Terms and Conditions for Remote Data Transmission

As at: June 2018, Commerzbank AG Vienna Branch, ~~Issued: February 2017~~Austria

1. Scope of services

(1) The Bank is available to its Customer (account holder who is not a consumer within the meaning of ZaDiG [Payment Services Act] 2018) for remote transmission of data by electronic means, hereinafter referred to ~~a "~~as "remote data transmission~~" or~~". Remote data transmission comprises placing orders and exchanging data (transmission of orders and download of information).

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

(3) Remote data transmission is possible via the EBICS interface (Annexes 1a to 1c).

(4) The structure of the data records and files for transmission of orders and download of information is described in the data format specification (Annex 3) or agreed upon separately.

2. Users and Subscribers, identification and security media

(1) Orders may only be placed via the EBICS interface by the Customer or the ~~Customer's~~Customer's authorised account representatives. The Customer and the authorised account representatives are hereinafter collectively ~~named~~referred to as "Users". To authorise order data transmitted by remote data transmission, each User requires individual identification media ~~which~~that must be activated by the Bank. The requirements for the identification media are defined in Annex 1a. If agreed with the Bank, orders transmitted by remote data transmission can be authorised with a signed accompanying document.

(2) For data exchange via the EBICS interface, the Customer may, in addition to the authorised agents, appoint ~~"~~"Technical Subscribers~~"~~" who ~~shall be~~are natural persons and who ~~will~~shall only be authorised to carry out the data exchange. Hereinafter, Users and Technical Subscribers ~~will~~are collectively ~~be called "~~referred to as "Subscribers~~".~~". To protect the data exchange, each Subscriber requires individual security media that must be activated by the Bank. The requirements to be met by the security media are specified in Annex 1a.

~~(3) Identification and security media are authentication instruments within the meaning of Art. 3 Z 17 ZaDiG.~~

3. Procedural provisions

(1) The requirements described in Annex 1a, in the technical interface documentation (Annex 1b) and in the data format specification (Annex 3) shall apply to the transmission method agreed upon between the Customer and the Bank. ~~The Customer is obliged to submit credit transfer orders and direct debit collection orders for payments in euros within the European Economic Area in the ISO 20022 format only, pursuant to chapter 2 of Annex 3. Direct debit collection orders for payments generated at a POS (point of sale) with the aid of a payment card that lead to a direct debit from a domestic payment account (Section 3 para 13 ZaDiG) have to be submitted in the ISO 20022 format.~~

(2) The Customer shall ~~be obligated to~~ ensure that all Subscribers comply with the ~~procedures~~remote data transmission procedure and the specifications ~~agreed with the Bank~~.

~~(3)~~ The assignment of data fields is governed by the completion and control

(3) guidelines applicable to the specific format used (Annex 3).

(4) The User shall supply the payee's/payer's correct ~~account identification code (account number or IBAN) and – if also required – the identification code of the payment service provider (bank code or BIC) of the payee's/ the payer's payment service provider (paying agent).~~customer identification information in accordance with the General Business Conditions (GBC). The payment service providers engaged in processing a payment order are authorised to process the payment solely on the basis of the ~~account~~customer identification ~~code and – if also supplied – the identification code of the payment service provider.~~information. Incorrect details may result in an order being misdirected. Any resulting losses and disadvantages ~~this causes~~ shall be borne by the Customer. This provision shall apply accordingly if any other orders (not payment orders) are transmitted by remote data transmission.

(5) Prior to the transmission of the order data to the Bank, a record of the full contents of the files to be transmitted and of the data transmitted for the verification of identification ~~must~~shall be prepared. Such ~~record must be~~records shall be demonstrably kept by the Customer for a minimum period of 30 calendar days from the date of execution indicated in the file (for transfers) or the maturity date (for direct debit transactions) or in the case of multiple dates, the latest date, in such a form that ~~it~~the file can be made available to the Bank again at short notice on request, unless otherwise agreed.

