Terms and Conditions for Electronic Data Transmission

Deutsche Bank
Aktiengesellschaft

Version: valid from 01. July 2018

The following Terms and Conditions for Electronic Data Transmission (EDT) apply to customers of Deutsche Bank AG (hereinafter referred to collectively as "Deutsche Bank").

1 Scope of services

(1) Deutsche Bank is available to its Customers (according to Clause 15 account holders and/or Customer Affiliate(s)), not being a consumer, for electronic data interchange, hereinafter referred to as "electronic data interchange" or "EDT". EDT comprises submission and retrieval of files (especially transmission of orders and download information). According to Clause 14 II Deutsche Bank is hereby authorised to forward orders and transmit orders for processing to its appropriate branch, subsidiary bank, or branch of the subsidiary bank, where the relevant account/s is/are held (account maintaining unit).

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

(3) EDT is available via the EBICS interface (Annexes 1a to 1c).

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

(5) Accounts held at a financial institution which does not belong to Deutsche Bank (third-party bank) can only be admitted to the EDT Service if Deutsche Bank receives sufficient written confirmation from the third-party bank that the Customer (i) has authorised the third-party bank, on the basis of respective account agreement(s) with the third-party bank, to carry out instructions forwarded by Deutsche Bank in accordance with the Terms and Conditions for Electronic Data Transmission and (ii) has concluded a separate agreement with the third-party bank in order to ensure that Deutsche Bank receives the account information for the account in question.

2 Users and participants, identification and security media

(1) Orders can only be placed by the Customer or its authorised agents, via the EBICS interface. The Customer and authorised agents are hereinafter collectively named "Users". To place orders within Deutsche Bank, each User requires individual identification media which must be activated by Deutsche Bank. The requirements for the identification media are defined in Annex 1a. If agreed with Deutsche Bank, orders transmitted by EDT can be authorised with a signed accompanying note.

(2) In addition to its authorised representatives, the Customer may designate "technical subscribers" who are solely authorised to exchange data via the EBICS interface. Users and technical subscribers are hereinafter collectively referred to as "Subscribers". To protect the data exchange, each Subscriber requires individual security media which must be activated by Deutsche Bank. The requirements for the security media are described in Annex 1a.

3 Procedural provisions

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

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

(3) The data files are assigned according to the assignment and control; guidelines for the format used (Appendix 3).

(4) The User must correctly state the customer identifier of the payee or the payer according to the relevant conditions.

The payment service providers involved in the settlement of the payment order are authorised to process the transaction exclusively on the basis of the the customer identifier. Any damages or losses which may arise therefrom shall be borne by the Customer.

(5) Prior to the transmission of the order data to Deutsche 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 of 30 calendar days from the date of execution as specified in the file (credit transfer) or the maturity date (direct debit) or in the case of multiple dates, the latest date in such form that it can be made available to Deutsche Bank again at short notice on request, unless otherwise agreed.

(6) In addition, the Customer must generate an electronic protocol for each submission and each retrieval of files according to section 10 of the EBICS specification link (Annex 1b) and must file this protocol with its documents and make them available to Deutsche Bank upon request.

(7) To the extent Deutsche 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 specifically marked.

(8) As agreed with Deutsche Bank, order data transferred via EDT is to be authorised either by an electronic signature or by a signed accompanying note. Such order data shall be effective as an order

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

or

b) for data submitted with an accompanying note:
   - if Deutsche Bank has received the accompanying note within the agreed period of time and
   - if the accompanying note has been signed in the appropriate manner.

003 44444 66 DBEN 1189 DFÜ IFC I 180426

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

(1) Depending on the transmission procedure agreed with Deutsche Bank, the Customer is obliged to ensure that all Users comply with the legitimation procedures described in Annex 1a.

