The Deutsche Bundesbank's procedural rules for communicating via EBICS with deposit-taking credit institutions and other account holders with a bank sort code

(EBICS procedural rules)

Effective date: 20 November 2017

Notes on the English translation

This translation has been prepared with the greatest possible care; however, in case of doubt, the German text is the authoritative version.

TABLE OF CONTENTS

REFERENCE DOCUMENTS

	Document	Title
1	Specifications for the EBICS connection	Annex 1 of the interface specifications for data telecommunication between the client and the credit institution in accordance with the data telecommunication agreement
2	EBICS implementation guide	EBICS implementation guide, supplement to the current data telecommunication agreement
3	Deutsche Bundesbank's General Terms and Conditions	General Terms and Conditions of the Deutsche Bundesbank
4	Procedural rules for SEPA direct debit	The Deutsche Bundesbank's procedural rules for the clearing and settlement of SEPA direct debits via the RPS SEPA-Clearer
5	Procedural rules for SEPA credit transfer	The Deutsche Bundesbank's procedural rules for the clearing and settlement of SEPA credit transfers via the RPS SEPA-Clearer
6	Procedural rules for SCC card payments	The Deutsche Bundesbank's procedural rules for the clearing and settlement of SCC card payments via the RPS SEPA-Clearer
7	Procedural rules for cheque	The Deutsche Bundesbank's procedural rules for the clearing and settlement of cheque via the Retail Payment System (RPS)
8	Procedural rules for CAM-Individual	Rules of procedure of the Deutsche Bundesbank for the settlement of euro payments and payments in foreign currencies via the customer access mechanism-individual (CAM-Individual)
9	Procedural rules for accessing electronic account information	The Deutsche Bundesbank´s procedural rules for accessing electronic account information

1 Description of the procedure

With respect to cashless payments, the Deutsche Bundesbank makes a distinction between credit institutions within the meaning of Article 4 (1) of Directive 2013/575/EU on the business of deposit-taking credit institutions (for which the Deutsche Bundesbank maintains PM, HAM and dotation accounts, and which can be participants in the Bundesbank's payment systems) and other account holders. The term "other account holder" encompasses payment service providers within the meaning of section 1 (1) numbers 2 to 5 of the Payments Services Oversight Act (*Zahlungsdiensteaufsichtsgesetz* or ZAG), credit institutions with a partial banking licence and public administrations.

With its electronic access for deposit-taking credit institutions and other account holders with a bank sort code (hereinafter "payment service provider"), which is based on the Electronic Banking Internet Communication Standard (EBICS), the Deutsche Bundesbank offers a communication channel based on accepted protocols and standards which is capable of processing the exchanging of data between banks efficiently, securely and cost-effectively.

Access is based on the current version (version 2.5) of the EBICS customer-bank standard (schema H004).

Therefore, for the settlement of interbank payment transactions, specifications are required which go beyond the EBICS protocol. These primarily relate to the deviations from the typical EBICS roles of customers and banks. Furthermore, for communication with payment service providers, the EBICS standard contains instruction types specified by the Deutsche Bundesbank which enable the usual data formats to be transferred between banks.

The following procedural rules define the amendments to the EBICS standard which are required for the exchange of data between banks, specifications for a fully automated processing system and the Deutsche Bundesbank's range of EBICS-based services.

2 Scope

These procedural rules apply solely to EBICS communication between the Deutsche Bundesbank and payment service providers and/or their computer service centres. For EBICS communication with public administrations and other account holders, the "Special terms and conditions of the Deutsche Bundesbank for account holders without a bank sort code concerning data telecommunication via EBICS (EBICS conditions)" apply.

These procedural rules apply to the following Deutsche Bundesbank specialised procedures as well as when accessing electronic account information.

- RPS SEPA-Clearer
- RPS cheque processing service
- Customer Access Mechanism-Individual (CAM-Individual)

In addition, the General Terms and Conditions of the Deutsche Bundesbank apply.

3 Eligibility to use EBICS

As a general rule, all payment service providers with an account at the Deutsche Bundesbank may take advantage of the EBICS communication procedure. Further details are specified in the relevant procedural rules for these specialised procedures. The current forms can be found under “Tasks/Payment systems/Servives/Forms” on the Deutsche Bundesbank’s website (www.bundesbank.de). In each case, they are to be submitted to the Deutsche Bundesbank customer service team that is responsible in each case. Bank branches can apply to use the EBICS communication channel through the customer service team responsible for their head office. In this case, applications are to be signed by authorised signatories representing the institution as a whole.

The account holder is obliged to provide the following information for the payment service provider's EBICS banking system.

- Host ID of the EBICS banking system
- EBICS URL or IP of the EBICS banking system
- Initialisation letters signed by the account holder for the public bank-specific keys (INI)
- Initialisation letters signed by the account holder for the public authentication and encryption keys (HIA)
- Information about the TLS server certificate of the EBICS banking system
- Hash values of the EBICS banking system’s public keys

Upon receipt of the application documents, the Deutsche Bundesbank issues the payment service provider with the access data that are needed to utilise EBICS. Said provider is required to enter the Deutsche Bundesbank in its master data as specified in the written agreement. At the same time, the payment service provider is entered in the Deutsche Bundesbank's EBICS system.

Once all system-related preparations have been completed, the account holder must submit the initialisation letters needed for activating the EBICS connection to the same customer service team to whom the application for use of EBICS as a communication channel was or will be submitted. The letters in question must bear the account-holder’s signature and be accompanied by the other documents that are required in order to cross-check the data (ie information about the TLS server certificate and the hash values for the public keys of the EBICS banking system). The customer service team will then pass the documents on to the competent master data administrator. When submitting order types INI and HIA electronically, it must be borne in mind that the validity of these instructions expires after 72 hours. If the initialisation letters are not received by the Deutsche Bundesbank master data administrator by this deadline, they will have to be resubmitted.

If a computer service centre is used as a communicating office, the key material used for securing EBICS transactions is exchanged with this computer service centre. As the authorised customer and participant for the accounts of the commissioning payment service providers, this computer service centre is recorded in the master data of the Deutsche

Bundesbank's EBICS system. The computer service centre receives the customer ID and participant ID required for submitting payments via EBICS.

Communication via EBICS occurs by means of an open network (internet) using an asymmetric cryptographic procedure. The payment service provider is required to secure its IT systems against internal and external threats in accordance with the specifications laid down by the Federal Financial Supervisory Authority (BaFin). Furthermore, the recommendations of the Federal Office for Information Security (BSI), as contained in the IT Baseline Protection Manual, are to be observed. In particular, the private cryptographic keys are to be handled with the utmost care and attention.

4 Roles of communication participants

The EBICS protocol was developed for the clearing and settlement of electronic payment transactions between customers and payment service providers. It therefore acts as a client-server protocol, ie communication always originates from the client. The EBICS protocol is therefore based on a role scenario in which the payment service provider always assumes the passive role, ie outgoing data deliveries are provided solely for collection.