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

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

(8) The order data submitted via remote data transmission shall be authorised either by an electronic signature or by a signed accompanying document, as agreed with the Bank. ~~Such order data shall be effective as an order~~

Such order data shall be effective as an order

~~a)~~ for data submitted with an electronic signature~~:~~

a) 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~~;~~, or

~~(b)~~b) for data submitted with an accompanying document~~:~~ if

- ~~if~~ the Bank receives the accompanying document in the agreed period and
- ~~if~~ the accompanying document has been signed in accordance with the account mandate.

4. Duties of conduct and care in dealing with the identification media that are required for the authorisation of orders

(1) ~~Given~~In accordance with the transmission procedure agreed with the Bank, the Customer shall ensure that all Users comply with the identification procedures specified in Annex 1a.

(2) The User may place orders by means of the identification media activated by the Bank. The Customer shall ~~cause~~obligate 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~~, as any ~~third~~other person who ~~has obtained possession of~~obtains the medium or a corresponding duplicate ~~thereof~~ can ~~misuse~~make improper use of the agreed services in ~~conjunction~~connection with the ~~corresponding~~ relevant password. The following shall be observed in particular to keep the identification media secret:

- ~~the~~The data identifying the User ~~may not~~shall be ~~stored outside the identification medium, for example on the computer's hard disk,~~

- ~~the identification medium must be removed from the reading device~~protected against unauthorised access and kept ~~safely after the end of the remote data transmission procedure,~~secure.

- ~~the~~The password protecting the identification medium may not be written down or stored electronically~~, and~~.

- ~~when~~When entering the password, care ~~must~~shall be taken to ensure that no other persons can steal it.

~~The Customer instructs the Bank to save the personal key of the Participant/User in a technical environment that is protected against unauthorised access. The Bank is also entitled to instruct a reliable service provider to do this. The password required to authorise the personal key will be replaced by a TAN using the photoTAN procedure.~~

~~The storage of the electronic key in a technical environment provided by the Bank (or by a service provider authorised by the Bank) (see No. 2.2.1 (5) of Annex 1a to the **Terms and Conditions for Remote Data Transmission**) is permitted.~~

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

With respect to connection via EBICS, the Customer is obliged to ensure that all Subscribers comply with the security procedures described in Annex 1a.

The Subscriber shall secure the data exchange by means of the security media activated by the Bank. The Customer is obliged to request each ~~User~~Subscriber 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~~shall be stored in a technical environment ~~which~~that is protected against unauthorised access~~. This is because~~, as any third person who gains access to the security medium or a duplicate thereof may misuse the data exchange.

6. ~~Suspending~~Blocking of identification and security media

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

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

(3) If misuse is suspected, the Bank ~~will suspend~~shall block the entire remote data transmission access. It ~~will~~shall immediately inform the Customer of this ~~suspension~~block outside the remote data transmission process. Such a ~~suspension~~block 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.

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

(3) The Bank ~~will~~shall verify the identification of the User(s~~),~~) and the authorisation of the order data transmitted by remote data transmission on the basis of the electronic signatures generated by the ~~Users~~User(s) with the identification media or on the basis of the accompanying document provided and ~~will~~shall check that the order data records ~~or as to the photoTAN provided~~ comply with the provisions specified in Annex 3. If this verification reveals any discrepancies, the Bank ~~will~~shall not process the ~~respective~~affected order data and ~~immediately inform~~will notify the Customer thereof immediately. The Bank ~~shall be~~is entitled to delete orders~~, which~~ that have not been fully authorised~~,~~ after expiry of the time limit separately ~~notified~~communicated 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~~shall provide proof of the errors in the files or data records in a suitable form and notify the User thereof immediately. The Bank is authorised to exclude files or data records with errors from further processing if a proper execution of the order cannot be ensured.

(5) The Bank shall be obliged to document the above procedures (cf. Annex 1a) and the forwarding of the orders for processing in the customer protocol. 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 status of the order. In the event of any discrepancies, the Customer should contact the Bank.

8. Recall

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

(2) The extent to which an order can be recalled shall be governed by the applicable ~~special~~ conditions (for example ~~Terms and~~, General Business Conditions ~~for Payment Services). Cancellation of orders can only~~). Order cancellations may take place outside the remote data transmission process~~. To do this,~~ or, if so agreed with the Customer ~~must inform~~, in accordance with the specifications of Section 11 of Annex 3. To this end, the customer shall notify the Bank of the ~~individual details given in~~particulars of the original order.

