signature. The private key must be protected against unauthorised readout and modification. The public key shall be disclosed to the credit institution in accordance with the procedure described in section 2.2. The User's key pair may also be used for communication with other credit institutions.

1.2 Remote data transmission password

In respect of FTAM connections, the data exchange between the Customer and the credit institution is secured by a remote data transmission password. Each User will receive a separate password from the credit institution in conjunction with the initialisation of the FTAM procedure (see section 2.1). The User must change this password during the initialisation procedure.

The Customer shall make sure that each User ensures that no third person gains knowledge of its remote data transmission password. Any third person who gains knowledge of the remote data transmission password can engage in data exchange with the credit institution.

To execute the data exchange, the User must enter its remote data transmission password.

2. Initialisation of the FTAM interface

2.1 Installation of the communication interface

The credit institution will provide the Users designated by the Customer with the items of information which are necessary for connecting via remote data transmission. These are:
– Customer ID
– Host name
– Datex-P NUA or ISDN-NUA
– Host type
– User ID
– Initial remote data transmission password
On the basis of this data, the Customer shall generate a bank parameter file for the credit institution, unless such file is made available to the Customer by the credit institution. The Customer shall define the required minimum number of electronic signatures for each order type.

Each Subscriber shall execute a function under its program to change the remote data transmission password ("PWA").

2.2 Initialisation of the keys

In addition to the general conditions described in section 1, the key pair used by the Subscriber must comply with the following requirements:

(1) The key pair must be assigned exclusively and unambiguously to the User.

(2) If the User generates the keys itself, the private keys must be generated by means which the User can keep under its sole control.

(3) If the key pair is made available by a third party, it must be ensured that the User is the sole recipient of the key.

(4) In order to use the private key, each User shall define a key password which secures access to the private key.

For initialisation of the User by the credit institution, the User's public key must be transmitted to the Bank system. To this end, the User will transmit its public key to the credit institution via two independent communication channels:
– via FTAM by means of the order types provided by the system for this procedure, and
– via an initialisation letter signed by the account holder or an authorised signatory.
For initialisation of the User, the credit institution shall verify the authenticity of the public key transmitted via FTAM on the basis of the initialisation letter signed manually by the account holder or an authorised signatory.

The initialisation letter shall contain the following data on the public key:
– "Electronic signature" as the designated purpose of the public key
– The respective version supported for each key pair
– Specification of exponent length
– Hexadecimal representation of the public key's exponent
– Specification of modulus length
– Hexadecimal representation of the public key's modulus
– Hexadecimal representation of the public key's hash value
The credit institution will verify the manual signature of the account holder or authorised signatory on the initialisation letter and will also verify whether the hash value of the User's public key transmitted via FTAM is identical to that transmitted in writing. If a positive verification is made, the credit institution will activate the relevant User for the agreed order types.

3. Placing orders with the credit institution

3.1 Placing orders by means of the electronic signature

The User shall verify the correctness of the files to be signed and ensure that only the verified data are signed electronically. Pursuant to the agreement with the credit institution, one or several electronic signatures will be generated for each file containing orders.

Orders and the corresponding electronic signature(s) are each contained in one file, which can be transmitted to the credit institution either together or separately.

The orders are deemed to be placed with the credit institution only if a signature file is transmitted in addition to the file containing the order data (for example payment order). The transmission date of this file may differ from the transmission date of the order file.

The Customer and the credit institution may agree that orders can be authorised by means of an accompanying note to be transmitted separately. In this case, the order is authorised after the credit institution positively verifies the User's signature on the accompanying note.

To download information from the credit institution, the desired download orders must be generated and sent to the credit institution. For this purpose, the User must enter the remote data transmission password. A banking ES is not required to download information.

3.2 Verification of identification by the credit institution

An incoming order is executed by the credit institution only after it has received and positively verified the necessary number of electronic signatures or the signed accompanying note.

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

3.3 Customer protocols

The credit institution will document the following transactions in Customer protocols:
– Transmission of the order data to the Bank system
– Transmission of information files from the Bank system to the Customer system
– Result of each verification of identification for orders from the Customer to the Bank system
– Further processing of orders if they concern the verification of signatures and the display of order data
– Decompression errors
The User is obliged to keep informed on the result of the verifications carried out by the credit institution by downloading the Customer protocol.

The User shall keep this protocol, the contents of which are in accordance with the provisions of section 1.7 of Annex 2b, in its files and submit it to the credit institution on request.

