Terms and Conditions for Electronic Data Transmission

Deutsche Bank
Aktiengesellschaft

Version valid from 18 November 2019

1 Scope of services

(1) Provided customers are not consumers, Deutsche Bank is available to said customers (according to Clause 15, account holders and/or customer affiliate(s)) for electronic data transmission, hereinafter referred to as "Electronic Data Transmission" or "EDT". EDT comprises the submission and retrieval of files (in particular the transmission of orders and accessing information). According to Clause 14 II, Deutsche Bank is hereby authorised to forward orders and transmit orders for processing to the appropriate branch, subsidiary bank, or branch of the subsidiary bank, where the relevant account(s) is/are held (unit maintaining the account).

(2) Deutsche Bank shall notify the customer of the types of services which the customer may use within the scope of EDT. The use of EDT is subject to the transaction 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 the transmission of orders and accessing information is stipulated in the Specifications for Data Formats (Annex 3).

(5) Accounts held at a financial institution that is not part of Deutsche Bank (third-party bank) may 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 the 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 subscribers, identification and security media

(1) Orders may only be placed by the customer or its authorised agents using the EBICS interface. The customer and authorised agents are hereinafter collectively referred to as "Users". To place orders within Deutsche Bank using an electronic signature, each User shall require individual identification media, which must be activated by Deutsche Bank. The requirements for identification media are specified in Annex 1a. If agreed with Deutsche Bank, orders transmitted by EDT may be authorised with a signed note accompanying the order.

(2) In addition to its authorised representatives, the customer may designate "technical subscribers" who are solely authorised to exchange data using the EBICS interface. Users and technical subscribers are hereinafter collectively referred to as "Subscribers". To protect data exchanges, each Subscriber shall require individual security media, which must be activated by Deutsche Bank. The requirements for security media are specified 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 Annex 1a as well as the requirements stipulated in the technical interface documentation (Annex 1b) and the data format specifications (Annex 3).

(2) The customer shall undertake to ensure that all Subscribers comply with the EDT procedures and specifications.

(3) Data fields are based on the assignment and control guidelines for the format used (Annex 3).

(4) Users shall correctly state the payee's or payer's customer ID pursuant 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 customer ID. Incorrect information may result in the order being misallocated. Any damages or losses which may arise as a result shall be borne by the customer.

(5) Prior to sending order data to Deutsche Bank, a record of the full contents of the files to be transmitted and of the data transmitted for verification of identification must be prepared. Unless otherwise agreed, such record must be kept by the customer for a minimum of 30 calendar days as of the date of execution as specified in the file (for credit transfers) or the due date (for direct debits) or, in the case of multiple dates, the latest date in such form that it may be made available to Deutsche Bank again at short notice on request.

(6) In addition, pursuant to Section 10 of the specifications for the EBICS interface (Annex 1b), the customer shall generate an electronic record of each submission and retrieval of files and must file this record, including its documentation, and shall provide the same to Deutsche Bank upon request.

(7) If and insofar as Deutsche Bank provides the customer with data on payment transactions which have yet to be conclusively processed, such data shall be considered merely non-binding information. Such data shall be specifically marked as such.

(8) As agreed with Deutsche Bank, order data sent via EDT shall be authorised either by virtue of an electronic signature or by a signed note accompanying the order. 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 electronic data transmission within the agreed period; and
   – if the electronic signatures can be successfully verified against the agreed keys;
   or

b) for data submitted with an accompanying note:
   – if Deutsche Bank has received the accompanying note within the period agreed; and
   – if the accompanying note has been duly signed.

003 44444 66 DBEN 1189 DFÜ IFC I 190919

4 Code of conduct and duties of care with respect to identification media used to authorise orders

(1) Depending on the transmission procedure agreed with Deutsche Bank, the customer shall undertake to ensure that all Users comply with the obligations arising from these Terms and Conditions and the identifications procedures specified in Annex 1a.

