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 from 17 March 2024

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

1 DESCRIPTION OF THE PROCEDURE 4
2 SCOPE 4
3 ELIGIBILITY TO USE EBICS 5
4 ROLES OF COMMUNICATION PARTICIPANTS 6
5 DETAILED DESCRIPTION OF THE PROCEDURE 8
5.1 SECURITY PROCEDURES 8
5.1.1 GENERAL SPECIFICATIONS 8
5.1.2 OVERVIEW OF THE KEYS IN USE 9
5.1.2.1 USE OF SEPARATE CLIENT AND SERVER KEYS BY THE PAYMENT SERVICE PROVIDER 10
5.1.2.2 USE OF COMBINED CLIENT AND SERVER KEYS BY THE PAYMENT SERVICE PROVIDER 11
5.1.3 KEY MANAGEMENT 12
5.1.3.1 INITIALISATION 12
5.1.3.2 EXCHANGE OF KEYS 13
5.1.3.3 REVOCATION 13
5.1.4 TLS SERVER CERTIFICATES 14
5.1.4.1 GENERAL INFORMATION 14
5.1.4.2 FINGERPRINT COMPARISON 14
5.2 TECHNICAL DESCRIPTION OF THE PROCEDURE 14
5.2.1 EBICS PARAMETERS 14
5.2.2 ALLOCATION OF ORDER NUMBERS 15
5.2.3 UPLOAD TRANSACTIONS 15
5.2.3.1 DIRECTION OF TRANSFER: PAYMENT SERVICE PROVIDER -> DEUTSCHE BUNDESBANK 15
5.2.3.2 DIRECTION OF TRANSFER: DEUTSCHE BUNDESBANK ⇨ PAYMENT SERVICE PROVIDER 17
5.2.4 DOWNLOAD TRANSACTIONS 17
5.2.5 CUSTOMER PROTOCOLS 18
6 TEST REQUIREMENTS 20

REFERENCE DOCUMENTS

	Document	Title
1	Specifications for the EBICS connection	Annex 1 of the interface specifications for remote data communication 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 collections	The Deutsche Bundesbank's procedural rules for the clearing and settlement of SCC collections via the RPS SEPA-Clearer
7	Procedural rules for cheques	The Deutsche Bundesbank's procedural rules for the clearing and settlement of cheques via the Retail Payment System (RPS)
8	Procedural rules for accessing electronic account information	The Deutsche Bundesbank's procedural rules for accessing electronic account information
9	Bank Sort Code Guideline	Bankleitzahlen-Richtlinie
10	Interbank Tape	Abkommen über das Interbankenband

1 Description of the procedure

In cashless payments, the Deutsche Bundesbank makes a distinction between credit institutions within the meaning of Article 4(1) of Regulation (EU) No 575/2013 (deposit-taking credit institutions), for which the Deutsche Bundesbank operates MCA, DCA and cash handling 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 1, 2, 4 and 5 of the Payment Services Oversight Act (*Zahlungsdiensteaufsichtsgesetz* – 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 providers”), 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 exchange of data between banks efficiently, securely and cost-effectively.

Access is based on version 3.0.2 of the EBICS customer-bank standard (schema H005), earlier versions are not supported.

Therefore, for the clearing and 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 BTF (business transactions & formats) parameters specified by the Deutsche Bundesbank which enable the usual data formats to be transferred between banks.

The following procedural rules define the supplements 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 remote data communication 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

In addition, the bank sort code file and the interbank tape can be transmitted via EBICS from the Deutsche Bundesbank to the payment service providers.

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 can use 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/Services/Forms" on the Deutsche Bundesbank's website (www.bundesbank.de/en). They are to be submitted to the responsible Deutsche Bundesbank customer service team. Institutions with branch networks 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 (i.e. information about the TLS server certificate and the hash values for the public keys of the EBICS banking system). The customer service team then passes the documents on to the responsible master data administrator. When submitting administrative order types INI and HIA electronically, it must be borne in mind that the validity of these orders expires after 120 hours. If the initialisation letters are not received by the Deutsche Bundesbank master data administrator by this deadline, they have to be resubmitted.

