COMMERZBANK
The bank at your side

TERMS AND CONDITIONS

for Remote Data Transmission

Obsah

1. Scope of Services

(1) The Bank provides its Clients (Account Holders) with the option to transmit data using electronic remote data transmission means („remote data transmission“).

Remote data transmission includes data upload and download (particularly the transmission of orders and the download of information).

(2) The Bank notifies the Client of the types of services the Client may use in the framework of remote data transmission. The use of remote data transmission is subject to the disposal limits agreed with the Bank.

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

(4) The structure of data records and files for the transmission of orders and for the download of data is described in the Data Format Specifications (Annex 3), or it will be agreed separately.

2. Users and Participants, Identification and Security Media

(1) Orders may be placed via the EBICS interface only by the Client or by persons authorized by the Client to have access to the account.

The Client and the Client’s authorized persons with access to the account are referred to as „Users“. To authorize the transmission of an order by remote data transmission, every User needs an individual identification medium, which must be activated by the Bank.

The requirements for the identification medium are laid down in Annex 1a.

If agreed with the Bank, orders transmitted using remote data transmission may be authorized by means of a signed accompanying document/summary order.

(2) For the purposes of data exchange via EBICS, the Client may designate „Technical Participants“ in addition to authorized persons. Technical Participants must be natural persons who are only authorized to carry out the exchange of data.

Users and Technical Participants are jointly referred to as „Participants“. To protect the exchange of data, every Participant needs an individual security medium, which must be activated by the Bank. The requirements for the security medium are laid down in Annex 1a.

3. Procedural Requirements

(1) The transmission method agreed between the Client and the Bank is subject to the requirements defined in Annex 1a, in the documentation for the technical interface (Annex 1b), and in the Data Format Specifications (Annex 3).

(2) The Client must ensure that all Participants conform to the procedure and specifications for remote data transmission.

(3) The assignment of data fields is subject to the instructions for data entry and verification applicable to the relevant specific format (Annex 3).

(4) The User must specify the payee‘s or the payer’s identification code in accordance with the applicable Terms and Conditions.

Payment service providers taking part in the processing of a payment order may process a payment solely based on the account identification code.

Incorrect data may result in the erroneous processing of an order.

The Client is to bear the cost of any damage or loss caused in connection with the foregoing. This provision applies commensurately to the transmission of any other orders (other than payment orders) using remote data transmission.

(5) Prior to the transmission of an order to the Bank, a record showing the entire content of the files to be transmitted and of data transmitted must be prepared for identification purposes. The record must be kept by the Client for at least 30 calendar days after the date, as shown on the record, on which the record is made (transfers) or after the due date (direct debit) or, if several dates apply, after the latest applicable date, where the format of the record must allow the record to be provided to the Bank upon request immediately and repeatedly, unless otherwise agreed.

(6) In addition, the Client must generate an automatic record for every data transmission and data exchange with content conforming to Section 10 of the EBICS Interface Specifications (Annex 1b), must keep the record on file, and must make it available to the Bank upon request.

(7) Where applicable, information provided by the Bank to the Client regarding payment transactions that have not been fully processed is non-binding. Such information is specially designated.

(8) An order transmitted using remote data transmission must be authorized using either an electronic signature or a signed accompanying document/summary order, depending on the Client's arrangement with the Bank.

Such an order is a valid order for:

a) Data submitted with an electronic signature, provided that:

- All required electronic signatures of Users have been received using remote data transmission within the agreed period, and
- Electronic signatures can be successfully verified based on approved keys, or

b) Data submitted with an accompanying document/summary order, provided that:

- The Bank receives the accompanying document/summary order by the agreed deadline, and
- The accompanying document/summary order is signed in accordance with account authorizations.

4. Duties relating to Actions and Care pertaining to the Use of Identification Media for Order Authorization

(1) Based on the transmission procedure agreed with the Bank, the Client must ensure that all Users comply with the identification procedures described in Annex 1a.

(2) The User may submit orders using identification media activated by the Bank.

The Client must ensure that every User takes measures preventing any third party from gaining possession of the User's identification medium or knowledge of the password protecting the same, where third-party possession of the medium, or of a duplicate thereof, and the applicable password is liable to

allow a third party to commit fraud regarding the agreed services. The following main requirements must be observed to prevent the identification media from disclosure:

- Data identifying the User must be protected from unauthorized access and must be secured,
- The password protecting the identification medium must not be marked or stored unprotected in electronic devices, and
- Care must be taken in entering the password to ensure that no other person is able to gain access to the password.