4. Change of the User keys

4.1 Change of the keys with automatic activation

If the validity period of the identification media used by the User is limited, the User must transmit the new public keys to the credit institution in good time prior to the expiration of such validity period. After the expiration of the old keys, a new initialisation must be made according to section 2.2.

If the User generates the keys itself, the User must renew the keys using the order types provided by the system for this purpose on the date agreed with the credit institution and must transmit the keys in good time prior to expiration of the old keys.

The following order type shall be used for automatic activation of the new key without renewed initialisation:
– update of the public banking key (PUB).
For this purpose, the User must supply a valid electronic signature for order type PUB. After successful verification of the electronic signature, only the new key shall be used.

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

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

4.2 Change of the keys with new initialisation

The User can replace the previous key pair by remote transmission of a new public key (order type "PUB"). The new key pair is activated only after

the credit institution receives the initialisation protocol (INI letter) generated for this purpose. Orders signed with the new key will only be executed thereafter.

After transmission of the new public key, all orders signed with the old key and still unprocessed by the credit institution will for security reasons no longer be executed. The User will immediately be informed thereof, for example by means of the Customer protocol. In particular this applies to the following orders:
– orders for which the verification of the electronic signature has not yet been completed by the credit institution, or
– orders which have not yet been transmitted to the credit institution at this time.
These orders must therefore be placed again with the credit institution if they are still to be executed.

For the period until the credit institution has received the corresponding manually signed initialisation letter and, after verification of said letter, until it has activated the new public key, an alternative identification procedure for placing orders (substitute process) may, if requested, be agreed with the credit institution for such interim period, which including the mail delivery period can easily last several days.

After the credit institution activates the new public key, the new key pair shall be used to authorise orders that have not yet been transmitted to the credit institution and to transmit such orders.

5. Suspension of User keys

If misuse of the key is suspected, the User is obliged to suspend the access authorisation to all Bank systems using the compromised key.

If the User is in possession of valid identification media, the User may suspend access authorisation via FTAM. If a message with order type "SPR" is sent, access (i.e. the public key and the remote data transmission password) for the relevant User with whose user ID the message was sent will be suspended. After suspension, no further orders can be placed by this User via FTAM until the User has been initialised again as described in section 2.

If the User is no longer in possession of valid identification media, the User may request suspension of the identification media outside the remote data transmission procedure by means of the suspension facility separately notified by the credit institution.

Outside the remote data transmission procedure, the Customer may request suspension of a User's identification and security media or of the entire remote data transmission access via the suspension facility notified by the credit institution.

Annex 2b: FTAM Specification

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

Annex 3: Specifications of the data formats

The specifications are published on the website http://www.companyworld.de/vertragsbedingungen under "CODAT – Data carrier exchange between Customer and Bank with 8", 5¼" and 3½" disks" and "CODAT – Magnetic tapes and 3½" disks (for international payments)".

Annex 4: Transmission of data in the event of a format change

If the Bank is unable to execute a credit transfer initiated by a customer on a paperless basis in the format "SEPA Credit Transfer" in this format because the beneficiary's credit institution named by the Customer does not yet support this format, the Bank will execute the credit transfer in a format supported by the beneficiary's credit institution.
The following lists only apply if the "Translation Rules MX pacs.008.001.01 to MT 103" of June 2007 are used.

(1) In the event of a format change, the following data elements cannot be transmitted:
– Different beneficiary
(Payment Information » Credit Transfer Transaction Information » Ultimate Creditor)
– Different remitter
(Payment Information » Ultimate Debtor and Payment Information » Credit Transfer Transaction Information » Ultimate Debtor)
– Identification of the beneficiary
(Payment Information » Credit Transfer Transaction Information » Creditor » Identification)
– Identification of the remitter
(Payment Information » Debtor» Identification)

(2) In the event of a format change, the following data elements can only be transmitted in part:
– Address of the beneficiary [the first 66 of the 140 originally possible characters are transmitted]
(Payment Information » Credit Transfer Transaction Information » Creditor » Postal Address)
– Address of the remitter [the first 66 of the 140 originally possible characters are transmitted]
(Payment Information » Debtor » Postal Address)
– Name of the beneficiary [the first 66 of the 70 originally possible characters are transmitted]
(Payment Information » Credit Transfer Transaction Information » Creditor » Name)
– Name of the remitter [the first 66 of the 70 originally possible characters are transmitted]
(Payment Information » Debtor » Name)
– Remittance information [customer reference and remittance information are both transmitted, but together not more than 130 characters. The customer reference (End to End Identification) is placed first and must always be entered fully.]
(Payment Information » Credit Transfer Transaction Information » Remittance Information)