(2) Users may place orders using the identification media activated by Deutsche Bank. The customer shall ensure that all Users take precautions to ensure that no third party gains possession of the User's identification media or knowledge of the password protecting it. This is because any third party who has obtained possession of the identification media or a duplicate thereof may be capable of misusing the agreed services in conjunction with the corresponding password. In particular, Users must comply with the following in order to protect identification media and passwords:

– the identification media must be kept secure and protected against unauthorised access;
– Users are not permitted to write down the password protecting the identification media, nor are they permitted to store a copy of the legitimation media together with the password or store the password electronically in an unsecured manner;
– no duplicates of the identification media are permitted; and
– when entering the password, care must be taken to ensure that no other persons can determine the characters entered.

5 Code of conduct and duties of care when handling security media required for data exchange

With respect to the EBICS interface, the customer shall undertake to ensure that all Subscribers comply with the security procedures specified in Annex 1a.
Subscribers shall secure data exchanges using the security media activated by Deutsche Bank. The customer shall undertake to request that each User ensure that no third party gains possession of security media or is able to use the same. In cases of storage in a technical system in particular, the Subscriber's security media must be stored in a technical environment which is protected against unauthorised access. This is because any third person who gains access to security media or duplicates thereof may misuse the data exchange.

6 Security of the customer's system

The customer shall ensure that the systems it uses for EDT are sufficiently protected. The security requirements applicable to the EBICS process are specified in Annex 1c.

7 Suspension of identification and security media

(1) If identification or security media are lost, third parties gain knowledge of the same or misuse of such media is suspected, the Subscriber shall immediately suspend EDT access or request that Deutsche Bank suspend EDT access. Further details are specified in Annex 1a. Subscribers may send Deutsche Bank notice of suspension at any time using the contact details supplied separately.

(2) Beyond the EDT process, customers may request the suspension of a Subscriber's identification and security media or EDT access as a whole using the suspension option provided by Deutsche Bank.

(3) Deutsche Bank shall suspend EDT access as a whole if there is reason to suspect that EDT access has been misused. Deutsche Bank shall inform the Customer accordingly outside of the EDT process. Such suspension may not be lifted via EDT.

8 Processing of incoming order data by Deutsche Bank

(1) Order data transmitted to Deutsche Bank via EDT is processed during the normal course of work.

(2) On the basis of the signatures generated by Subscribers with their security media, Deutsche Bank shall verify whether the sender is authorised to perform the data exchange in question. Should such verification reveal any discrepancies, Deutsche Bank shall not process the order data in question and shall notify the customer immediately thereof.

(3) Deutsche Bank shall verify the User's or Users' identification and the authorisation of the order data transmitted via EDT on the basis of the electronic signatures produced by the User(s) within the identification media or the note accompanying the order and shall verify consistency between the order records and the provisions contained in Annex 3. Should such verification reveal any discrepancies, Deutsche Bank shall not process the order data in question and shall notify the customer immediately thereof. Deutsche Bank is entitled to erase order data not fully authorised upon the expiry of the period indicated separately by Deutsche Bank.

(4) If, pursuant to Annex 3, errors are identified through Deutsche Bank's verification of files or data records, Deutsche Bank shall provide proof of such errors in files or data records in a suitable format and shall notify the User immediately thereof. Deutsche Bank is authorised to exclude files or data records with errors from further processing if it is unable to ensure the proper execution of the order.

(5) Deutsche Bank shall undertake to document these procedures (see Annex 1a) and any forwarding of orders for processing in the customer log. The customer, in turn, shall undertake to promptly retrieve the customer log and ensure they are informed of the processing of the order. In the event of any discrepancies, customers should contact Deutsche Bank.

(6) Special features applicable to urgent payments: Pursuant to the provisions of this paragraph, Deutsche Bank shall execute both euro-denominated domestic payment orders and foreign payment orders as "urgent" for accounts covered by this Agreement, provided this is indicated by the business transaction code used for urgent orders and the orders have an electronic signature. The same shall apply to regional holidays, i.e. holidays that are not TARGET holidays. For euro-denominated foreign payment orders, special configuration guidelines are outlined in the data format specifications in Annex 3.
Customers shall undertake to retrieve reports on urgent payment orders immediately upon their issuance.

