HypoVereinsbank Member of UniCredit

ANNEXES TO THE TERMS AND CONDITIONS OF REMOTE DATA TRANSMISSION

valid from 14. September 2019

Annex 1a: EBICS connection
Annex 1b: Specification of EBICS connection (Please find the specification under www.ebics.de)
Annex 1c: Security requirements of the EBICS Customer system
Annex 2: currently not assigned
Annex 3: Specification of Data Formats (Please find the specification under www.ebics.de)

Note: The present translation is provided for the Customer's convenience only. The original German text of the Terms and conditions for Remote Data Transmission (»Bedingungen für Datenfernübertragung«) is binding in all respects. In the event of any divergence between the English and the German texts, constructions, meanings or interpretations, the german text, costruction, meaning or interpretation shall govern exclusively.

HypoVereinsbank Member of UniCredit

Further details on the bank are provided in the List of Prices and Services.

ANNEX 1A TO THE TERMS AND CONDITIONS OF REMOTE DATA TRANSMISSION

EBICS connection

1 Identification and security procedures

The Customer (Account Holder) shall indicate the RDT Participants and their authorisations to the Bank.

The following identification and security procedures shall be used for the EBICS connection:

– Electronic signatures
– Authentication signature
– Encryption

The Participant shall possess an individual pair of keys, consisting of a private key and a public key, for each identification and security procedure. The public Participant keys must be disclosed to the Bank in accordance with the procedure set out in Section 2. The public bank keys must be protected against unauthorised alteration in accordance with the procedure set out in Section 2. The Participant's key pairs may also be used for communication with other banks.

1.1 Electronic signatures

1.1.1 Electronic signatures of Participants

The following signature classes shall be defined for the electronic signatures (ESs) of Participants:

– Single signature (Type »E«)
– First signature (Type »A«)
– Second signature (Type »B«)
– Transport signature (Type »T«)

Type »E«, »A« or »B« ESs are referred to as »banking ESs«. Banking ESs are used to authorise orders. Orders may require several banking ESs which must be provided by different Users (Account Holders and their authorised representatives). For each order type supported, a minimum number of required banking ESs shall be agreed between the Bank and the Customer.

Type »T« ESs, which are called »transport signatures«, are not used for banking authorisation of orders, but solely for transmitting orders to the bank system. »Technical Participants« (see Section 2.2) may only be assigned a type »T« ES.

The programme used by the Customer can generate different messages (e.g. domestic and international payment orders, but also messages for initialisation, calling up protocols and retrieving account and turnover information, etc.). The Bank shall let the Customer know which types of message can be used and which type of ES must be applied in each case.

1.1.2 Authentication signature

In contrast to the ES, which is used to sign order data, the authentication signature is configured via the individual EBICS message including the control and login data and the ES contained therein. With the exception of a few system-determined order types defined in the EBICS Specification, the authentication signature is provided by both the Customer system and the bank system in every transaction step. The Customer must ensure the use of software which, in accordance with the EBICS Connection Specification (see Annex 1b), verifies the authentication signature of each EBICS message transmitted by the Bank, taking into account the current validity and authenticity of the Bank's stored public keys.

1.2 Encryption

In order to ensure the secrecy of the banking data at application level, the order data must be encrypted in accordance with the EBICS Connection Specification (see Annex 1b) by the Customer, taking into account the current validity and authenticity of the Bank's stored public keys.

In addition, transport encryption is required on the external transmission routes between the Customer and bank systems. The Customer must ensure the use of software which, in accordance with the requirements of the EBICS Connection Specification (see Annex 1b), verifies the current validity and authenticity of the server certificates used by the Bank for this purpose.

2 Initialisation of the EBICS connection

2.1 Establishing the communication link

Communication is established using a URL (Uniform Resource Locator). Alternatively, an IP address for the respective Bank may be used. The URL or IP address shall be disclosed to the Customer on conclusion of the agreement with the Bank.

To initialise the EBICS connection, the Bank shall provide the following data to the Participants named by the Customer:

– URL or IP address of the Bank
– Name of the Bank
– Host ID
– Permitted version(s) of the EBICS protocol and security procedures
– Partner ID (Customer ID)
– User ID
– System ID (for technical Participants)
– Further specific details of Customer and Participant authorisations.

For the Participants assigned to the Customer, the Bank shall issue a User ID which clearly identifies the Participant. If one or more technical Participants are assigned to the Customer (multi-User system), the Bank shall issue a system ID in addition to the User ID. If no technical Participant is specified, the system ID and User ID are identical.