(2) The User may place orders by means of the legitimation media activated by Deutsche Bank. The Customer shall ensure that all Users take precautions that no third party obtains possession of the User's legitimation 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 – particular to keep the legitimation media secret:

- the data legitimising the User shall be kept secure and protected against unauthorized access,
- the password protecting the legitimation medium may not be written down or stored electronically, and
- when entering the password, case must be taken to ensure that no other persons can steal it.

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

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

Subscribers shall secure the data exchange by means of the security media activated by Deutsche 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 to 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.

6 Suspension of legitimation and security media

(1) If the legitimation or security media are lost, become known to third parties or misuse of such media is suspected, the Subscriber must immediately suspend EDT access or request Deutsche Bank to suspend the EDT access. Further details are stipulated in Annex 1a. The Subscribers can send Deutsche Bank a blocking notice at any time, using the contact details supplied separately if necessary.

(2) Outside the EDT process, the Customer may request suspension of a Subscriber's legitimation and security media or the entire EDT access via the suspension facility provided by Deutsche Bank.

(3) Deutsche Bank will suspend the entire EDT access, if there is reason to suspect that EDT access has been misused. Deutsche Bank will inform the Customer accordingly outside the EDT process. This suspension cannot be lifted using EDT technology.

7 Processing of incoming order data by Deutsche Bank

(1) The order data transmitted to Deutsche Bank by EDT are processed during the normal course of work.

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

(3) Deutsche Bank will verify the legitimation if the User(s) and the authorisation of the order data transmitted by the EDT on the basis of the electronic signatures produced by the User(s) within the legitimation media or the accompanying supporting note and shall check the correspondence between the order records and the provisions contained in Annex 3. If this verification reveals any discrepancies, Deutsche Bank will not process the affected order data and will notify the Customer thereof immediately. Deutsche Bank is entitled to delete order data not fully authorised after expiry of the time limit that is separately indicated by Deutsche Bank.

(4) If errors are revealed by Deutsche Bank's verification of files or data records, Deutsche Bank will provide proof of the errors in the files or data records in a suitable form and notify the User thereof immediately. Deutsche 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) Deutsche Bank shall be obliged to document these procedures (see Appendix 1a) and the forwarding of the orders for processing in the Customer protocol. The Customer in turn shall be obliged to retrieve the Customer report promptly and to keep himself/herself informed of the processing of the order. In the event of any discrepancies, the Customer should contact Deutsche Bank.

(6) Special features applicable to urgent payments: For accounts under this Agreement, in accordance with the provisions of this paragraph, the bank will execute both euro-denominated domestic payment orders and foreign payment orders as "urgent" provided these are marked by the business transaction code used for urgent orders and have an electronic signature. The same applies to regional holidays, i.e. holidays that are not TARGET holidays. For euro-denominated foreign payment orders, special configuration guidelines are outlined in Appendix 3, Specifications of data formats. The Customer is obliged to retrieve the report on the urgent payment orders directly after they have been issued.

Provided Deutsche Bank has received properly issued urgent domestic payment orders by 2 p.m., the bank will arrange for same-day settlement and forwarding to the Deutsche Bundesbank Target2 clearing system with specification of same-day value. If Deutsche Bank receives such orders between 2 p.m. and 4.30 p.m., it will endeavour to carry out transmission with same-day value dates. In accordance with our Deutsche Bundesbank cut-off times for same-day processing via its Target2 clearing system, as of October 2008, all orders issued after 4.30 p.m. will not be processed until the following business day.

Provided the bank has received properly issued urgent foreign payment orders by 3.30 p.m., the bank will arrange

003 44444 66 DBEN 1189 DFÜ IFC I 180426

for same-day settlement and forwarding to the Deutsche Bundesbank Target2 clearing system with specification of same-day value. If the bank receives such orders between 3.31 p.m. and 4.30 p.m., it will endeavour to carry out transmission with same-day value dates, although this can no longer be assured. Euro-denominated urgent payments that the bank receives after 4.30 p.m. will not be executed until the following business day. In each case, the pre-requisite being that the payee's bank clearing system is open and that the payee's bank is connected to an open clearing system. If these criteria are not met, the bank can process the payment at its own discretion using the DTAZV format "SWIFT urgent" payment type.