003 44444 66 DBEN 1189 DFÜ IFC I 190919

Provided Deutsche Bank has received properly issued urgent domestic payment orders by 2 pm, Deutsche Bank shall arrange for same-day settlement and forwarding to the Deutsche Bundesbank Target2 clearing system, specifying same-day value. If Deutsche Bank receives such orders between 2 pm and 4:30 pm, it shall endeavour to carry out transmission at same-day value. As of October 2008, in accordance with our Deutsche Bundesbank cut-off times for same-day processing via its Target2 clearing system, all orders issued after 4:30 pm shall not be processed until the following business day.
Provided Deutsche Bank has received properly issued urgent foreign payment orders by 3:30 pm, Deutsche Bank shall arrange for same-day settlement and forwarding to the clearing system of the payee's bank, specifying same-day value. If Deutsche Bank receives such orders between 3:31 pm and 4:30 pm, it shall endeavour to carry out transmission at same-day value, although this can no longer be guaranteed. Urgent euro-denominated payments received by Deutsche Bank after 4:30 pm shall not be executed until the following business day. In each case, execution requires that the payee's bank clearing system be open and that the payee's bank be connected to an open clearing system. If these criteria are not met, the bank may process the payment at its own discretion using the "SWIFT urgent" DTAZV format payment type.
Deutsche Bank shall settle urgent domestic payment orders and urgent foreign payment orders in euros as individual transactions.

9 Recall

(1) Customers are entitled to recall files before the order data is authorised. Individual order data may only be changed by recalling the entire file and placing the order again. Deutsche Bank is only able to accept a recall if it is received in good time such that the recall can be taken into account during the course of normal working procedures.

(2) The ability to cancel an order shall depend on the special conditions that apply to it (e.g. conditions for payment transactions). Pursuant to the specifications set out in Section 11 of Annex 3, orders may only be recalled outside of the EDT process if agreed with the account holder. To do so, the customer must inform Deutsche Bank of the individual details of the original order.

(3) In addition to Clause 8 Paragraphs 1 and 2, both a recall as well as a cancellation may be sent to Deutsche Bank electronically as part of the EDT process using the respective transaction code identifier. Information on the status of recall and cancellation requests submitted may also be provided electronically using the respective transaction code identifier.

10 Order execution

(1) Deutsche Bank shall execute orders if all the following requirements for execution have been fulfilled:
– The order data sent via EDT has been authorised in accordance with Clause 3 (8);
– The correct data format has been used;
– The credit limit has not been exceeded.
– The requirements for execution pursuant to any special criteria relating to the order type in question have been met (e.g. sufficient funds pursuant to the Terms and Conditions for Payment Transactions).

(2) If the conditions for executing the order as outlined in Paragraph 1 above are not met, Deutsche Bank shall not execute the order and shall notify the customer immediately thereof through the method of communication agreed. Where possible, Deutsche Bank shall notify the customer of the reasons and errors which caused the order not to be executed and any possible ways to correct such errors.

(3) If and insofar as SEPA instant credit transfers have been ordered via EDT and such transactions cannot be executed because the recipient bank is not available for SEPA instant credit transfers, Deutsche Bank and the customer hereby agree that such transactions be executed as SEPA transfers. The remitting bank shall be informed of this through a pain.002 message, which the bank shall provide for access by the customer via EDT. The customer and Deutsche Bank may agree separately that SEPA instant credit transfers in such cases not be converted to SEPA transfers and that such transfers simply be refused.

(4) If and insofar as SEPA instant credit transfers are ordered via EDT, the customer and Deutsche Bank hereby agree the following deviations from the Special Terms and Conditions for SEPA Instant Credit Transfers:

a) Depending on the number of transactions submitted, SEPA instant credit transfers may be processed within minutes instead of a few seconds.

b) Depending on the attributes of the EDT process, SEPA instant credit transfers may only be made using EBICS on TARGET business days (Mondays to Fridays, with the exception of 1 January, Good Friday, Easter Monday, 1 May, 25 and 26 December), provided a connection can be made to the bank's EBICS server. The acceptance times applicable to SEPA transfers shall apply to SEPA instant credit transfers.

c) If and insofar as a SEPA instant credit transfer is not accepted by the recipient bank for reasons other than those stated in Paragraph 3 and can ultimately not be executed, the provisions stipulated in Paragraph 2 shall apply.