2.2 Initialisation of keys

2.2.1 First initialisation of Participant keys

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

1. The key pairs are assigned exclusively and unambiguously to the Participant.
2. If the Participant generates their keys independently, the private keys must be generated by means which the Participant can keep under their sole control.
3. If the keys are made available by a third party, it must be ensured that the Participant obtains sole possession of the private keys.
4. As regards the private keys used for identification, each User shall define a password for each key which protects access to the respective private key.
5. As regards the private keys used to protect the data exchange, each Participant shall define a password for each key which protects access to the respective private key. This password may be dispensed with if the Participant's security medium is stored in a technical environment which is protected against unauthorised access.

Initialisation of the Participant by the Bank requires transmission of the Participant's public keys to the bank system. For this purpose, the Participant shall transmit their public keys to the Bank via two independent communication channels:

– via EBICS by means of the system-determined order types provided for this purpose.
– via an initialisation letter signed by the Account Holder or an authorised representative.

For initialisation of the Participant, the Bank shall verify the authenticity of the public Participant keys transmitted via EBICS on the basis of the initialisation letters signed by the Account Holder or an authorised representative.

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

– Purpose of the public key
– Electronic signature
– Authentication signature
– Encryption
– Version supported by each key pair
– Specification of exponent length
– Hexadecimal representation of the public key's exponent
– Specification of the modulus length
– Hexadecimal representation of the public key's modulus

– Hexadecimal representation of the public key's hash value
The Bank shall verify the signature of the Account Holder or authorised representative on the initialisation letter and whether the hash values of the Participant's public key transmitted via EBICS are identical with those transmitted in writing. If verification is positive, the Bank shall activate the relevant Participant for the agreed order types.

2.3 Initialisation of bank keys

The Participant shall collect the Bank's public key using a system-determined order type specifically designated for this purpose.
The hash value of the public bank key shall additionally be made available by the Bank via a second communication channel agreed separately with the Customer.
Before using EBICS for the first time, the Participant shall verify the authenticity of the public bank keys sent to them by Remote Data Transmission by comparing their hash values with the hash values notified by the Bank via the separately agreed communication channel.
The Customer must ensure use of software which verifies the validity of the server certificates used in transport encryption by means of the certification path notified separately by the Bank.

3 Special obligations to exercise due diligence when creating identification and security media

When Customers generate their own identification and security media in accordance with the EBICS specification standards and initialise them at the Bank, the Customer must ensure the following:
– Confidentiality and integrity of the identification medium in all phases of the authentication process, including display, transmission and storage.
– Private participant keys saved on the identification and storage media shall not be saved in unencrypted form.
– The identification medium must be locked after five consecutive incorrect attempts to enter the password.
– The private and public participant keys must be created in a secure environment.
– The identification and security media must be exclusively and uniquely assigned to and used by the Participant.

4 Placing orders with the Bank

The User shall verify the accuracy of the order data and ensure that only this data is signed electronically. When initialising communication, the Bank shall first conduct Participant-related authorisation verifications, such as order type authorisation or, if applicable, agreed limit verifications. The results of further banking verifications such as limit verifications or account authorisation verifications shall be notified to the Customer in the Customer protocol at a later date.

Order data transmitted to the bank system may be authorised a follows:
1. All necessary banking ESs are transmitted together with the order data.
2. If a Distributed Electronic Signature (Verteilte Elektronische Unterschrift [VEU]) has been agreed with the Customer for the respective order type and the ESs transmitted are insufficient for banking authorisation, the order is stored in the bank system until all necessary ESs have been submitted.
3. If the Customer and the Bank agree that order data delivered by Remote Data Transmission may be authorised by means of a separately transmitted accompanying note (Begleitzettel)/batch order (Sammelauftrag), a transport signature (type »T«) must be provided for the technical protection of the order data instead of the User's banking ES. To this end, the file must bear a special tag indicating that there are no further ESs for this order other than the transport signature (type »T«). The order is authorised once the Bank has successfully verified the User's signature on the accompanying note (Begleitzettel)/batch order (Sammelauftrag).

4.1 Issuing orders by means of the Distributed Electronic Signature (VEU)

The manner in which the Distributed Electronic Signature will be used by the Customer must be agreed with the Bank.
The Distributed Electronic Signature shall be used if orders are to be authorised independently of the transport of the order data and, if applicable, by several Participants.
Until all banking ESs necessary for authorisation are available, the order can be deleted by an authorised User. If the order has been fully authorised, it can only be recalled/revoked in accordance with Section 9 of the Terms and Conditions for Remote Data Transmission.
The Bank may delete orders that have not been fully authorised after expiry of the time limit notified separately by the Bank.