Where a computer service centre is used as a contact point, the key material used for securing EBICS transactions is exchanged with this computer service centre. This computer service centre is recorded in the master data of the Deutsche Bundesbank's EBICS system as the authorised customer and participant for the accounts of the payment service providers applying to use EBICS. The computer service centre receives the customer ID and participant ID required for submitting payments via EBICS.

Communication via EBICS is via 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, must be followed. In particular, the private cryptographic keys must be handled with the utmost care and attention. The software used must always be kept up to date. Furthermore, the EBICS security concept of EBICS SC must be observed.

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, i.e. communication always originates from the client. Accordingly, the EBICS protocol is based on a role scenario in which the payment service provider always assumes the passive role, i.e. 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 communication 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 submissions to the Deutsche Bundesbank.

Conversely, the Deutsche Bundesbank always assumes the active role in the case of outgoing data deliveries to payment service providers. In terms of the terminology used in the EBICS specifications, 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 implemented by the payment service provider depends on how that provider implements it. A communication system implementing this role scenario 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 in participant initialisation so that the banking system's public keys are "made available for collection". There is no provision for "actively" sending them.

(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 order to which the customer protocol refers. Similarly, in the case of deliveries, 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 EBICS specifications:

- the transfer of the BTF parameters to the Deutsche Bundesbank;
- the result of the electronic signature authentication 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 is stated;
- a check of the hash values attached to the public bank-specific key upon first use of 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 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 submission 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. The corresponding messages are described in the respective procedural rules.

Computer service centres

Where 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 participant ID required for submitting payments via EBICS communication. A check is carried out on the signatures of the computer service centre. By virtue of this 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 carry out the account authorisation check. Where files are submitted 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 based on 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 transactions via EBICS. As with the provisions set out in the EBICS specifications, three RSA key pairs (key length: at least 2048 bits) are provided for each participant:

- public / private bank-specific keys;
- public / private authentication keys;
- public / private encryption keys.

One pair of keys is used exclusively for the bank-specific signature of orders. A single 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 orders 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 order code “DZHNN” be used for send orders.

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 EBICS specifications.

Download transactions constitute an exception to the rule of securing all data with an electronic signature. Collection data can be requested using the order code “DZHNN” until the payment service provider’s electronic signature has been implemented.

The security procedures of EBICS version 3.0.2 listed below are permitted:

- authentication signature in accordance with “X002”;
- encryption in accordance with “E002”;
- electronic signature in accordance with 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 is merely to show 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 used 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.

[1] Currently only envisaged in EBICS.

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 depends on what is implemented by the payment service provider. It may be the case that a payment service provider uses one 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.

5.1.2.2 Use of combined client and server keys 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 used 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 depends on what is implemented by the payment service provider. It may be the case that a payment service provider uses one 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 carried out using administrative order types "INI" and "HIA" as per the requirements of the EBICS specifications.

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 administrative 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 encryption and the authentication signature are delivered with the administrative order type "HPB"; the signature key will not be provided. Once this stage is complete, the payment service provider will be able to transmit send orders 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 is done in the same way as when the payment service provider initialises itself in the Deutsche Bundesbank's EBICS system, i.e. using administrative order types "INI" and "HIA". For this, the Deutsche Bundesbank requires the payment service provider's bank 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 administrative 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 email sent to the functional 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/en > Tasks > Payment systems > Publications > Procedural rules. The payment service provider is required to collect and activate the new public keys for submission using administrative order type “HPB”.

Where a new public key is introduced 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 itself will update the public keys in the payment service provider's EBICS system for delivery using administrative 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 itself is responsible for updating the keys for submission in the Deutsche Bundesbank's EBICS system using administrative 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 keys are updated by the Deutsche Bundesbank using administrative order type “HPB”, and the new keys are then activated once the new hash values have been positively verified.