This allocation of roles cannot be used for the settlement of interbank payment transactions. The exchange of data in interbank payments assumes that the communicating partners have equal roles (peer-to-peer communication). In the case of communication between the Deutsche Bundesbank and a payment service provider, the sending communication partner always assumes the active role of the client. This means that the payment service provider always assumes the active role in the case of data transmissions to the Deutsche Bundesbank.

Conversely, the Deutsche Bundesbank always assumes the active role in the case of outgoing data submissions to payment service providers. In terms of the terminology used in the data telecommunication agreement, the Deutsche Bundesbank acts as a kind of banking system for submissions by payment service providers. In the case of deliveries, the Deutsche Bundesbank generally acts as a customer system. The role scenario therefore changes depending on the direction of transfer. How this role scenario is conceived by the payment service provider depends on how that provider implements it. A communication system depicting this role behaviour is hereinafter referred to as an EBICS system.

There are two main exceptions to the basic principle that data are always sent “actively”.

a) EBICS mechanisms are used as part of the participant initialisation with the result that the banking system's public keys are “made available for collection”. There is no provision for “active” sending.

b) "Customer protocols" are not actively sent to the recipient by the Deutsche Bundesbank. Instead, they must be collected, following their creation by the Deutsche Bundesbank's EBICS system, by the submitter of the instruction to which the customer protocol refers. In the case of deliveries, by the same token, the Deutsche Bundesbank

expects the recipient to provide a customer protocol which it will periodically collect as part of its sender's oversight activities.

In the relationship between a payment service provider and the Deutsche Bundesbank, the customer protocol performs the function of logging events which occur prior to processing in the specialised applications. Specifically, the following steps are logged in line with the data telecommunication agreement.

- The transfer of the order type to the Deutsche Bundesbank.
- The result of the electronic signature verification and the decompression procedure.
- The transmission for processing in the specialised application, provided the checks were successful at EBICS level; if not, the corresponding error code should be stated.
- A check of the hash values attached to the public bank-specific key upon first using a previous public bank key

The submitting payment service provider cannot assume that the files submitted to the Deutsche Bundesbank's specialised applications have been successfully transmitted until it has been informed via the customer protocol that the submission and the signature check have been completed successfully. The payment service provider must therefore collect the customer protocol in order to receive timely information as to whether the data transmission was successful or whether errors occurred prior to processing in the specialised applications so that counter measures can be taken if necessary.

Message files

The Deutsche Bundesbank informs the submitting party of technical processing errors/checks and/or processed payments in the specialised applications by means of message files

- Message type pacs.002SCL for the processing of SEPA payments using the SEPA-Clearer. In addition, at the close of every SEPA-Clearer business day each participant receives a separate end-of-day report for each service used (ie a daily reconciliation report for credit transfers [DRC], a daily reconciliation report for direct debits [DRD] – the latter being split into a report on SEPA Core direct debits and one on SEPA B2B direct debits – and/or a daily reconciliation report for SEPA card clearing collections [DRR SCC]). Each report summarises all the bulk transactions submitted to and delivered from the SEPA-Clearer on that business day.
- For instructions to CAM-Individual, the following M messages are used. M3 message “Notification of a non-processable file”, M7 message “Notification of payments which have not been executed or have been cancelled”, M8 message “Notification of non-processable data records”. In addition, an M9 message is created to confirm files which have been processed and delivered.
- For transaction volume enquiries relating to the collection of electronic account information, the M3 message format is used to report a request file that cannot be processed or has been transferred in duplicate.

- When issuing electronic instructions to the cheque processing service provided by the Deutsche Bundesbank's RPS, use should be made of message type pacs.002SVV. In addition, at the close of every business day, each participant receives a separate daily reconciliation report for each service used. For BSE cheques, this takes the form of a daily reconciliation report for SVV BSE (DRD BSE). In the case of ISE cheques and ISE returned cheques, this entails a daily reconciliation report for SVV ISE (DRD ISE) and a daily reconciliation report for ISR (DRD ISR) respectively. Each report constitutes a summary of all the bulk transactions submitted to and delivered from the Deutsche Bundesbank's RPS cheque clearing service in the course of the business day in question.

Computer service centres

If a computer service centre is used, the key material used for securing EBICS transactions is exchanged with this computer service centre (see also No 3). The computer service centre acts as an authorised customer and participant for the accounts of the originating payment service providers. It receives the customer ID and the participant ID required for submitting payments via EBICS communication. A check is carried out on the signatures of the computer service centre. Owing to this required authorisation, the computer service centre has the status of a full EBICS participant and not just that of a technical participant in accordance with the EBICS terminology (see also Specifications for the EBICS connection, No 3.7, Technical participants).

In the RPS SEPA-Clearer and the RPS cheque processing service, the 11-character BIC in the XML file header ("sending institution" field) of the submitted file is used to make the account verification check. In the case of submission via a computer service centre, this is the (technical) BIC of the computer service centre; in the case of direct submissions by the payment service provider for its own accounts, it is the account holder's BIC. For all other submissions, the authorisation check is effected on the basis of the bank sort code or the bank-sort-code-free giro account number of the payment service provider specified in the A record of the files.

5 Detailed description of the procedure

5.1 Security procedures

5.1.1 General specifications

The security procedures specified in the EBICS protocol are used to secure the transactions via EBICS. As with the provisions set out in the data telecommunication agreement, three RSA key pairs are provided for each participant.

- Public / private bank-specific keys
- Public / private authentication keys
- Public / private encryption keys

A single pair of keys is used for the bank-specific signature of the instructions. Only one pair of keys can be used for authenticating the participant in the banking system and for decrypting transaction keys. The Deutsche Bundesbank uses the same pair of physical keys for both the authentication keys and the encryption keys. Different key pairs are used for submissions to the Deutsche Bundesbank and deliveries by the Deutsche Bundesbank.

All active send instructions are secured with an electronic signature. This applies both to submissions to the Deutsche Bundesbank and deliveries by the Deutsche Bundesbank to payment service providers. No accompanying slips may be used as a means of authenticating transactions when data are exchanged with payment service providers; nor can the instruction code “DZHNN” be used for send instructions.

The successful verification of a payment service provider's electronic signature authorises the Deutsche Bundesbank to forward the data to the specialised application for processing. The Deutsche Bundesbank's delivery data, which are likewise secured with an electronic signature, should only be processed after the successful verification of the electronic signature. The electronic signature corresponds to a class E bank-specific electronic signature as specified in the data telecommunication agreement.

Download transactions constitute an exception to the rule of securing all data with an electronic signature. Collection data can be requested using the instruction code “DZHNN” until the electronic signature has been entered in the data telecommunication agreement. Once the electronic signature has been implemented in customer-bank business, communication with the Deutsche Bundesbank is possible only using the instruction code “OZHNN”.

The security procedures of the EBICS version 2.5 listed below are permitted.