5. Duties relating to Actions and Care pertaining to the Use of Security Media for Data Exchange

As regards communication via EBICS, the Client must ensure that all Participants comply with the security procedures described in Annex 1a.

Participants must carry out data exchange using a security medium activated by the Bank.

The Client must ensure that all Participants take measures preventing any third party from gaining possession of or being able to use the security medium. In particular, if the medium is kept in an IT system, the Participant's security medium must be stored in an environment that is protected against unauthorized access to prevent third-party access to the security medium, or a duplicate thereof, and any fraudulent exchange of data.

6. Suspension of Identification and Security Media

(1) If the identification or security medium is lost or disclosed to a third party, or if fraud involving the medium is suspected, the Participant must immediately request the Bank to suspend or block access to remote data transmission. See Annex 1a for further details.

The Participant can also request the Bank to suspend access at any time using separately provided contact data.

(2) In addition to suspending remote data transmission, the Client may request the suspension of the Participant's identification and security media, or the suspension of full access to remote data transmission using a device, which permits such suspension, provided by the Bank.

(3) If fraud involving the medium is suspected, the Bank will fully suspend access to remote data transmission, and will inform the Client of such suspension by means other than remote data transmission.

Such suspension cannot be cancelled using remote data transmission.

7. Processing of Incoming Order Data by the Bank

(1) Order data transmitted to the Bank using remote data transmission are processed using the Bank's standard procedures.

(2) Based on signatures generated by Participants using the security medium, the Bank verifies the sender's authorization to carry out data exchange.

If the verification process reveals any discrepancies, the Bank does not process the applicable order, and notifies the Client to that effect immediately.

(3) The Bank verifies the identity of the User(s) and the authorization of order data transmitted using remote data transmission based on electronic signatures generated by the Users using the identification medium, or based on a provided accompanying document/ summary order, and verifies that data records pertaining to order data are compliant with the requirements laid down in Annex 3.

If the verification process reveals any discrepancies, the Bank does not process the applicable order, and notifies the Client to that effect immediately.

The Bank may delete order data relating to an order that is not fully authorized after the expiry of a time limit separately specified by the Bank.

(4) If the Bank's verification of files or data records as per Annex 3 reveals errors, the Bank will provide evidence regarding such errors in such files or data records using a suitable form, and will inform the User to that effect immediately.

If unable to ensure the proper execution of an order, the Bank may exclude files or data records containing errors from further processing.

(5) The Bank must use a record to document the above procedures (see Annex 1a) and the transmission of orders for processing.

The Client must request the record and information on the status of processed orders without delay. In the event of discrepancies, the Client must contact the Bank.

8. Order Revocation

(1) The Client may revoke a transmitted file prior to the authorization of order data. Specific order data may only be changed by revoking the entire file and resubmitting the order. The Bank may only accept revocation if it is delivered at a time allowing it to be taken into account in the course of the standard work process.

(2) The extent to which an order may be recalled is subject to the applicable special conditions (such as the Terms and Conditions for Payment Services).

An order may be revoked by means other than remote data transmission and in accordance with the provisions of Section 11, Annex 3, if so agreed with the Client. In such a case, the Client must inform the Bank of the specific details stated in the original order.

9. Order Execution

(1) The Bank executes an order provided that all of the following order execution requirements have been fulfilled and complied with:

- Order data submitted using remote data transmission must be authorized in accordance with Section 3, Paragraph 8,
- The required data format must be complied with,
- The order limit must not be exceeded,
- Requirements for order execution must be complied with in accordance with the special conditions applicable to the relevant order type, and
- Order execution must not violate any other legal requirements.

(2) If the requirements for order execution laid down in Paragraph 1 are not complied with, the Bank will not execute the order and will inform the Client to that effect without delay, using the agreed communication channel. Wherever possible, the Bank will inform the Client of the reasons and errors due to which an order is not executed and of options available to correct such errors. The foregoing does not apply if the disclosure of the reasons were to violate the law.

10. Client's System Security

The Client must take appropriate measures to secure systems the Client uses for remote data transmission. The security requirements that apply to the EBICS process are laid down in Annex 1c..

11. Liability

11.1 Bank Liability for Unauthorized Orders and Orders Not Executed, Executed Incorrectly, or Executed Late
The Bank's liability for unauthorized orders and orders not executed, executed incorrectly, or executed late is subject to the special conditions agreed for a given order type (such as the Terms and Conditions for Payment Services).