The bank will settle urgent domestic payment orders and urgent foreign payment orders in euro as individual transactions.

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 changes by recalling the whole file and placing the order again. Deutsche Bank can only accept a withdrawal if it is received in good time so that it can be taken into account in the course of the normal working procedures.

(2) The extent to which an order can be recalled depends on the relevant special conditions (for example Corporate Customer Terms and Conditions for Payment Transactions)- or if agreed with the account holder, according to the specifications in the Section 11 of Annex 3. Orders can only be recalled outside the EDT process. To do this, the Customer must inform Deutsche Bank of the individual details of the original order.

(3) In addition to Clause 8 (1) and (2) above a recall-request as well a recall as a revocation-request can be electronically sent to Deutsche Bank in connection with the EDT process in a way of using the respective Order Type identifier. Status information regarding submitted recall-requests and revocation-requests can also be electronically delivered by a way of the relevant Order Type Identifier.

9 Processing orders

(1) Deutsche Bank will process the orders if all the following requirements for processing have been fulfilled:

- the order data transmitted by EDT has been authorised in accordance with Clause 3 (8),
- the defined data format must be complied with,
- the credit limit must not be exceeded,
- the processing requirements according to the special criteria in relation to the relevant order type are met (e.g. sufficient funds according to terms for Corporate Customer Terms and Conditions for Payment Transactions).

(2) If the conditions for processing outlined in sub-section 1 above are not fulfilled, Deutsche Bank will not process the order and will notify the Customer hereof immediately through the agreed communication channel. As far as possible, Deutsche Bank will notify the Customer of the reasons and errors which caused the order not to be processes and the possible ways to correct these errors.

10 Security of the Customer's system

The Customer shall ensure that the systems used for the EDT are equally protected. The security requirements that are applicable relating to the EBICS process are described in Annex 1c.

11 Liability

11.1 The Bank's liability for an unauthorised EDT transaction and an unprocessed, incorrectly or lately processed EDT transaction

Deutsche Bank's liability for an unauthorised and for an unprocessed, incorrectly or lately processed transaction depends on the special conditions agreed for the respective order type (for example Corporate Customer Terms and Conditions for Payment Transactions).

11.2 Customer's liability for misuse of the legitimation or security media

11.2.1 Liability of the Customer for unauthorised payment transactions prior to the suspension notice

(1) If unauthorised payment transactions are processed prior to the suspension notice due to a misuse of a legitimation or security media, without having been lost, stolen or otherwise mislaid the account holder shall be liable for the damages incurred by Deutsche Bank as a result from the Subscriber's willful misconduct or negligence of its obligation to exercise due care and conduct obligations. § 675 German Civil Code shall not apply.

(2) The account holder is not obliged to pay compensation for damage according to Clause 11.2.1 (1) above if the Subscriber was unable to issue the suspension notice according to Clause 6 (1) has not secured the possibility of receiving the suspension notice, which is how the damage could have been prevented.

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

(4) Clauses 11.2.1 (2) and (3) shall not apply if the Subscriber acted with fraudulent intent.

11.2.2 Liability of the Customer for other unauthorised transactions before a request to 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, theft, other mislaying or other misuse of the identification or security medium. If Deutsche Bank contributed to the occurrence of a loss through any fault of its own, the principled of contributory negligence shall determine the extent to which Deutsche Bank and the Customer are liable.

11.2.3 Liability of the Bank following the suspension notice

As soon as Deutsche 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 EDT transactions. This shall not apply if a Subscriber has acted fraudulently.

003 44444 66 DBEN 1189 DFÜ IFC I 180426

11.3 Disclaimer
Liability claims are excluded if the circumstances giving rise to a claim are based on an unusual and unforeseeable event over which the party making the claim has no influence and the consequences of which could not have been avoided by it despite applying the necessary care.