- Authentication signature in accordance with “X002”
- Encryption in accordance with “E002”
- Electronic signature in accordance with A004, A005 and A006

The distributed electronic signature and X.509 certificates are not supported at present.

The validity period of the keys used conforms with the recommendations of the Federal Network Agency (*Bundesnetzagentur*) and the Federal Office for Information Security.

5.1.2 Overview of the keys in use

Depending on the role and the direction of communication, deployment of the EBICS security procedures for communication between the Deutsche Bundesbank and the payment service providers necessitates the use of various “logical” keys and key pairs for the various security procedures.

In this context, “logical” refers to the use of separate keys, depending on the type of communication relationship and the type of EBICS system implementation (separate client and server system, combined client and server system).

In physical terms, several logical keys can be identical (see No 5.1.1).

The following table shows which keys may be used for communication between the Deutsche Bundesbank and payment service providers.

BACp =	Bundesbank authentication key client public key
BACs =	Bundesbank authentication key client secret key
BASp =	Bundesbank authentication key server public key
BASs =	Bundesbank authentication key server secret key
BECp =	Bundesbank electronic signature key client public key
BECs =	Bundesbank electronic signature key client secret key
BESp =	Bundesbank electronic signature key server public key (not defined in the EBICS at present)
BESs =	Bundesbank electronic signature key server secret key (not defined in the EBICS at present)
BVCp =	Bundesbank encryption key client public key
BVCs =	Bundesbank encryption key client secret key
BVSp =	Bundesbank encryption key server public key
BVSs =	Bundesbank encryption key server secret key
KACp =	Payment service provider authentication key client public key
KACs =	Payment service provider authentication key client secret key
KAp =	Payment service provider authentication key public key
KAs =	Payment service provider authentication key secret key
KASp =	Payment service provider authentication key server public key
KASs =	Payment service provider authentication key server secret key
KECp =	Payment service provider electronic signature key client public key
KECs =	Payment service provider electronic signature key client secret key
KEp =	Payment service provider electronic signature key public key
KEs =	Payment service provider electronic signature key secret key
KESp	Payment service provider electronic signature key server public key (not defined in the EBICS at present)
KESs =	Payment service provider electronic signature key server secret key (not defined in the EBICS at present)
KVCp =	Payment service provider encryption key client public key
KVCs =	Payment service provider encryption key client secret key
KVp =	Payment service provider encryption key public key
KVs =	Payment service provider encryption key secret key
KVSp =	Payment service provider encryption key server public key
KVSs =	Payment service provider encryption key server secret key

Table 1: General overview of keys

The abbreviations used here to denote keys apply exclusively to this document and do not correspond with the terms used in the EBICS specifications.

Two different scenarios are considered.

1 The payment service provider uses separate client and server keys.

2 The payment service provider uses combined client and server keys.

5.1.2.1 Use of separate client and server keys by the payment service provider

The following keys are used.

	Deutsche Bundesbank		Payment service provider	
	Client	Server	Client	Server
Authentication	BACs BACp	BASs BASp	KACs KACp	KASs KASp
Encryption	BVCs BVCp	BVSs BVSp	KVCs KVCp	KVSs KVSp
Electronic signature	BECs BECp	(BESs)[1] (BESp)[1]	KECs KECp	(KESs)[1] (KESp)[1]

Table 2: Use of separate keys

These are put to use depending on the direction of transfer and the type of transfer (upload/download transaction) (see No 5.2).

The payment service provider has the following secret keys.

KACs = Payment service provider authentication key client
KASs = Payment service provider authentication key server
KVCs = Payment service provider encryption key client
KVSs = Payment service provider encryption key server
KECs = Payment service provider electronic signature client

These are logical keys which are used in one of the respective roles. In physical terms, KACs, KASs, KVCs and KVSs can be identical, which means that only three secret keys can be used and securely saved instead of five. The Deutsche Bundesbank uses physically identical keys for BVCs/BACs and BASs/BVSs. The secret BESs and KESs keys are only envisaged in EBICS and are not currently used in communication with the Bundesbank.

The Deutsche Bundesbank administers the following public keys of the payment service provider.

KACp = Payment service provider authentication key client
KASp = Payment service provider authentication key server
KVCp = Payment service provider encryption key client
KVSp = Payment service provider encryption key server
KECp = Payment service provider electronic signature client

These are logical keys. The number of physical keys is dependent on the implementation by the payment service provider. It may be the case that a payment service provider uses a physical key for several logical keys (for example, KACp, KASp, KVCp and KVSp could be identical in physical terms). The Deutsche Bundesbank uses physically identical keys for BVCp/BACp and BASp/BVSp. The public BESp and KESp keys are only envisaged in EBICS and are not currently used in communication with the Deutsche Bundesbank.

[1] Currently only envisaged in EBICS.

5.1.2.2 Use of a combined client and server key by the payment service provider

The following keys are used.

	Deutsche Bundesbank		Payment service provider
	Client	Server	
Authentication	BACs BACp	BASs BASp	KAs KAp
Encryption	BVCs BVCp	BVSs BVSp	KVs KVp
Electronic signature	BECs BECp	(BESs)[1] (BESp)[1]	KEs KEp

Table 3: Use of combined keys

These are put to use depending on the direction of transfer and the type of transfer (upload/download transaction) (see No 5.2).

The payment service provider has the following secret keys.

KAs = Payment service provider authentication key

KVs = Payment service provider encryption key

KEs = Payment service provider electronic signature key

These are logical keys which are used in one of the respective roles. In physical terms, KAs and KVs can be identical, which means that only two secret keys can be used and securely saved instead of three. The Deutsche Bundesbank uses physically identical keys for BVCs/BACs and BASs/BVSs. The secret BESs key is only envisaged in EBICS and is not currently used in communication with the Deutsche Bundesbank.

The Deutsche Bundesbank administers the following public keys of the payment service provider.

KAp = Payment service provider authentication key

KVp = Payment service provider encryption key

KEp = Payment service provider electronic signature key

These are logical keys. The number of physical keys is dependent on the implementation by the payment service provider. It may be the case that a payment service provider uses a physical key for several logical keys (KAp and KVp could be identical in physical terms). The Deutsche Bundesbank uses physically identical keys for BVCp/BACp and BASp/BVSp. The public BESp key is only envisaged in EBICS and is not currently used in communication with the Deutsche Bundesbank.

5.1.3 Key management

5.1.3.1 Initialisation

Once the payment service provider has received the bank parameters from the Deutsche Bundesbank, it has to initialise itself in the Deutsche Bundesbank's EBICS system. Initialisation is effected using order types “INI” and “HIA” in accordance with the specifications stated in the data telecommunication agreement.

Once the hash values delivered with the application for approval have been positively verified, the Deutsche Bundesbank changes the status of the keys that were transferred by the payment service provider to “activated”. The payment service provider collects the Deutsche Bundesbank's public keys using order type “HPB”. Once the Deutsche Bundesbank's public keys have been positively verified against the hash values published by the Deutsche Bundesbank via a separate channel, they are to be activated by the payment service provider. The payment service provider is sent the currently valid hash values for submission together with the bank parameters.