~~**9. Execution of orders**~~

9. Order execution

(1) The Bank ~~will~~shall execute ~~the~~ orders if all of the following requirements for execution have been fulfilled:

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

(2) If the execution conditions ~~for execution outlined in sub-section~~pursuant to paragraph 1 ~~are~~have not ~~fulfilled~~been met, the Bank ~~will~~shall not execute the order and ~~will~~shall inform the ~~Customer that~~customer of non-execution of the order ~~has not been executed without undue delay through~~ immediately and in the agreed ~~communication channel. As far as~~manner. If possible, the Bank ~~will~~shall notify the ~~Customer,~~customer of the reasons and errors ~~which caused~~that resulted in non-execution of the order ~~not to be executed,~~ and ~~the possible ways to correct~~how these errors~~.~~ can be rectified. This shall not apply if ~~giving~~the statement of reasons ~~would violate any~~is in breach

of other ~~legal~~statutory provisions.

10. Security of the Customer's system

The Customer shall ensure ~~an~~ adequate protection of the systems ~~that he uses~~used by the Customer for remote data transmission. The security requirements applicable to the EBICS procedure are specified in Annex 1c.

11. Liability

~~11.1~~11.1. Liability of the Bank in the event of unauthorised orders ~~and orders not~~ or non-executed ~~or executed~~, incorrectly executed or delayed remote data transmission

The ~~Bank´s~~General Business Conditions govern the Bank's liability in the event of unauthorised orders ~~and orders not~~ or non-executed ~~or executed~~, incorrectly ~~is based on the special conditions arranged for the order type in question (e.g. terms and conditions for payment services).~~executed or delayed remote data transmission.

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

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

(1) The provisions of Section 68 (2), (5) and (6) ZaDiG 2018 are waived. If unauthorised payment ~~transaction~~transactions prior to a blocking request ~~is~~are based on the use of a lost, stolen or otherwise missing identification or security medium, or on any other form of misuse of the aforementioned, the Customer shall be liable for all of the losses consequently incurred by the Bank if the Subscriber is responsible for ~~their~~the identification or security medium being lost, stolen or otherwise missing, or otherwise misused. The Customer shall also be liable ~~if they neglect~~in the event of failing to select ~~one of their~~an appointed ~~Subscribers~~Subscriber with due care and/or ~~if they fail~~of failing to regularly verify that the Subscriber ~~is fulfilling its~~ fulfils the obligations ~~in accordance with~~under these ~~terms and conditions.~~Conditions.

~~(1)~~ If the Bank contributed to the generation of a loss due to culpable conduct, the ~~degrees~~degree to which the loss must be borne by ~~both~~ the Customer and by the Bank ~~are~~is determined on the basis of the principles of contributory negligence.

(2) The Customer is not obliged to provide compensation for the loss pursuant to ~~sections~~para. 1~~ and 2~~ if the Subscriber was unable to lodge a blocking request in accordance with ~~section~~Section 6 ~~sub-section~~para. 1 because the Bank failed to ensure that a blocking request could be submitted, thereby causing the loss.

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

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

~~11.2.2~~11.2.2. Liability of the Customer in the event of other unauthorised transactions prior to a blocking request

The provisions of Section 68 (2), (5) and (6) ZaDiG 2018 are waived. If an unauthorised transaction prior to a blocking request, which is not a payment transaction, is based on the use of a lost, stolen or otherwise missing identification or security medium, or on any other form of misuse of the aforementioned, the Customer shall be liable for the losses consequently incurred by the Bank if the Subscriber is responsible for their identification or security medium being lost, stolen or otherwise missing, or otherwise misused. The Customer shall also be liable ~~if they neglect~~in the event of failing to select ~~one of their~~an appointed ~~Subscribers~~Subscriber with due care and/or ~~if they fail~~of failing to regularly verify that the Subscriber ~~is fulfilling its~~ fulfils the obligations ~~in accordance~~

withunder these terms and conditions.Conditions. If the Bank contributed to the generation of a loss due to culpable con- ductconduct, the degreesdegree to which the loss must be borne by both the Customer and by the Bank areis determined on the basis of, the principles of contributory negligence.