11 Liability

11.1 Deutsche Bank's liability for unauthorised EDT transactions and unexecuted EDT transaction or EDT transactions executed incorrectly or late

Deutsche Bank's liability for unauthorised EDT transactions and unexecuted EDT transaction or EDT transactions executed incorrectly or late shall depend on the special conditions agreed for the order type in question (e.g. Terms and Conditions for Payment Transactions).

11.2 Customer's liability for misuse of identification or security media

11.2.1 Customer's liability for unauthorised payment transactions prior to notice of suspension

(1) If unauthorised payment transactions are processed prior to notice of suspension due to misuse of identification or security media where such media has not been lost, stolen or otherwise misplaced, the account holder

003 44444 66 DBEN 1189 DFÜ IFC I 190919

shall be liable for damages incurred by Deutsche Bank as a result of the Subscriber's wilful misconduct or neglect of its obligation to exercise due care and adhere to the code of conduct. Section 675v of the German Civil Code (Bürgerliches Gesetzbuch) shall not apply.

(2) The account holder is not obliged to pay compensation for damages pursuant to Paragraph 1 above if the Subscriber was unable to issue the notice of suspension pursuant to Clause 7 Paragraph 1 because Deutsche Bank had not ensured its ability to receive such notice of suspension, which would have prevented said damages.

(3) Liability for losses resulting during the period for which the credit limit applies shall be limited to the agreed credit limit.

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

11.2.2 Customer's liability for other unauthorised transactions prior to notice of suspension

If unauthorised transactions other than payment transactions result from the use of lost, stolen or otherwise missing identification or security media or any other misuse of such media prior to notice of suspension, the customer shall be liable for the resulting loss, theft, other misplacement or other misuse of the identification or security media. If Deutsche Bank contributed to the occurrence of such loss through any fault of its own, the statutory principles of contributory negligence shall determine the extent to which Deutsche Bank and the customer are liable.

11.2.3 Deutsche Bank's liability following notice of suspension

Once Deutsche Bank has received notice of suspension from a Subscriber, it shall accept any and all losses arising thereafter as a result of any unauthorised EDT transactions. This shall not apply if a Subscriber has acted with fraudulent intent.

11.3 Liability disclaimer

Liability claims shall be excluded if the circumstances giving rise to such claims are based on unusual and unforeseeable events over which the party making the claim has no influence and the consequences of which could not have been avoided by the same, despite taking all due care.

12 Third-party banks; third-party services

(1) If and insofar as accounts held with third-party banks are covered by the EDT service, the customer shall conclude separate agreements with such third-party banks in each case regarding the type and scope of the EDT service.

(2) If either Party relies on third-party services within the scope of the EDT service, it shall be liable to the respective other Party for any and all actions, errors or omission by said third party to the same extent as if it had performed said actions itself or were itself responsible for said acts of omission. For the purposes of this Agreement, such third party shall be deemed to be acting on behalf of the Party that commissioned it.

13 Term, termination

(1) The Agreement shall enter into force on the day the order is first processed by Deutsche Bank, whereupon the customer's offer is conclusively accepted. The Agreement is concluded for an indefinite period of time. Deutsche Bank shall inform the customer if it declines to register an account or a User.

(2) Both the customer – on its own behalf and on behalf of each customer affiliate – and Deutsche Bank may terminate the Agreement as a whole by giving not less than 30 calendar days' written notice to the respective other Party.

(3) Both the customer – on its own behalf and on behalf of each customer affiliate – and Deutsche Bank may terminate the Agreement as a whole with immediate effect for good cause which makes it unacceptable for the terminating party to continue the business relationship, even having given due consideration to the legitimate concerns of the respective other Party.

(4) Pursuant to Clause 13 Paragraphs 2 or 3, each customer affiliate may terminate the Agreement on its own behalf and for Deutsche Bank with respect to one or more customer affiliates (which should be specified in the notice of termination).

14 Validity of account agreements with units maintaining accounts

(1) Except as expressly stipulated otherwise in this Agreement, the agreements between the customer and any units maintaining accounts shall remain in full force and effect and shall remain unaffected by this Agreement.