The Deutsche Bundesbank's public keys for the encryption and the authentication signature are delivered with the order type “HPB”. The signature key will not be provided until the electronic signature for payment service providers has been incorporated into the data telecommunication agreement. Once this stage is complete, the payment service provider will be able to transmit send instructions to the Deutsche Bundesbank.

For data deliveries by the Deutsche Bundesbank to a payment service provider, the Deutsche Bundesbank initialises itself in the latter's EBICS system. This occurs in the same way that the payment service provider initialises itself on the Deutsche Bundesbank's EBICS system using order types “INI” and “HIA”. For this, the Deutsche Bundesbank requires the payment service provider's banking parameters which are submitted with the application for approval. The hash values of the keys that are used by the Deutsche Bundesbank for the delivery are sent to the payment service provider in the form of an initialisation letter. The payment service provider is required to compare the values of the keys transmitted using EBICS against the values in the initialisation letters. Once the keys have been positively verified against the initialisation letters, they are to be activated by the payment service provider. The Deutsche Bundesbank collects the latter's public keys using order type “HPB” and activates these once they have been positively verified against the hash values that were communicated separately by the payment service provider.

5.1.3.2 Exchange of keys

The Deutsche Bundesbank's keys have a defined validity period; the Deutsche Bundesbank generates a new public key once a year. The exact time at which this changeover is made and the new hash values are communicated to the payment service providers via an e-mail sent to the address specified for this purpose as part of the EBICS customer ID data in accordance with form 4750 “Application for communication via EBICS”. Information on the changeover can also be found on the Deutsche Bundesbank website at www.bundesbank.de > Tasks > Payment systems > Publications > Procedural rules. The payment service provider is required to collect and activate the new public keys for submission using order type “HPB”.

Upon introducing a new public key as at a specific reference date, the new public key and its predecessor are supported concurrently for a period of no more than three months. See point 5.2.3.1 for more information on the special circumstances associated with the first-time submission of a file using the old key (following the generation of a new key).

The Deutsche Bundesbank performs the update of the public keys on the payment service provider's EBICS system for delivery using order types “PUB” and “HCA”.

The Deutsche Bundesbank is to be informed in good time if a payment service provider is planning to exchange the keys. The payment service provider is responsible for updating the keys for submission in the Deutsche Bundesbank's EBICS system using order types “PUB” and “HCA”. The hash values of the new keys are to be sent to the Deutsche Bundesbank for delivery. In this case, the update of the keys is performed by the Deutsche Bundesbank using order type “HPB” and the new keys are then activated once the new hash values have been positively verified.

5.1.3.3 Blocks

The Deutsche Bundesbank is to be informed immediately if a payment service provider's active keys are compromised. At the same time, the affected keys are also to be blocked. The keys can be blocked in one of two ways.

- By written instruction to the Deutsche Bundesbank, Central Office, Z 201-2 (Fax: +49 69 9566 50 8067) to have the relevant public keys blocked. This instruction must be signed by authorised representatives or signatories.
- By blocking the keys in the Deutsche Bundesbank's EBICS system using order type “SPR”.

The immediate result of the instruction to initiate a block using order type “SPR” is that all deliveries secured with the blocked keys are rejected. In addition, the affected public keys are also to be blocked on the payment service provider's EBICS system, with the result that no further deliveries can be made by the Deutsche Bundesbank using the compromised keys. New pairs of keys have to be generated by the payment service provider and new initialisation letters sent to the Deutsche Bundesbank to enable communication to be re-established.

If the Deutsche Bundesbank's keys are compromised, the Deutsche Bundesbank will immediately re-initialise itself using valid keys.

5.1.4 TLS server certificates

5.1.4.1 General information

At the transport level, an SSL certificate is required for the TLS-based server authentication to create an encrypted connection (standard port 443) between the Deutsche Bundesbank and the customer systems.

To simplify the certificate verification procedure for customers, the Deutsche Bundesbank supports certification by a commercial trust centre, the CA certificates of which are already integrated into most of the keystores. For customers, the authenticity of the Deutsche Bundesbank's public key can therefore be confirmed by automatically checking the digital signature of the CA.

For live operations, the Deutsche Bundesbank also requires customers to issue certificates which have been certified by a commercial trust centre.

According to a recommendation of the Federal Office for Information Security (BSI)[2], only the current encryption version TLS 1.2 is supported with the "cipher suites" supported and recommended under TLS 1.2.

5.1.4.2 Fingerprint comparison

As an additional support service for checking the authenticity of a certificate, the currently valid fingerprint will be published on the Deutsche Bundesbank's website as a separate annex to this document.

5.2 Technical description of the procedure

5.2.1 EBICS parameters

Parameters similar to those in the data telecommunication agreement are used for communication between a payment service provider and the Deutsche Bundesbank. Here, the participant ID and the customer ID of the Deutsche Bundesbank are specified and are announced with the authorisation documents. The participant ID and customer ID for payment service providers are also issued by the Deutsche Bundesbank. The structure of the customer ID conforms with the content of the EBICS specifications. It always consists of eight characters and starts with a letter of the alphabet.

The Deutsche Bundesbank's bank parameters can be called up from the EBICS system using order type "HPD".

All submissions and deliveries are encrypted (with the exception of order types INI and HIA) and compressed. Encryption (hybrid procedure 3DES/RSA) and compression (ZIP compressed format) comply with the specifications in the data telecommunication agreement.

The parameters and the information which are relevant for transmission via EBICS are not communicated in the file name but via the EBICS XML envelope.

5.2.2 Allocation of an order number

The specifications for the EBICS connection stipulate that since version 2.5 (schema H004) the order number is assigned by the bank server.

An error message will be generated whenever an order number is assigned by the customer system.

[2] BSI TR-02102-2 (https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html)

5.2.3 Upload transactions

5.2.3.1 Direction of transfer: payment service provider -> Deutsche Bundesbank

All files submitted to the Deutsche Bundesbank are EBICS upload transactions to the Deutsche Bundesbank's EBICS system.

Each time communication is established, the Deutsche Bundesbank checks the hash value of the currently valid public key. Should the result of the check prove negative during the period when the Deutsche Bundesbank is concurrently supporting two public keys (see point 5.1.3.2), the customer will receive an error code message stating the EBICS return code “EBICS_BANK_PUBKEY_UPDATE_REQUIRED” when a file is first submitted following the generation of a new key and the system registers that the old key is being used. The error message draws attention to this occurrence and the need to make a corresponding update. In addition, a one-off entry is made in the customer report to flag the outdated public key. The rejected file must then be submitted afresh using either the old or the new key.

Further orders can be sent by the payment service provider during the transition period using the old public key or the old hash value. These will be accepted without triggering another error message or requiring an additional entry in the customer report.