11.2.311.2.3. Liability of the Bank subsequent toafter a blocking request is made

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

12. Waiver of Articles 9, 10 ECG

12. Waiver of the discretionary provisions of the E-Commerce Act and ZaDiG 2018

The provisions of the Articlessections 9 and 10 of the ECG (Austrian E-– Commerce Act (ECG) are hereby waived.

The following provisions of the Austrian Payment Services Act (ZaDiG) 2018 do not form an integral part of the contract for the Customer: the provisions of the third main section of ZaDiG 2018 as well as sections 32-54 [information requirements], Section 56 (1) [prohibition against charging fees for the fulfilment of information requirements or for corrective and safeguarding measures], Section 58 (3) [withdrawal of authorisation], Section 66 (1) and (3) [proof of authentication and execution of payment transactions], Section 68 (2),(5) and (6) [liability for unauthorised payment transactions], Section 70 (1) and (3) [refunds for a payment transaction initiated by the payee] and Section 80 [payment service providers' liability for non-execution, defective or late execution of payment transactions].

In Section 68 (1), the words "up to the amount of EUR 50" shall not apply to entrepreneurs.

13. Final provisions

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

Annexes:

Annex 1a: EBICS interface

Annex 1b: Specification for the EBICS interface

Annex 1c: Security requirements for the EBICS customer system

Annex 2: Not currently in use Annex

Annex 3: Data format specification

Annex 1a: EBICS interface

If an unauthorised transaction prior to a blocking request which is not a payment transaction is based on the use of a lost, stolen or otherwise missing identification or security medium or on any other form of misuse of the aforementioned, the Customer shall be liable for the losses consequently incurred by the Bank if the Subscriber is responsible for their identification or security medium being

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 the EBICS interface:

- Electronic signatures
- Authentication signature

- Encryption

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

~~1.1~~1.1. Electronic signatures

~~1.1.1~~1.1.1. Electronic signatures of the Subscribers

The following signature classes are defined for the electronic signatures (ESs) of ~~the Subscribers:~~Subscribers (which do not represent qualified signatures within the meaning of the Signature and Trust Services Act [SVG]):

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

Electronic signatures of the types "E", "A" or "B" are described as bank-technical ESs and are used for the authorisation of orders. Orders may require several bank-technical ESs to be applied by different Users (account holders and their authorised account representatives). For each order type supported, a minimum number of bank-technical 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~~Subscribers" (see ~~section~~Section 2.2) may only be assigned an ES of type "T".

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

~~1.2~~1.2. Authentication signature

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

~~The authentication signature may also be rendered using the photoTAN procedure in the technical environment of the Bank or that of an authorised service provider. They carry out the necessary verification for the Customer.~~

~~1.3~~1.3. Encryption

To ensure the secrecy of banking data on the application level, the order data ~~must~~shall be encrypted in accordance with the specification for the EBICS interface (cf. Annex 1b) by the

Customer, who must also take into account the current validity and authenticity of the credit institution's saved public keys.

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

2. Initialisation of the EBICS interface

~~2.1~~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 with the credit institution.

For initialising the EBICS interface, 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~~Technical Subscribers)
- Further specific details on Customer and Subscriber authorisations

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

~~2.2~~2.2. Initialisation of the keys

~~2.2.1~~2.2.1. First initialisation of the Subscriber keys

The key pairs used by the Subscriber for the bank-technical ES, the encryption of the order data and the authentication signature shall, in addition to the general conditions described in ~~section~~Section 1, comply with the following requirements:

~~1.~~(1) The key pairs ~~must~~shall be signed exclusively and unambiguously to the Subscriber.

~~2.~~(2) If the Subscriber generates the keys, the private keys ~~must~~shall be generated by means ~~which the Subscriber~~that can ~~keep~~be kept solely under ~~his/her sole~~the Subscriber's control.

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

~~4.~~(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.~~(5) With respect to the private keys used to protect the data exchange, each Subscriber shall define a password for each key which protects access to the respective private key. ~~The photoTAN may be used by the Participant instead of a password if the security medium of the Subscriber is saved by the Bank in a technical environment that is protected against unauthorised access.~~ Further, the 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~~Subscribers shall transmit their public keys to the credit institution via two independent communication channels:

- via the EBICS interface by means of the order types provided by the system for this procedure, and
- via an initialisation letter signed by the account holder or an authorised account representative.