(2) The customer agrees and shall ensure that each unit maintaining accounts 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 been forwarded to it directly by such persons acting on behalf of the customer as the holder of the account in question, (iii) may therefore assume that such orders were duly given and authorised by the customer and are binding for such branch, office or affiliate, (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 the provisions stipulated in (i) to (iv) above, is a beneficiary of the limitations on liability and indemnity claims as stipulated in Clause 11.

15 Extension to customer affiliates; appointment of a principle authorised agent

(1) The extension of the EDT service to any company belonging to the customer's group of companies shall require that company accede to this Agreement via a separate accession agreement.

(2) Upon acceding to this Agreement, such company shall become a "customer affiliate" under this Agreement, and shall appoint the customer as its principle authorised agent to issue and receive any and all statements and declarations and to perform all actions provided for in this Agreement or considered by it to be necessary or useful in connection therewith. The customer and customer af-

003 44444 66 DBEN 1189 DFÜ IFC I 190919

filiate hereby warrant to Deutsche Bank and ensure that, in connection with such appointment, the customer and customer affiliate have performed any acts, made any disclosures and given any consent 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 Applicable law

(1) These Terms and Conditions are subject to German law.

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

17 Final provision

The Annexes mentioned in these Terms and Conditions form part of the Agreement concluded with the customer.

Annex 1a: EBICS Interface

Annex 1b: EBICS Interface Specifications

Annex 1c: EBICS Customer System Security Requirements

Annex 2: presently empty

Annex 3: Data Format Specifications

Annex 1a: EBICS Interface

1 Identification and security procedures

The customer (account holder) shall inform Deutsche Bank of any Subscribers and their authorisations with respect to the EDT service.

The following identification and security procedures are used for EBICS:
– electronic signatures
– authentication signature
– encryption

For each identification and security procedure, the Subscriber has an individual key pair consisting of a private and a public key. The public Subscriber keys shall be disclosed to Deutsche Bank in accordance with the procedures stipulated in Section 2 below. The public bank key must be protected against unauthorised alteration in accordance with the procedures stipulated in Section 2 below. The Subscriber's key may also be used for communication with other banks.

1.1 Electronic signatures

1.1.1 Subscribers' electronic signatures

The following signature classes are defined for electronic signatures:
– individual signature (type "E")
– first signature (type "A")
– second signature (type "B")
– transport signature (type "T")

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

Type "T" electronic signatures are referred to as transport signatures and cannot be used to authorise orders. They serve only for the transmission of orders to bank systems. "Technical Subscribers" (see Section 2.2) may only be assigned a type "T" electronic signature.

The software used by the customer may generate different messages (e.g. domestic and foreign payment orders, but also messages concerning initialisation, report access and retrieval of account and transaction information, etc.) Deutsche Bank shall notify the customer of which message types may be used and which electronic signature type must be used for this purpose.

1.1.2 Authentication signature

Unlike electronic signatures used to authorise 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 specifications, authentication signatures must be supplied by both the customer's system and Deutsche Bank's bank

003 44444 66 DBEN 1189 DFÜ IFC I 190919

system in every transaction step. The customer shall ensure that software is used which verifies the authentication signature of each EBICS message sent by Deutsche Bank, taking into account the current validity and authenticity of Deutsche Bank's stored public key pursuant to the EBICS specifications (see Annex 1b)

1.2 Encryption

To ensure the confidentiality of banking data on the application level, order data shall be encrypted by the customer in accordance with and on the basis of the validity and authenticity of Deutsche Bank's stored public key pursuant to the EBICS specifications (see Annex 1b).

In addition, transport encryption must be used for the external transmission path between the customer's and Deutsche Bank's systems. Customers shall ensure the use of software that verifies the current validity and authenticity of the server certificates used by Deutsche Bank in accordance with the EBICS specifications (see Annex 1b).

2 Initialisation of the EBICS interface

2.1 Setting up the communication interface

Communication is done using a URL (uniform resource locator). Alternatively, an IP address belonging to the relevant bank may be used. Deutsche Bank shall inform the customer of the URL or IP address upon conclusion of the Agreement.