Subsequently, EBICS participant-specific authorisation checks are performed, eg to identify whether the participant is authorised to initiate a specific order type. The results of other technical validation procedures, eg account eligibility checks, are conveyed to the PSP at a later date as part of the customer report.

The following order types can be used for submissions to the Deutsche Bundesbank.

5.2.3.1.1 Submissions to the RPS SEPA-Clearer

Order type	Text	Format
QB1	BILATERAL INPUT CREDIT FILE (BCF) SEPA Credit Transfer (pacs.008) SEPA Payment Cancellation Request (camt.056 SCT) SEPA Credit Transfer Return (pacs.004 SCT) SEPA Resolution of Investigation (camt.029)	BBkBCFBlkCdtTrf
QC1	INPUT CREDIT FILE (ICF) SEPA Credit Transfer (pacs.008) SEPA Payment Cancellation Request (camt.056 SCT) SEPA Credit Transfer Return (pacs.004 SCT) SEPA Resolution of Investigation (camt.029)	BBkICFBlkCdtTrf

Order type	Text	Format
QD5	INPUT CORE DEBIT FILE (CORE IDF) SEPA Direct Debit (pacs.003) SEPA Payment Cancellation Request (camt.056 SDD) SEPA Reject (pacs.002) SEPA Reversal (pacs.007) SEPA Return/Refund (pacs.004 SDD)	BBkIDFBlkDirDeb
QD6	INPUT B2B DEBIT FILE (B2B IDF) SEPA Direct Debit (pacs.003) SEPA Payment Cancellation Request (camt.056 SDD) SEPA Reject (pacs.002) SEPA Reversal (pacs.007) SEPA Return (pacs.004 SDD)	BBkIDFBlkDirDeb
QK1	SCC INPUT DEBIT FILE (SCC IDF) Interbank Card Clearing Collection (pacs.003 SCC) Interbank Reversal (pacs.007 SCC) Interbank Return/Refund (pacs.004 SCC) Supplementary Data Field (supl.017)	BBkIDFBlkSCC

Table 4: Order types for submissions to the RPS SEPA-Clearer

5.2.3.1.2 Submissions to CAM-Individual

Order type	Text	Format
QG1	GT file; same-day euro credit transfers from payment service providers	BBk DTA pursuant to the annex of the procedural rules for CAM-Individual, No 1.7[3] > EBCDIC/unpacked > Record length field: 4Bn[4]
QG2	GT file; same-day euro credit transfers from payment service providers	BBk SWIFT pursuant to the annex of the procedural rules for CAM-Individual[3], No 1.8.1 > EBCDIC/unpacked > Record length field: 6Bn[4]

[3] Rules of procedure of the Deutsche Bundesbank for the settlement of euro payments and payments in foreign currencies via the customer access mechanism-individual (CAM-Individual)
[4] Record length field; 4Bb = 4 bytes binary in field A1 or 1,.4Bn = 4 bytes numeric and 6Bn = 6 bytes numeric.

Order type	Text	Format
QDT	DT file; same-day international credit transfers (in euro) from payment service providers	BBk-SWIFT pursuant to the annex of the procedural rules for CAM-Individual system,[3] No 1.8.2 > EBCDIC/unpacked > Record length field: 6Bn[4]
QWT	WT file; foreign payment transfers (in foreign currency) from payment service providers	

Table 5: Order types for submissions to CAM-Individual

5.2.3.1.3 Transaction volume enquiries addressed to KTO2 / electronic account information (EAI)

Order type	Text	Format
QMA	MA file containing interim transaction volume and balance enquiries	BBk SWIFT pursuant to the annex of the procedural rules for EAI, No 1.5 [5] > A and E record EBCDIC/unpacked > Record length field: 6Bn[4]

Table 6: Order type for transaction enquiries addressed to KTO2 / EAI

5.2.3.1.4 RPS cheque processing service

Order type	Text	Format
QS1	SVV BSE INPUT DEBIT FILE BSE cheque (pacs.003 SVV) BSE return account of cheques (pacs.004 SVV)	BBkIDFBlkSVV
QS2	SVV ISE INPUT DEBIT FILE ISE cheque (pacs.003 SVV)	BBkIDFBlkSVV
QS3	SVV ISR INPUT DEBIT FILE ISE return account of cheques (pacs.004 SVV)	BBkIDFBlkSVV

Table 7: Order type for submissions to the Bundesbank's RPS cheque clearing service

Transaction initialisation occurs in accordance with the EBICS standard. As the Deutsche Bundesbank does not currently provide any public signature keys for submissions with the order type "HPB", the maximum frequency (maxOccurs) for the element `BankPubKeyDigests/Signature` is to be set at 0. The usage data are transmitted in accordance with the EBICS standard.

The submitted data are to be kept for at least ten business days in case they have to be resent.

For the above-mentioned order types, only the instruction attribute "OZHNN" is permitted. The following keys are used.

[5] The Deutsche Bundesbank´s procedural rules for accessing electronic account information

Scenario 1: payment service provider uses separate keys

	Deutsche Bundesbank		Payment service provider	
	Signing, encryption	Check, decryption	Signing, encryption	Check, decryption
Authentication	BASs	KACp	KACs	BASp
Encryption	-	BVSs	BVSp	-
Electronic signature	-	KECp	KECs	-

Table 8: Separate keys for submission

Scenario 2: payment service provider uses combined keys

	Deutsche Bundesbank		Payment service provider	
	Signing, encryption	Check, decryption	Signing, encryption	Check, decryption
Authentication	BASs	KAp	KAs	BASp
Encryption	-	BVSs	BVSp	-
Electronic signature	-	KEp	KEs	-

Table 9: Combined keys for submission

5.2.3.2 Direction of transfer: Deutsche Bundesbank ⇨ payment service provider

All files delivered by the Deutsche Bundesbank are EBICS upload transactions to the payment service provider's EBICS system. The following order types are used for deliveries by the Deutsche Bundesbank.

5.2.3.2.1 Deliveries from the RPS SEPA-Clearer

Order type	Text	Format
QB2	BILATERAL SETTLED CREDIT FILE (BCF) SEPA Credit Transfer (pacs.008) SEPA Payment Cancellation Request (camt.056 SCT) SEPA Credit Transfer Return (pacs.004 SCT) SEPA Resolution of Investigation (camt.029)	BBkBCFBlkCdtTrf
QC2	CREDIT VALIDATION FILE (CVF) SEPA Reject Credit Transfer via the SEPA-Clearer (pacs.002 SCLSCT)	BBkCVFBlkCdtTrf
QC3	SETTLED CREDIT FILE (SCF) SEPA Credit Transfer (pacs.008) SEPA Return (pacs.004 SCT) SEPA Payment Cancellation Request (camt.056 SCT) SEPA Resolution of Investigation (camt.029)	BBkSCFBlkCdtTrf