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

The initialisation letter shall contain the following data for each public subscriber key:

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

The credit institution ~~will~~shall verify the signature of the account holder or authorised account representative on the initialisation letter and also whether the hash values of the ~~subscriber's~~Subscriber's public key transmitted via EBICS are identical to those transmitted in writing. If the verification is positive, the credit institution ~~will~~shall 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 bank-technical ESs. The separate transmission of a signed initialisation letter may be omitted.~~

~~2.3~~2.3. Initialisation of the bank keys

The Subscriber ~~will~~shall 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~~communicated 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~~communicated by the credit institution.

3. ~~3.~~ Placing orders with the Bank

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

~~The authorisation of orders may also be granted by entering the photoTAN shown on the mobile or a reading device and the electronic signature will be subsequently generated in the secure technical environment.~~

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

~~1.~~(1) All required bank-technical electronic signatures ~~will~~shall be transmitted together with the order data.

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

~~3.~~(3) If the Customer and the Bank agree that order data submitted by means of remote data transmission may be authorised by means of a separately transmitted accompanying document, a transport signature (type "T") ~~must~~shall be supplied for technical protection of the order data instead of the User´s bank-technical ES. To this end, the file ~~must~~shall 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 document.

~~3.1~~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.

~~In the case of a distributed electronic signature, the approval and thus the authorisation by means of the second banking signature may take place by using the photoTAN or by authorising an order using the app provided by the Bank.~~

Until all bank-technical 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~~Section 8 of the Terms and Conditions for Remote Data Transmission can be made.~~-~~

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

~~3.2~~3.2. Verification of identification by the Bank

An incoming order is executed by the Bank only after the necessary bank-~~-~~technical ES(s) or the signed accompanying document ~~has~~have been received and positively verified.

~~3.3~~3.3. Customer protocols

The Bank ~~will~~shall 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 shall keep informed ~~on~~of the result of the verifications carried out by the credit institution by ~~downloading~~promptly calling up the customer protocol ~~without undue delay~~.

The Subscriber shall include this protocol, the contents of which correspond to the provisions of ~~section~~Section 10 of Annex 1b in their 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~~shall transmit the new public keys to the Bank in good time prior to the expiry date of such validity period. After the expiry date of the old keys, a new initialisation ~~must~~shall be made.

If the Subscriber generates keys ~~himself~~, the subscriber keys ~~must~~shall 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~~Update of the public bank-technical key (PUB)

~~and~~

- ~~update~~Update of the public authentication key and the public encryption key (HCA) ~~or alternatively~~
- ~~update~~Update of all three above-~~-~~mentioned keys (HCS~~).~~)

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

If the electronic signature could not be

~~suspension of the identification and security media outside the remote data transmission procedure via the suspension facility separately notified by the Bank.~~

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

~~Annex 1b: Specification for the EBICS interface~~

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

~~Annex 1c: Security requirements for the EBICS customer system~~

positively verified, the provisions described in ~~section~~Section 7 ~~subsection~~para. 3 of the Terms and 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~~shall be placed again using the new key.

5. ~~Suspension~~Blocking of ~~the Subscriber~~subscriber keys

If misuse of ~~the~~ subscriber keys is suspected, the Subscriber ~~must suspend~~shall block 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~~block access authorisation via the EBICS interface. If a message with order type “SPR” is sent, access ~~will~~shall be ~~suspended~~blocked for the relevant Subscriber whose user ID was used to send the message. After ~~suspension~~blocking, the Subscriber can place no further orders via the EBICS interface until the access has been initialised again as described in ~~section~~Section 2.

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

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

Annex 1b: Specification for the EBICS interface

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

Annex 1c: Security requirements for the EBICS customer system

In addition to the security measures described in Annex 1a ~~section~~Section 5, the Customer ~~must~~shall observe the following requirements:

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

The Customer ~~is exclusively responsible~~bears sole responsibility for ~~the implementation of~~implementing these requirements.

Annex ~~2.~~2c: Not currently in use

Annex 3~~.~~: Data format specification

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