To enable the EBICS interface, Deutsche Bank shall provide Subscribers designated by the customer with the following data:
– the bank's URL or IP address
– 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 Subscriber authorisations

The Bank shall assign one User ID uniquely identifying the Subscriber assigned to the customer. If and insofar as one or more technical Subscribers are assigned to the customer (multi-user system), Deutsche Bank shall assign a system ID in addition to the User ID. If no technical Subscribers are defined, the system ID and User ID are identical.

2.2 Initialisation of Subscriber keys

In addition to the general terms and conditions stipulated in Section 1 above, the key pairs used by Subscribers for qualified electronic signatures, order data encryption and authentication signatures must also meet the following requirements:
1. 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 their sole control.
3. If keys are provided 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 exchange, each User shall define a password for each key which protects access to the respective private key. It is possible to dispense with this password if the Subscriber's security medium is stored in a technical environment protected against unauthorised access.

The Subscriber's public key must be transmitted to the banking system for the Subscriber's initialisation with Deutsche Bank. For this purpose, the Subscriber shall transmit its public keys to Deutsche Bank using two (2) independent methods of communication:
– via EBICS by means of the relevant system-related order types,
– via an initialisation letter signed by the account holder or an authorised signatory.

For the Subscriber's initialisation, Deutsche Bank shall verify the authenticity of the public Subscriber keys transmitted via EBICS using the initialisation letter signed by the account holder or an authorised signatory.

Said initialisation letter shall contain the following data for each public Subscriber key:
– purpose of the public Subscriber key
– electronic signature
– authentication signature
– encryption
– the specific 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 shall verify the signature of the account holder or authorised signatory on the initialisation letter and shall verify whether the hash values of the Subscriber's public key transmitted via EBICS are identical to those transmitted in writing. If said verification results in a positive outcome, Deutsche Bank shall approve the Subscriber in question for the agreed order types.

2.3 Initialisation of bank keys

The Subscriber shall use a system-specific order type provided specially to obtain Deutsche Bank's public key.

The hash value of the public bank key shall also be provided by Deutsche Bank using a second method of communication to be agreed separately with the customer.

Prior to the first use of EBICS, the Subscriber shall verify the public bank keys sent via EDT by comparing their hash values with the hash values provided by the Bank via a separately agreed method of communication.

The customer shall ensure that it uses software that verifies the validity of the server certificates used in connection with the transport encryption by means of a certification path separately provided by Deutsche Bank.

003 44444 66 DBEN 1189 DFÜ IFC I 190919

3 Special duties of care when generating identification and security media by the customer

If and insofar as the customer generates its identification and security media itself in accordance with the provisions stipulated in the EBICS specifications and initialises the same at its bank, it shall ensure the following:

– The confidentiality and integrity of the identification media must be ensured throughout all authentication stages, including display, transmission and storage.
– Private Subscriber keys may not be stored in plain text on identification and security media.
– The identification medium must be blocked after the fifth (5th) incorrect password attempt at the latest.
– Private and public Subscriber keys must be generated in a secure environment.
– Identification and security media must be exclusively and unambiguously assigned to and used by the Subscriber.

4 Placing orders with the bank

The User shall verify the accuracy of the order data and ensure that only verified data is signed electronically. Upon initialisation of communication, the bank shall first carry out Subscriber-related authorisation verifications, such as order type authorisation or verification of any agreed limits. The results of additional banking verifications, such as limit verifications or account authorisation verifications, shall later be notified to the Customer in the report. Orders transmitted to the bank's system may be authorised as follows:

1. All the necessary qualified electronic signatures are transmitted along with the order data.
2. If the distributed electronic signature has been agreed with the customer for the respective order type and the electronic signatures sent are insufficient for banking authorisation, the order shall be stored in the bank's system until such time as all electronic signatures required are provided.
3. If and insofar as the customer and the bank agree that orders sent via EDT may be authorised by virtue of notes accompanying the order sent separately, a transport signature (type "T") must be supplied for the technical protection of the order data in place of the User's qualified electronic signatures. To this end, this file must bear a special code indicating that there are no further electronic signatures for this order other than the transport signature (type "T"). Orders shall be approved upon successful verification of the signature of the User on the notes accompanying the order.