Order type	Text	Format
QK2	SCC DEBIT VALIDATION FILE (SCC DVF) SCC Reject Card Clearing Collection via the SEPA-Clearer (pacs.002SCLSCC)	BBkDVFBlkSCC
QK3	SCC DEBIT NOTIFICATION FILE (SCC DNF) Interbank Card Clearing Collection (pacs.003 SCC) Supplementary Data Field (supl.017)	BBkDNFBlkSCC
QK4	SCC SETTLED DEBIT FILE (SCC SDF) Interbank Reversal (pacs.007 SCC) Interbank Return/Refund (pacs.004 SCC) Supplementary Data Field (supl.017)	BBkSDFBlkSCC
QK5	SCC UNSETTLED DEBIT FILE (UDF) SEPA Direct Debit (pacs.003) SEPA Return/Refund (pacs.004)	BBkUDFBlkSCC
QK6	SCC RESULT OF SETTLEMENT FILE (RSF) SEPA Reject (pacs.002SCLSCC)	BBkRSFBlkSCC
QR1	DAILY RECONCILIATION REPORT FOR CREDIT TRANSFERS (DRC) – no XML structure –	EBCDIC
QR5	DAILY RECONCILIATION REPORT FOR SCC (DRR SCC) – no XML structure –	EBCDIC
QD7	DEBIT CORE VALIDATION FILE (DVF) SEPA Reject Direct Debit via the SEPA-Clearer (pacs.002 SCLSDD)	BBkDVFBlkDirDeb
QD8	DEBIT CORE NOTIFICATION FILE (DNF) SEPA Direct Debit (pacs.003) SEPA Payment Cancellation Request (camt.056 SDD) SEPA Reject (pacs.002)	BBkDNFBlkDirDeb
QD9	SETTLED CORE DEBIT FILE (SDF) SEPA Return/Refund (pacs.004 SDD) SEPA Reversal (pacs.007)	BBkSDFBlkDirDeb
QDA	DEBIT B2B VALIDATION FILE (DVF) SEPA Reject Direct Debit via the SEPA-Clearer (pacs.002 SCLSDD)	BBkDVFBlkDirDeb
QDB	DEBIT B2B NOTIFICATION FILE (DNF) SEPA Direct Debit (pacs.003) SEPA Payment Cancellation Request (camt.056 SDD) SEPA Reject (pacs.002)	BBkDNFBlkDirDeb

Order type	Text	Format
QDC	SETTLED B2B DEBIT FILE (SDF) SEPA Return (pacs.004 SDD) SEPA Reversal (pacs.007)	BBkSDFBlkDirDeb
QDD	UNSETTLED DEBIT CORE FILE (UDF) SEPA Reject (pacs.002SDD) SEPA Direct Debit (pacs.003) SEPA Return/Refund (pacs.004SDD)	BBkUDFBlkDirDeb
QDE	UNSETTLED DEBIT B2B FILE (UDF) SEPA Reject (pacs.002SDD) SEPA Direct Debit (pacs.003) SEPA Return/Refund (pacs.004 SDD)	BBkUDFBlkDirDeb
QDF	RESULT OF SETTLEMENT CORE FILE (RSF) SEPA Reject (pacs.002 SCLSDD)	BBkRSFBlkDirDeb
QDG	RESULT OF SETTLEMENT B2B FILE (RSF) SEPA Reject (pacs.002 SCLSDD)	BBkRSFBlkDirDeb
QR3	DAILY RECONCILIATION REPORT FOR CORE DIRECT DEBITS (DRD CORE) – no XML structure –	EBCDIC
QR4	DAILY RECONCILIATION REPORT FOR B2B DIRECT DEBITS (DRD B2B) – no XML structure –	EBCDIC
QSD	SEPA-Clearer Directory Conveyed in the rocs data record format of the European Automated Clearing House Association (EACHA)	According to XML schema: Rocs.001.001.06

Table 10: Order types for deliveries from the RPS SEPA-Clearer

5.2.3.2.2 Deliveries from CAM-Individual

Order type	Text	Format
QG3	GT file; same-day euro credit transfers to payment service providers	BBk DTA pursuant to the annex to the CAM-Individual procedural rules[3], No 1.7 > EBCDIC/unpacked > Record length field: 4Bn[4]
QG4	GT file; same-day euro credit transfers to payment service providers	BBk SWIFT pursuant to the annex to the CAM-Individual procedural rules[3], No 1.8.1 > A and E record EBCDIC/unpacked > Record length field: 6Bn[4]

Order type	Text	Format
QWA	Settlement of foreign payment transfer orders (WA files)	BBk SWIFT pursuant to the annex to the CAM-Individual procedural rules[3], No 1.8.2 > A and E record EBCDIC/unpacked > Record length field: 6Bn[4]
QM3	M3 message: Notification of a non-processable file	M messages pursuant to annex to the CAM procedural rules[3], No 1.9 > EBCDIC/unpacked > Record length field: 4Bn**Fehler! Textmarke nicht definiert.**
QMH	M6 message: Free text message	
QM7	M7 message: Notification of payments which have not been executed or have been cancelled owing to a lack of cover	
QM8	M8 message: Notification of non-processable data records	
QM9	M9 message: Notification of processed payments and delivered files	

Table 11: Order types for deliveries from CAM-Individual

5.2.3.2.3 Deliveries from KTO2 / electronic account information

Order type	Text	Format
QMU	Interim transaction and balance reports	BBk SWIFT pursuant to the annex to the procedural rules for accessing electronic account information[5], No 1.5 > A and E record EBCDIC/unpacked > Record length field: 6Bn[4]
QMK	MK file, end-of-day statement	
QMN	M3 file: notification that an MA file could not be processed	

Table 12: Order types for deliveries from KTO2 /electronic account information

5.2.3.2.4 Deliveries from the Deutsche Bundesbank's RPS cheque clearing service

Order type	Text	Format
QS4	SVV BSE DEBIT VALIDATION FILE BSE reject by the Deutsche Bundesbank (pacs.002 SVV)	BBkDVFBlkSVV
QS5	SVV BSE DEBIT NOTIFICATION FILE BSE cheque (pacs.003 SVV)	BBkDNFBlkSVV
QS6	SVV BSE SETTLED DEBIT FILE BSE return account of cheques (pacs.004 SVV)	BBkSDFBlkSVV