12 Third-party banks; services from third parties
(1) If accounts held at third-party banks are covered by the EDT Service, the Customer will in each case conclude separate agreements with these third-party banks about the type and scope of the EDT Service.

(2) If one of the Parties makes recourse to services from third parties within the scope of the EDT service, it shall be liable to the other Party for all actions, errors or acts of omission by this third party to the same extent as if it had performed the actions itself or were itself responsible for the acts of omission. For the purposes of this Agreement, the third party shall be deemed to be acting on behalf of the Party that commissioned it.

13 Effective Date, Termination
(1) The EDT Agreement comes into force on the day the order is first processed by Deutsche Bank, whereupon the Customer's offer is being conclusively accepted. It shall have an indefinite term. Deutsche Bank shall inform the Customer if it declines to register an account or a User.

(2) Both, the Customer for itself and for each Customer Affiliate, and Deutsche Bank may terminate the EDT Agreement in whole by giving not less than thirty (30) calendar days' written notice to the other Party.

(3) Both, the Customer for itself and for each Customer Affiliate, and Deutsche Bank may terminate the EDT Agreement in whole with immediate effect, if reasonable cause arises which makes it unacceptable for the terminating party to continue the business relationship, even after having given due consideration to the legitimate concerns of the other Party.

(4) In accordance with Clause 13 (2) or (3), each Customer Affiliate, for itself or Deutsche Bank may terminate the EDT Agreement in relation to one or more Customer Affiliates (which should be named in the notice of termination).

14 Validity of Account Agreements with Units
(1) Except as expressly provided otherwise in this EDT Agreement, the agreements of the Customer and any Customer Affiliate with any account maintaining Unit shall remain in full force and effect and unaffected by this EDT Agreement.

(2) The Customer and each Customer Affiliate agrees and undertakes that each unit that is a branch, office or affiliate of Deutsche Bank (i) is authorised and instructed to process and execute all orders forwarded to it by Deutsche Bank, (ii) is entitled to treat such orders as if they had directly been forwarded to it such person acting on behalf of the Customer or such Customer Affiliate which is the account holder of the affected Account, (iii) may assume that such orders were duly given and authorised by the Customer or such Customer Affiliate respectively, (iv) is authorised to provide Deutsche Bank with all information relating to the accounts affected by these conditions, and (v) in consideration of it acting in reliance on (i) to (iv) above, is a beneficiary of the limitations on liability to, and indemnities from, the Customer and such Customer Affiliate pursuant to Clause 11 above.

15 Extension to Customer Affiliates; Appointment of Agent
(1) The extension of the EDT Service to any company belonging to the Customer's group of companies requires that company to accede to this EDT Agreement via separate Accession Agreement.

(2) Upon acceding to this EDT Agreement, such company becomes a "Customer Affiliate" under this EDT Agreement, and shall appoint the Customer as its agent to issue and receive all declarations and to perform all actions provided for in this EDT Agreement or considered by it to be necessary or useful in connection therewith. The Customer and the Customer Affiliate hereby warrant and represent to Deutsche Bank that, in connection with such appointment, the Customer and the Customer Affiliate have performed any acts, made any disclosures, and given any consents necessary to release the Customer from any restriction under any law against self-dealing or similar restrictions which would otherwise render its acting on behalf of a Customer Affiliate ineffective.

16 Governing Law; Submission to Jurisdiction
(1) This EDT Agreement shall be governed by and construed in accordance with German law.

(2) Place of jurisdiction for all legal action arising out of or in connection with this EDT Agreement shall be Frankfurt am Main, Germany. However, any legal action against a Party to this EDT Agreement may also be brought in the courts competent for such Party's place of domicile.

17 General
The Annexes mentioned in these Terms and Conditions are part of the EDT Agreement concluded with the Customer.
Annex 1a: EBICS Interface
Annex 1b: EBICS Specification
Annex 1c: Security requirements for the EBICS system
Annex 2: presently empty
Annex 3: Specification of the data formats

Annex 1a: EBICS Interface

1 Identification and security procedures
The Customer (account holder) shall inform the Bank of the Subscribers and their authorisations with respect to the EDT Service.