11.2 Client Liability for Fraud Involving the Identification or Security Medium

11.2.1 Client Liability for Unauthorized Payment Transactions prior to a Blocking Request

(1) Liability in case that the Client is not a consumer. If an unauthorized payment transaction completed prior to a blocking request involves the misuse of the identification or security medium, the Client is liable for losses subsequently incurred by the Bank if the Participant acts negligently or deliberately and in doing so violates requirements pertaining to conduct and care.

11.2.2 Client Liability for Other Unauthorized Payment Transactions prior to a Blocking Request

If an unauthorized transaction, which is not a payment transaction, is completed prior to a blocking request based on the use of a lost or stolen identification or security medium or on any other form of fraud involving the identification or security medium, and if loss is consequently incurred by the Bank, the Client and the Bank are liable for the loss based on the principle of contributory negligence.

11.2.3 Bank Liability after a Blocking Request

The Bank is liable for any and all losses incurred due to unauthorized transactions effected after a blocking request is received from a Participant. The foregoing does not apply if a Participant acts with the intent to commit fraud.

11.3 Disclaimer of Liability
Claims relating to liability are excluded if the circumstances constituting the basis of a claim stem from an irregular or unforeseeable event, over which the party claiming such an event has no control and the consequences of which could not be prevented despite the use of due care and diligence.

12. Miscellaneous

The annexes referred to in these Terms and Conditions constitute a part of the agreement entered into with the Client.

Annexes:

Annex 1a: EBICS Interface

Annex 1b: EBICS Interface Specifications

Annex 1c: EBICS Client System Security Requirements

Annex 2: Currently not in use

Annex 3: Data Format Specifications

Annex 1a: EBICS Interface

1. Identification and Security Procedures

The Client (Account Holder) must inform the credit institution of Participants and their remote data transmission authorizations.

The following identification and security procedures are used for the EBICS interface:

- Electronic signatures,
- Authentication signature,
- Encryption.

For each identification and security process, the Participant has an individual key set, which consists of a private key and a public key.

The Participant's public keys may be provided to the credit institution using the procedure described in Section 2.

The Bank's public keys must be protected against unauthorized alteration using the procedure described in Section 2. The Participant's key set may also be used for communication with other credit institutions.

1.1 Electronic Signatures

1.1.1 Participant Electronic Signatures

The following signature classes are defined for Participant electronic signatures (ES):

- Single signature (Type „E"),
- First signature (Type „A"),
- Second signature (Type „B"),
- Transport signature (Type „T").

Electronic signatures typically used in banking are Type „E", „A", and „B" electronic signatures. Banking electronic signatures are used for the authorization of orders. Several banking electronic signatures of several Users may be required for the authorization of orders (Account Holder and persons authorized to use the account). A minimum number of required banking electronic signatures are agreed by the Client and the credit institution for each supported order type.

Type „T" electronic signatures are designated transport signatures that may not be used for order authorization; they may only be used for the transmission of orders to the Bank system. „Technical Participants" (see Section 2.2) may only be assigned a Type „T" electronic signature.

The program used by the Client is able to generate various messages (such as domestic and international payment orders as well as messages concerning initialization, record download, and account and turnover information). The credit institution informs the Client of message types that may be used and the electronic signature type that must be applied in specific cases.

1.2 Authentication Signature

Unlike the electronic signature, which is used to sign orders, the authentication signature is used for an individual EBICS message and is configured using verification and login data and electronic signatures contained therein. Save for several system-related order types, which are defined in the EBICS interface specifications, authentication signatures must be submitted by both the Client's system and the Bank's system during each step of a transaction. The Client must use software, which verifies authentication signatures in every EBICS message transmitted by the credit institution in conformity to the EBICS interface specifications (see Annex 1b), that takes into account the validity and authenticity of the credit institution's current public keys.

1.3 Encryption

To preserve the confidential nature of banking data at the application level, order data must be encrypted by the Client in accordance with the EBICS interface specifications (see Annex 1b). The Client must take into account the validity and authenticity of the credit institution's current public keys. In addition, transport encryption must be used for the external transmission paths between the Client's and the Bank's systems. The Client must use software that verifies, in accordance with the EBICS interface specifications (see Annex 1b), the current validity and authenticity of server certificates used by the credit institution.