Order type	Text	Format
QS7	SVV ISE DEBIT VALIDATION FILE ISE reject by the Deutsche Bundesbank (pacs.002 SVV)	BBkDVFBlkSVV
QS8	SVV ISE DEBIT NOTIFICATION FILE ISE cheque (üacs.003 SVV)	BBkDNFBlkSVV
QS9	SVV ISR SETTLED DEBIT FILE ISE return account of cheques (pacs.004.SVV)	BBkSDFBlkSVV
QSA	SVV ISR DEBIT VALIDATION FILE ISE return account of cheques reject by Deutsche Bundesbank (pacs.002 SVV)	BBkDVFBlkSVV
QSB[6]	SVV BSE UNSETTLED DEBIT FILE (UDF) BSE cheque (pacs.003SVV) BSE return account (pacs.004SVV)	BBkUDFBlkSVV
QSC[6]	SVV ISE UNSETTLED DEBIT FILE (UDF) ISE cheque (pacs.003SVV)	BBkUDFBlkSVV
QSE[6]	SVV ISR UNSETTLED DEBIT FILE (UDF) ISE return account (pacs.004SVV)	BBkUDFBlkSVV
QSF[6]	SVV BSE RESULT OF SETTLEMENT FILE (RSF) BSE reject by Deutsche Bundesbank (pacs.002SVV)	BBkRSFBlkSVV
QSG[6]	SVV ISE RESULT OF SETTLEMENT FILE (RSF) ISE reject by Deutsche Bundesbank (pacs.002SVV)	BBkRSFBlkSVV
QSH[6]	SVV ISR RESULT OF SETTLEMENT FILE (RSF) ISE return account reject by Deutsche Bundesbank (pacs.002SVV)	BBkRSFBlkSVV
QR6	DAILY RECONCILIATION REPORT FOR SVV BSE (DRD ISE)	EBCDIC
QR7	DAILY RECONCILIATION REPORT FOR SVV ISE (DRD ISE)	EBCDIC
QR8	DAILY RECONCILIATION REPORT FOR SVV ISR (DRD ISR)	EBCDIC

Table 13: Order types for deliveries from the cheque clearing service

The transaction initialisation occurs in accordance with the EBICS standard. As no payment service provider public signature keys with the order type HPB are issued for deliveries, the maximum frequency (maxOccurs) for the element `BankPubKeyDigests/Signature` is set at 0. The usage data are transmitted in accordance with the EBICS standard.

[6] valid from November 2018

On request, a second data delivery is possible up to a maximum of ten business days after the first successful delivery.

The above-mentioned order types are delivered with the instruction attribute “OZHNN” only. The following keys are used.

Scenario 1: payment service provider uses separate keys

	Deutsche Bundesbank		Payment service provider	
	Signing, encryption	Check, decryption	Signing, encryption	Check, decryption
Authentication	BACs	KASp	KASs	BACp
Encryption	KVSp	-	-	KVSs
Electronic signature	BECs	-	-	BECp

Table 14: Separate keys for deliveries

Scenario 2: payment service provider uses combined keys

	Deutsche Bundesbank		Payment service provider	
	Signing, encryption	Check, decryption	Signing, encryption	Check, decryption
Authentication	BACs	KAp	KAs	BACp
Encryption	KVp	-	-	KVs
Electronic signature	BECs	-	-	BECp

Table 15: Combined keys for deliveries

5.2.4 Download transactions

Download transactions represent an exception in terms of EBICS communication with the Deutsche Bundesbank. The following order types are realised as download transactions.

Order identification	Description
HPB	Collect the Deutsche Bundesbank's or payment service provider's public keys
HPD	Collect bank parameters
HAC	Download customer protocol (XML-format)
PTK	Download customer protocol (DTAUS0-Format)
HKD	Collect customer and participant information
HTD	Call up customer and participant information

Table 16: Order types for retrievals from the EBICS system

The payment service provider's EBICS system must offer order types “HPB”, “HPD” and “PTK”/“HAC” to enable the Deutsche Bundesbank to call up data.

The Deutsche Bundesbank uses order type “HPD” to provide its current bank parameter data for communication via EBICS. Customer protocols are provided using order type “HAC” or “PTK”.

5.2.5 Customer protocols

Customer protocols are made available for download using order type “HAC”. During a transitional period customer protocols are also provided by using order type “PTK”.

The download of customer protocols with order type “HAC” or order type “PTK”, if used during the transitional period, has to be requested with form 4750 “Application for communication via EBICS – payment service providers with a bank sort code”.

Note:
Payment service providers which have already established an EBICS connection with the Deutsche Bundesbank need to successfully complete appropriate tests in order to extend the range of services currently used in the live environment, ie through the addition of the order type “HAC”.

The Deutsche Bundesbank's customer protocol is EBICS-compliant according to section 10 of the Specifications for the EBICS connection (applying to order type “HAC”) and section 4.2 of the Common Integrative Implementation Guide to Supplement the EBICS Specification (applying to order type “PTK”).

The error codes defined in the customer-bank standard are used in the customer protocol, with the result that automated processing is possible (error codes for “HAC” are shown in section 10.3 of the EBICS specifications). If a payment service provider is not authorised to submit instructions for the BIC specified in the tag `<SndgInst>` of the file header, the instruction is rejected with the participant-related EBICS error code [27] “unauthorised signatory” (for order type “PTK”) and error code DS0H “NotAllowedAccount” (unauthorised signatory) for order type “HAC”. The customer protocols can be called up for a maximum of ten business days.

In exchange for the data delivered by the Deutsche Bundesbank, the receiving payment service provider has to create an EBICS customer protocol in accordance with the data telecommunication agreement. It must likewise ensure that a customer protocol file notification is created for each order. The file notification should be structured as described in the descriptions of the Deutsche Bundesbank customer protocol (tables 17 to 20).

For the order types shown in tables 4 to 7, a file notification is displayed in the customer protocol.

The file notification for order types QB1, QC1, QD5, QD6, QK1, QS1, QS2 and QS3 includes the following SEPA payment file header information.

Description	Field name	XML element file header
Type of payment	File type	`FType`
Sender's 11-character BIC	Sending institution	`SndgInst` [7]
Creation date	File date and time	`FDtTm`
Number of payment records (total number of bulks)	Total number of bulks	For `FType` = "CORE IDF": `NumDDBlk + NumPCRBlk + NumREJBlk + NumRVSBlk + NumRFRBlk` For `FType` = "B2B IDF": `NumDDBlk + NumPCRBlk + NumREJBlk + NumRVSBlk + NumRFRBlk` For `FType` = "SCC IDF": `NumDDBlk + NumPCRBlk + NumREJBlk + NumRVSBlk + NumRFRBlk` For `FType` = "ICF": `NumCTBlk + NumRFRBlk + NumPCRBlk + NumROIBlk` For `FType` = "BCF": `NumCTBlk + NumPCRBlk + NumROIBlk + NumRFRBlk`
Sender's file reference	File reference	`FileRef`

Table 17: Structure of the customer protocol file notification for submissions to the RPS SEPA-Clearer and the RPS cheque processing service

Sample content of a QC1 file:

```
…
<AddtlInf>==========================================</AddtlInf>
<AddtlInf>ICF</AddtlInf>
<AddtlInf>Sender's BIC                          : BANKDEFF500</AddtlInf>
<AddtlInf>Creation date                         :2012-04-03T10:11:35</AddtlInf>
<AddtlInf>Number of payment records             :397</AddtlInf>
<AddtlInf>Sender's file reference               :1234567890123456</AddtlInf>
<AddtlInf>==========================================</AddtlInf>
</StsRsnInf>
…
```

For order types QG1, QG2 and QDT the file notification is structured as follows.