The following identification and security procedures are use for EBICS:
– Electronic signatures
– Authentication signature
– Encryption

For each identification and security procedure the Subscriber has an individual key pair which consists of a private and a public key. The public Subscriber keys shall be

003 44444 66 DBEN 1189 DFÜ IFC I 180426

disclosed to the Bank in accordance with the procedures described in section 2 below. The public Bank key must be protected against unauthorised alteration in accordance with the procedures described in section 2 below. The Subscriber's key may also be used for communication with other banks.

1.1 Electronic signatures

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

"E", "A" and "B" type electronic signatures are referred to as qualified electronic signatures. Qualified electronic signatures are used for the authorisation of orders. Orders may require several qualified electronic signatures to be applied by different Users (account holders and their Attorney). For each supported order type, a minimum of number of qualified electronic signatures shall be agreed between the Bank and the Customer.

Type "T" electronic signature are designed to transport signatures and cannot be used to authorize orders, but only for transmission of orders to the bank systems. "Technical Subscribers" (see section 2.2) can only be assigned a type "T" electronic signature.

The software used by the Customer can generate different messages (for example domestic and foreign payments orders, but also for messages concerning initialisation, reporting download and retrieval of account and transaction information, etc.) The Bank notifies the Customer of which message types can be used and which electronic signature type is to be used for this purpose.

1.2 Authentication signature
Unlike the electronic signature, which is used to authorize order data, the authentication signature only considers the control and login data of an individual EBICS message including the electronic signature contained therein. With the exception of a few system-related order types contained 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 1b), verifies the authentication signature of each EBICS message transferred by the Bank which takes into account the current validity and authenticity of the Bank's saved public key.

1.3 Encryption
To ensure the security of banking data on the application level, the data is to be encrypted by the Customer in accordance and on the basis of the validity and authenticity of the stored public key belonging to the Bank according to the EBICS Specification (see Annex 1b).

In addition, transport encryption must be utilised for the external transmission path 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 1b), the current validity and authenticity of the server certificates applied by the credit institution.

2 Initialisation of the EBICS interface

2.1 Registration of the communication interface
Communication is initialised by utilising a URL (Uniform Resource Locator). Alternatively, an IP address belonging to the relevant Bank may be used. The Customer will be informed of the URL or IP on conclusion of the EDT Agreement.

To enable the EBICS interface, the Bank shall provide the Subscribers designated by the Customer with the following data:
– URL or IP address of the Bank
– Name of the Bank
– Host ID
– Permitted version(s) of the EBICS protocol and security process
– Partner ID (Customer ID)
– User ID
– System ID (for technical Subscribers)
– Further specific details on Customer and Subscribers authorisations

For the Subscribers assigned to the Customer, the Bank will assign one User ID uniquely identifying it. In so far as one or more technical Subscribers are assigned to the Customer (multi-user system), the Bank will assign a system ID in addition to the User ID. If there are no technical Subscribers defined, the system ID and User ID are identical.

2.2 Initialisation of the Subscriber keys

In addition to the general conditions described in section 1 above, the pairs of keys used by the Subscribers for the qualified electronic signature, the encryption of the order data and the authentication signature must also meet 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 for protection of the data interchange, each User shall define a password for each key which protects access to the respective private key. It is possible to dispense with this

003 44444 66 DBEN 1189 DFÜ IFC I 180426

password if the Subscriber's security medium is stored in a technical environment protected against unauthorised access.

The Subscriber's public key needs to be transmitted to the Bank for the Subscriber's initialistion with the Bank. For this purpose the Subscriber shall transmit its public keys to the Bank via two independent communication channels:
– via EBICS by means of the relevant system related order types,
– via initialisation letter signed by the account holder or an authorised signatory.