2. EBICS Interface Initialization

2.1 Installation of Communication Interface

Communication is initialized using the URL (Uniform Resource Locator). Alternatively, the applicable credit institution's IP address may be used. The URL and the IP address are disclosed to the Client upon the entry into an agreement with the credit institution. For the purposes of EBICS interface initialization, the credit institution provides the following data to Participants designated by the Client:

- URL or IP address of the credit institution,
- Name of the credit institution,
- Host ID,
- Permitted version(s) of the EBICS protocol and security procedures,
- Partner ID (Client ID),
- User ID,
- System ID (for Technical Participants),
- Additional specific details on Client and Participant authorization.

The credit institution assigns one user ID that clearly identifies Participants assigned to the Client. Where one or more Technical Participants are assigned to the Client (multi-user system), the credit institution assigns a System ID in addition to the User ID. If no Technical Participant is defined, the System ID and the User ID are identical.

2.2 Initialization of Keys

2.2.1 First Initialization of Participant Keys

In addition to the general requirements laid down in Section 1, the key set used by the Participant for banking electronic signatures, order data encryption, and the authentication signature must meet the following requirements:

(1.) The key set must be assigned exclusively and unambiguously to the Participant.

(2.) If the keys are generated by the Participant, the private keys must be generated using a method that is under the Participant's sole control.

(3.) If the keys are made available by a third party, measures must be taken to ensure that the Participant is the sole recipient of the private keys.

(4.) As regards the private keys used for identification, every User must set a password for each key to protect access to the applicable private key.

(5.) As regards the private keys used to protect data exchange, every User must set a password for each key to protect access to the applicable private key. The use of a password as per the above is not mandatory if the Participant's security medium is stored in a technical device that is protected from unauthorized access.

The transmission of the Participant's public keys to the Bank system is necessary for the initialization of the Participant by the credit institution. For this purpose, the Participant

must transmit his/her public keys to the credit institution via two independent communication channels:

- The EBICS interface using the order types provided by the system for this process, and
- An initialization letter signed by the Account Holder or a person authorized to use the account.

To initialize the Participant, the credit institution verifies the authenticity of the Participant's public keys transmitted via EBICS based on initialization letters signed by the Account Holder or a person authorized to use the account.

The initialization letter must contain the following information for each of the Participant's public keys:

- Purpose of the Participant's public key,
- Electronic signature,
- Authentication signature,
- Encryption,
- The applicable version for each key set,
- Specification of the exponent length,
- Hexadecimal record of the public key exponent,
- Specification of modulus length,
- Hexadecimal record of the public key modulus,
- Hexadecimal record of the public key hash value.

The credit institution verifies the signature of the Account Holder or the person authorized to use the account in the initialization letter and ensures that the hash values of the Participant's public key transmitted via EBICS match values transmitted in writing. If the verification is positive, the credit institution activates the relevant Participant for the agreed order types.

2.3 Initialization of Bank Keys

The Participant downloads the credit institution's public key with the order type specifically provided by the system for this purpose. The hash value of the Bank's public key will be subsequently made available by the credit institution via a second communication channel separately agreed with the Client. Prior to the first data transmission via EBICS, the Participant must verify the authenticity of the Bank's public keys sent using remote data transmission by comparing their hash values with the hash values provided by the credit institution via the separately agreed communication channel. The Client must ensure the use of software that verifies the validity of server certificates used in connection with transport encryption by means of a certification path provided separately by the credit institution.

3. Submission of Orders to the Bank

The User must verify the accuracy of order data and ensure that only verified data are signed electronically. After the initialization of communication, the Bank first verifies the Participant's authorizations, such as order type authorization and the verification of agreed limits. The results of the Bank's further verifications, such as limit verification or the verification of the right to use the account, will be reported to the Client at a later time in the Client record. Orders transmitted to the Bank system may be authorized as follows:

(1.) All necessary banking electronic signatures are transmitted together with order data.

(2.) If a distributed electronic signature is agreed with the Client for a given order type and transmitted electronic signatures are insufficient for the Bank's authorization, the applicable order is stored in the Bank system until all required electronic signatures are applied.

(3.) If the Client and the Bank agree that orders and order data submitted using remote data transmission may be authorized by means of separately transmitted accompanying document/summary order, a transport signature (Type „T“) must be supplied for the purpose of protecting order data by technical means instead of the User‘s banking electronic signature. For this purpose, the file must contain a special code indicating that no electronic signatures exist for such an order other than the transport signature (type „T“). The order is authorized after the credit institution successfully verifies the User’s signature on the accompanying document/summary order.