Description	Field name	Item
Type of payment	File designation/file type	A2
Bank sort code	Bank sort code of the file recipient; in the case of submissions, the bank sort code of the account-holding Bundesbank branch.	A3

[7] The BIC of the SEPA-Clearer is entered here as the sending institution (in production mode: MARKDEFF).

Description	Field name	Item
Account number	Bank sort code of the file sender	For submissions by payment service providers with a bank sort code: A4. For submissions by PSPs without a bank sort code: A9.
Customer	File sender's identifier	A5
Creation date	File creation date	A6
File number	Unique number of the file	A7
Number of payment records	Number of data records	E3
Sum total of the amounts	Sum of the amounts in euro	E9a

Table 18: Structure of the customer protocol file notification (for euro-denominated payment orders) in EA format

For order type QWT, the file notification is structured as follows.

Description	Field name	Item
Type of payment	File designation/file type	A2
Bank sort code	Bank sort code of the file recipient; in the case of submissions, the bank sort code of the account-holding Bundesbank branch.	A3
Account number	Bank sort code of the file sender	For submissions by payment service providers with a bank sort code: A4. For submissions by payment service providers without a bank sort code: A9.
Customer	File sender's identifier/bank name	A5
Creation date	File creation date	A6
File number	Unique number of the file	A7
Number of payment records	Number of data records	E3
Sum total of the amounts	Sum total of the amount fields	E5

Table 19 Structure of the customer protocol file notification for foreign currency payments

For order type QMA, the file notification is structured as follows.

Description	Field name	Item
Type of payment	File designation/file type	A2
Bank sort code	Bank sort code of the file recipient; in the case of submissions, the bank sort code of the account-holding Bundesbank branch.	A3
Account number	Bank sort code of the file sender	For submissions by payment service providers with a bank sort code: A4. For submissions by payment service providers without a bank sort code: A9.
Submitting party	File sender's identifier	A5
Creation date	Date Business day	A6
File number	Unique number of the file	A7
Number of data records	Number of data records	E3

Table 20: Structure of the customer protocol file notification for transaction volume enquiries

The protocols are to be kept for at least ten business days so that they can be called up by the Deutsche Bundesbank.

Key management and the other order types inherent in the system must be logged in accordance with the EBICS specifications. These protocols are likewise to be made available by the Deutsche Bundesbank and by the payment service provider for ten business days.

5.3 Backup procedure

For EBICS communication with payment service providers, the backup procedure is to send the messages by data telecommunication on the next business day.

6 Test requirements

Please consult the "Annex on testing the procedural rules for communicating via EBICS with deposit-taking credit institutions and other account holders with a bank sort code" for further information on the testing procedure.

DEUTSCHE BUNDESBANK
EUROSYSTEM

Annex on testing the Deutsche Bundesbank's procedural rules for communicating via EBICS with deposit-taking credit institutions and other account holders with a bank sort code

Table of contents

Admission to the procedure and test procedure

1 General

Outlined below are the framework conditions for the tests which have to be performed successfully by the Deutsche Bundesbank and a participant or an IT service provider commissioned by that participant to act on its behalf (hereinafter referred to solely as "the participant"), prior to going live.

When conducting the test, it is important to verify whether the software used by the participant conforms with the stipulations set out in the procedural rules. This can be done using designated sample test scenarios (see section 5).

2 Registering for the test

The participant must apply for the test procedure using the online application form on the Bundesbank's website.

www.bundesbank.de → Tasks → Payment systems → Services → Customer Test Centre → Test procedure

The specialised application-specific data required for the test procedure are taken from the applications for productive participation, which must be submitted via the responsible Bundesbank customer service team.

3 Testing

Authorisation to participate in the tests is strictly restricted to participants meeting the following criteria

- The necessary infrastructure (notably hardware, software, communication channel) is in place.
- The required communication channels with the Bundesbank have been established (see No 4).
- In-house quality assurance tests have been carried out successfully.
- Registration with the Bundesbank as a test participant stating the required data (BIC, sort code, contact(s), etc) is complete (see No 2 regarding the online form).
- All the necessary production forms have been submitted according to the procedural rules.

The tests are coordinated by the Bundesbank's Customer Test Centre.

Customer Test Centre Z 421
Postfach 10 11 48
40002 Düsseldorf, Germany
Tel: +49 211 874 2343
E-mail: testzentrum@bundesbank.de

4 Initialising the EBICS connection

4.1 Payment service provider ⇨ Deutsche Bundesbank

Order	Description
HIA	Send the public authentication key and public encryption key
INI	Send the public bank-specific key
HPB	Collect the Bundesbank's or payment service provider's public keys

4.2 Deutsche Bundesbank ⇨ payment service provider

Order	Description
HIA	Send the public authentication key and public encryption key
INI	Send the public bank-specific key
HPB	Collect the Bundesbank's or payment service provider's public keys

4.3 Download transactions (in both directions)

Order	Description
HAC	Collect customer protocols after initialisation

5 Exchanging data via the EBICS connection – sample test scenarios

At this stage, it is necessary to test the successful exchange of data via EBICS using the individual specialised procedure(s) applied for.

The target applications of the Bundesbank are

- RPS SEPA-Clearer (SCL)
- RPS cheque processing service
- Customer Access Mechanism (CAM)
- Electronic account information (KTO2/EAI)

based on the data formats described in the respective procedural rules. The test master data and test scenarios required in each case are determined by the Customer Test Centre in consultation with the test participants.

6 Test definition and contents

It should be noted that the test data transmitted to the Bundesbank during the authorisation and compliance tests are anonymised real data and that the submitting party is responsible for anonymising them. The Bundesbank reserves the right to use submitted test data, eg for tests with the recipient bank of a payment.

Normally, no data are forwarded to other CSMs during authorisation tests. If the customer wishes the payments to be settled in the T2 CUST environment, this must be arranged bilaterally with the test centre.

In addition to the test scenarios listed above, further discretionary tests may be performed at the request of the test participant, provided the necessary resources are available at the Customer Test Centre.

Participants must ensure that the test schedule is documented.

7 Initial certification and renewal of the test certificate

Participants receive a written notification confirming the successful completion of the required authorisation tests (initial certification). By the same token, the participant is required to confirm to the Bundesbank's test centre that the tests have been completed successfully.

This certification solely encompasses the sample test scenarios mentioned in No 5 and confirms the successful performance of the tests under the conditions (in particular with regard to hardware, software and the communication channel) applying at the time of testing.

If a participant makes adjustments after initial certification, in particular with regard to hardware, software or the communication channel, it must reapply for certification and reconfirm successful completion of the test.

The scope of the testing needed to reapply for certification is based on the sample test scenarios specified in No 5 and is to be coordinated between the respective participant and the Bundesbank’s Customer Test Centre on a case-by-case basis. Here, too, the participant in question is required to register for the test procedure in advance of the adjustments becoming operational (see No 2).