4.1 Placing orders using the distributed electronic signature (VEU)

The manner in which the distributed electronic signature is used by the customer shall be agreed with the bank.

Distributed electronic signatures shall be used where orders must be authorised individually of the transport of the order data and, where applicable, by several Subscribers.

Until such time as all qualified electronic signatures necessary for authorisation have been provided, the order may be erased by an authorised User. If the order has been fully authorised, only a recall pursuant to Section 9 of the Terms and Conditions for EDT may be made.

The bank is entitled to erase orders that have not been fully authorised upon the expiry of the deadline separately indicated by the bank.

4.2 Verification of identification by the Bank

Incoming orders sent via EDT shall be executed by the Bank only once the necessary qualified electronic signature(s) or the signed note accompanying the order has/have been received and positively verified.

4.3 Customer reports

Deutsche Bank shall document the following transactions in the customer's records:

– transmission of order data to the banking system
– transmission of information files from the bank's system to the customer's system
– result of each verification of identification for orders from the customer to the bank's system
– further processing of orders if they concern the verification of signatures and the display of order data

The Subscriber shall undertake to keep themselves informed regarding the outcome of verifications carried out by the bank by promptly downloading customer records.

The Subscriber shall include these records, the contents of which correspond to the provisions of Annex 1b Section 10, in its documentation and submit the same to the bank upon request.

5 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 shall transmit the new public keys to the bank in good time prior to the expiry of such period of validity. Upon expiry of the old keys, a new initialisation must be undertaken.

If the Subscriber generates its key itself, the Subscriber keys shall be renewed using the order types provided by the system for this purpose on the date agreed with the bank. The keys must be transmitted in good time prior to the expiry of the old keys.

The following order types shall be used to automatically activate new keys without renewed Subscriber initialisation:

– update of public banking key (PUB)

and

– update of public authentication key and the public encryption key (HCA)

or, alternatively,

– update of all three above-mentioned keys (HCS).

PUB and HCA or HCS order types shall be assigned a valid electronic signature for banking. After the keys have been successfully changed, only the new keys may be used.

If the electronic signature could not be positively verified, the provisions described in Section 8 Paragraph 3 of the Terms and Conditions for EDT shall be followed.

The key may only be changed once the processing of all orders has been completed. Otherwise, orders that have yet to be processed must be placed again using the new key.

003 44444 66 DBEN 1189 DFÜ IFC I 190919

6 Suspension of Subscriber keys

In the event of any suspicion of misuse of Subscriber keys, the Subscriber shall undertake to suspend access authorisation for all banking systems that uses the compromised key(s).

If the Subscriber is in possession of valid identification and security media, the Subscriber may suspend access authorisation via EBICS. If a message with order type "SPR" is sent, access shall be suspended for the relevant Subscriber whose User ID was used to send the message. After suspension, the Subscriber is unable to place any further orders via EBICS until such access has been re-initialised as specified in Section 2.

If the Subscriber is no longer in possession of valid identification and security media, the Subscriber may request suspension of identification and security media outside the EDT process via the suspension facility separately provided by Deutsche Bank.

The customer may request the suspension of a Subscriber's identification and security media or of EDT access as a whole via the suspension facility as provided by Deutsche Bank.

Annex 1b: EBICS Interface Specifications

These specifications are published online at www.ebics.org.

Annex 1c: EBICS Customer System Security Requirements

In addition to the security measures stipulated in Annex 1a Section 6, customers shall comply with the following requirements:

- The software used by the customer for the EBICS process shall comply with the requirements stipulated 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.
- A virus scanner must be installed and must be regularly updated, including with respect to virus definitions and/or files.
- The EBICS customer system must be configured such that the Subscriber must log in before the system can be used. Customers must login as normal users 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 manipulation.
- If updates relevant to security are available for the operating system in use or for other software relevant to security that may have been installed, such updates shall be installed on EBICS customer systems.

The implementation of these requirements is solely the responsibility of the customer.

Annex 2: presently empty

Annex 3: Data Format Specifications

These specifications are published online at www.ebics.org.

003 44444 66 DBEN 1189 DFÜ IFC I 190919