3.1 Submission of Orders using the Distributed Electronic Signature
The procedure for the use of the distributed electronic signature by the Client is agreed with the credit institution. The distributed electronic signature is used where orders are to be authorized independently of the transmission of order data, if possible by several Participants. An order may be deleted by an authorized User before all banking electronic signatures necessary for authorization are applied. Once an order is fully authorized, only revocation as per Section 8 of the Terms and Conditions for Remote Data Transmission is allowable. After the expiration of the applicable time limit announced by the Bank, the Bank may delete orders that have not been fully authorized.

3.2 Verification of Identification by the Bank
An incoming order is executed by the Bank after the required banking electronic signature or signed accompanying document/summary order is received and undergoes positive verification.

3.3 Client Record
The Bank uses Client records to document the following transactions:

- Transmission of order data to the Bank system,
- Transmission of information files from the Bank system to the Client‘s system,
- Result of all identification verifications for orders transmitted by the Client to the Bank system,
- Further processing of orders concerning the verification of signatures and the display of order data.

The Participant must acknowledge information on the outcome of verifications carried out by the credit institution by downloading the Client record immediately. The Participant must include the foregoing record, the contents of which correspond to the provisions of Section 10 of Annex 1b, in his/her files and submit it to the credit institution upon request.

4. Change of the Participant Key with Automatic Activation

If the validity of the identification and security media used by the Participant is limited, the Participant must transmit new public keys to the Bank in a timely manner prior to the expiration date. New initialization must be carried out after the expiry date of the old keys. If the Participant‘s keys are generated by the Participant, the keys must be renewed using the order types provided by the system for this purpose on the date agreed with the credit institution. The keys must be submitted in a timely manner before the expiration of the old keys. The following order types are used for the automatic activation of new keys without renewed Participant initialization:

- Update of the public banking key (PUB),
- Update of the public authentication key and the public encryption key (HCA),
- Update of all of the three foregoing keys (HCS).

The User may supply a valid banking electronic signature for the PUB, HCA, and HCS order types. Once the keys are successfully changed, only the new keys may be used. If an electronic signature cannot be positively verified, the procedure described in Section 7, Paragraph 3 of the Conditions for Remote Data Transmission applies. The keys may be changed only after all orders have been completely processed. Otherwise, unprocessed orders must be resubmitted using the new key.

5. Suspension of Participant Keys

If fraud involving the use of the Participant's keys is suspected, the Participant must suspend access to all Bank systems using the compromised key(s). If the Participant is in possession of valid identification and security media, the Participant can suspend access via the EBICS interface. If a message with a Type „SPR" order is sent, access is suspended for the relevant Participant whose User ID is used to send the message. After suspension, the Participant can place no further orders via the EBICS interface until access is reinitialized in accordance with the procedure described in Section 2. If the Participant is no longer in possession of valid identification and security media, the Participant can request suspension of the identification and security media by means other than remote data transmission using a suspension facility provided by the Bank. Using means other than remote data transmission, the Client may request the suspension of a Participant's identification and security media, or the suspension of full access to remote data transmission using a suspension facility provided by the Bank.

COMMERZBANK
The bank at your side

Annex 1b: EBICS Interface Specifications

The specifications are posted on the Internet at http://www.ebics.com.

Annex 1c: EBICS Client System Security Requirements

In addition to the security measures described in Section 5 of Annex 1a, the Client must comply with the following requirements:

- The software used by the Client for the EBICS procedure must be compliant with the requirements laid down in Annex 1a.
- The EBICS Client system must not be used without a firewall. A firewall is an application that monitors all incoming and outgoing messages and only permits known or authorized communication.
- The Client must use an antivirus program, which must be regularly updated and must contain the most recent virus definitions.
- The EBICS Client system must be configured so as to require a Participant to log in as a regular user, as opposed to the administrator authorized to carry such tasks as software installation, before the system can be used.
- Internal IT communication channels for unencrypted banking data or for unencrypted EBICS messages must be protected against interception and misapplication.
- If security updates are available for the operating system currently in use or for other installed security-related software, such updates must be applied to the EBICS Client systems.

The Client is solely responsible for compliance with the foregoing requirements.

COMMERZBANK
The bank at your side

Annex 2:

Currently not in use

COMMERZBANK
The bank at your side

Annex 3: Data Format Specifications

The specifications are posted on the Internet at http://www.ebics.com.

Your Commerzbank branch:

Commerzbank Aktiengesellschaft

pobočka Praha
Jugoslávská 934/1, Vinohrady
120 00 Prague 2

Telephone: +420 221 193 111
Fax: +420 221 193 699

www.commerzbank.cz