4.2 Verification of identification by the Bank

Order data delivered by Remote Data Transmission shall be executed as an order by the Bank only after the necessary banking ESs or the signed accompanying note (Begleitzettel)/batch order (Sammelauftrag) have been received and positively verified.

4.3 Customer protocols

The Bank shall document the following in Customer protocols:
– Transmission of the order data to the bank system
– Transmission of information files from the bank system to the Customer system
– Result of each verification of identification for orders from the Customer to the bank system
– Further processing of orders where these concern signature verification and the display of order data
The Participant shall consult the result of the verifications carried out by the Bank by promptly calling up the Customer protocol. The Participant shall file this protocol, the contents of which shall comply with the provisions of Section 10 of Annex 1b, in its records and make it available to the Bank on request.

5 Change of Participant keys with automatic activation

If the identification and security media used by the Participant are valid for a limited period of time, the Participant must transmit the new public Participant keys to the Bank promptly before the expiry date. After the expiry date of the old keys has passed, a new initialisation must be performed.
If the Participant generates their keys personally, they must renew the Participant keys using the system-determined order types provided for this purpose and transmit them promptly before expiry of the old keys.

To automatically activate new keys without renewed Participant initialisation, the following order types shall be used:
– update of the public banking key (PUB) and
– update of the public authentication key and the public encryption key (HCA) or alternatively
– update of all three above keys (HCS).
The order types PUB and HCA or HCS must be provided with a valid User banking ES for this purpose. After the keys have been successfully changed, only the new keys may be used.
If the electronic signature could not be positively verified, the procedure specified in Section 8 (3) of the Terms and Conditions for Remote Data Transmission shall apply.
The key may be changed only after all orders have been fully processed. Otherwise, any orders not yet executed must be placed again using the new key.

6 Blocking of Participant keys

If misuse of the Participant keys is suspected, the Participant shall be obligated to block their access authorisation for all bank systems using the compromised key(s).
If the Participant is in possession of valid identification and security media, they can block their access authorisation via EBICS. By sending a message with an »SPR« order type, access will be

blocked for the Participant whose User ID was used to send the message. After blocking, no further orders can be placed by this Participant via EBICS until the reinitialisation referred to in Section 2 has been carried out.
If the Participant is no longer in possession of valid identification and security media, they can request blocking of the identification and security media outside the RDT procedure via the blocking facility notified separately by the Bank.

The Customer may request blocking of a Participant's identification and security media or the entire Remote Data Transmission access outside the RDT procedure via the blocking facility notified by the Bank.

HypoVereinsbank Member of UniCredit

Further details on the bank are provided in the List of Prices and Services.

ANNEX 1B TO THE TERMS AND CONDITIONS OF REMOTE DATA TRANSMISSION

Specification of EBICS Connection

Please find the specification under www.ebics.de

HypoVereinsbank Member of UniCredit

Further details on the bank are provided in the List of Prices and Services.

ANNEX 1C TO THE TERMS AND CONDITIONS OF REMOTE DATA TRANSMISSION

Security requirements of the EBICS Customer system

In addition to the security measures set out in Annex 1a (6), the Customer must comply with the following requirements:

– The software used by the Customer for the EBICS procedure must meet the requirements set out in Annex 1a.

– EBICS Customer systems may not be used without a firewall. A firewall is an application which monitors all incoming and outgoing messages and allows only known or authorised connections.

– A virus scanner must be installed and regularly updated with the latest virus definition files.

– The EBICS Customer system should be configured in such a way that Participants must log in before using it. They should log in as a normal User and not as an administrator who is authorised, for example, to carry out programme installations.

– The internal IT communication channels for unencrypted banking data or for unencrypted EBICS messages must be protected against interception and manipulation.

– If security-related updates are available for the operating system in use and for other security-related software programmes that have been installed, they should be used to update the EBICS Customer systems.

The Customer shall be exclusively responsible for compliance with these requirements.

HypoVereinsbank Member of UniCredit

Further details on the bank are provided
in the List of Prices and Services.

ANNEX 2 TO THE TERMS AND CONDITIONS OF REMOTE DATA TRANSMISSION

Currently not assigned

HypoVereinsbank Member of UniCredit

Further details on the bank are provided in the List of Prices and Services.

ANNEX 3 TO THE TERMS AND CONDITIONS OF REMOTE DATA TRANSMISSION

Speification of Data Formats

Please find the specification under www.ebics.de