For the Subscriber's initialisation, the Bank 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 the exponent length
– Hexadecimal form of the public key's exponent
– Specification of modulus length
– Hexadecimal form of the public key's modulus
– Hash value of the public key in hexadecimal form

The Bank will verify the signature of the account holder or Attorney 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 Bank will activate the relevant Subscriber for the agreed order types.

2.3 Initialisation of the bank keys
The Subscriber uses a specially provided system-specific order type to obtain the Bank's public key.

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

Prior to the first transmission via EBICS, the Subscriber shall verify the public bank keys sent by EDT by comparing their hash values with the hash values notified by the Bank via separately agreed communication channel.

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

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 verification 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 report.

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

1. All the necessary qualified electronic signatures are transmitted along with the order data.

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

3. If the Customer and the Bank agree that orders transferred via EDT 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 electronic signatures. To this end, this file must bear a special code (D-file) indicating that there are no further electronic signatures for this order other than the transport signature (type "T"). The orders are approved after successful verification of the signature of accompanying notes.

3.1 Placing orders by means of the distributed electronic signature (VEU)
The manner in which the distributed electronic signature (VEU) will be used by the Customer shall be agreed with the Bank.

Distributed Electronic Signature (VEU) shall be used where orders are to be authorised individually of the transport of the order data and, if applicable, by several Subscribers. Until all qualified electronic signatures 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 8 of the Terms and Conditions for EDT can be made.

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

3.2 Verification of identification by the Bank
An incoming order is executed by the Bank only after the necessary qualified electronic signature or the signed accompanying note has/ have been received and positively verified.

3.3 Customer reports
The Bank will document the following transactions in the Customers reports:
– Transmission of order data to the banking system.
– Transmission of information files from the banking system to the Customer system.
– Result of each verification of identification for orders from the Customer to the banking system.
– Further processing of orders if they concern the verification of signatures and the display of order data.

003 44444 66 DBEN 1189 DFÜ IFC I 180426

The Subscriber is obliged to keep informed on the result of the verifications carried out by the Bank by downloading the Customer report promptly.

The Subscriber shall include this report, the contents of which correspond to the provisions of section 10 of Annex 1b and submit it to the Bank upon 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 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 be made.

If the Subscriber generates its key 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 Bank. The keys must be transmitted in good time before expiration of the old keys. The following order types are to be used for an automatic activation of the new keys without renewed Subscriber initialisation:

- Update of public banking key (PUB)
- Update of public authentication key and the public encryption key (HCA)

or, alternatively,

- Update of all three above mentioned keys (the public bank-technical subscriber key, the public identification and authentication key and the public encryption key) (HCS).

The PUB and HCA or HCS order types are to be assigned a valid qualified electronic signature. 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 7 (3) of the Terms and Conditions for EDT is followed.

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

5 Suspension of Subscriber keys

If misuse of the Subscriber keys is suspected, the Subscriber must suspend the access authorisation for all baking systems using the compromised key(s). If the Subscriber has the 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 blocked 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 EDT process via the suspension facility separately provided by the Bank.

The Customer may request suspension of a Subscriber's identification and security media or of the entire EDT access via the suspension facility notified by the Bank.

003 44444 66 DBEN 1189 DFÜ IFC I 180426

Annex 1b: EBICS Specification

The specification is published on the website www.ebics.de.

Annex 1c: Security requirements for the EBICS system

In addition to the security measures described in Annex 1a item 5, the Customer must 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.
- 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 normal user and not as an administrator who is authorised, for instance, to carry out program installation.
- The internal IT communication channels for unencrypted banking data or for unencrypted EBICS messages must be protected against interception and manipulations.
- 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 implementation of these requirements is solely the responsibility of the Customer.

Annex 2: presently empty

Annex 3: Specification of the data formats

The specifications of the data formats are published on the website www.ebics.de.

003 44444 66 DBEN 1189 DFÜ IFC I 180426