5.1.3.3 Revocation

The Deutsche Bundesbank is to be informed without delay if a payment service provider's active keys are compromised. At the same time, the affected keys must also be revoked. The keys can be revoked in one of two ways:

- By written instruction to the Deutsche Bundesbank, Central Office, Z 201-2 (fax: +49 (0)69 9566 50 8067) to have the relevant public keys revoked. This instruction must be signed by authorised representatives or signatories.
- By revoking the keys in the Deutsche Bundesbank's EBICS system using administrative order type “SPR”.

The immediate result of a revocation order using order type “SPR” is that all deliveries secured with the revoked keys are rejected. In addition, the affected public keys should also be revoked in 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 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 likewise requires customers to produce certificates issued by a commercial trust centre. Certificates deposited by customers are automatically checked for validity once a day by the Deutsche Bundesbank. This is carried out, first, by checking them against the certificate revocation list (CRL) stored in the certificate and, second, by checking the certificate’s validity date. If a certificate is on the CRL, or the CRL is not available, or the validity of a certificate has expired and a new certificate cannot be obtained, the customer must arrange for the certificate to be exchanged without delay. If, in the case of a revoked certificate, communication is to continue by means of that certificate, the customer should provide the Deutsche Bundesbank with written confirmation to this effect (by email or fax).

According to a recommendation issued by the Federal Office for Information Security,[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 EBICS specifications are used for communication between a payment service provider and the Deutsche Bundesbank. Here, the participant ID and the

[2] BSI TR-02102-2

customer ID of the Deutsche Bundesbank are entered as standard and made known 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 requirements 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 administrative order type "HPD".

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

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

Technical business transactions are sent using BTF (business transactions & formats) parameter values. The relevant BTF parameter values for business correspondence with the Deutsche Bundesbank can be found in the annex.

5.2.2 Allocation of order numbers

The specifications for the EBICS connection stipulate that 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.

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 Bundesbank first reviews the order parameters. In the event of an invalid administrative order type or a non-permitted combination of BTF parameter values, the transaction is returned with the technical return code "EBICS_INVALID_ORDER_IDENTIFIER", or "EBICS_UNSUPPORTED_ORDER_TYPE" for an order that is valid but not supported by the Bundesbank. Therefore, to avoid returns, only the combinations of BTF parameter values defined in the annex should be used when communicating with the Deutsche Bundesbank. Filling optional fields for MessageName in the BTF parameters will likewise result in orders being rejected.

Having successfully checked the order parameters, the Deutsche Bundesbank checks the hash value of the currently valid public key. Should the result of the check prove negative during the period in which 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 generation of a new key and the system registers that the old key is being used. The error message states that the old key has been used and the need to update it. In addition, a one-off entry is made in the customer protocol to flag the outdated public key. The rejected file must then be resubmitted using either the old or the new key.

Further orders can be sent by the payment service provider during the changeover 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 protocol.

Subsequently, EBICS participant-specific authorisation checks are performed. The results of further bank-specific validation checks, e.g. account authorisation checks, are conveyed to the payment service provider at a later date as part of the customer protocol. The Deutsche Bundesbank does not check whether duplicate submissions have been made based on the hash value of the submitted order.

Transaction initialisation is carried out in accordance with the EBICS standard. As the Deutsche Bundesbank does not currently provide a public signature key for submissions with the administrative 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 re-sent.

For the delivery of files, only the order attribute “OZHNN” is permitted. The following keys are used:

Scenario 1: payment service provider uses separate keys

	Deutsche Bundesbank		**Payment service provider**	
	Signing, encrypting	Checking, decrypting	Signing, encrypting	Checking, decrypting
Authentication	BASs	KACp	KACs	BASp
Encryption	-	BVSs	BVSp	-
Electronic signature	-	KECp	KECs	-

Table 4: Separate keys for submission

Scenario 2: payment service provider uses combined keys

	Deutsche Bundesbank		**Payment service provider**	
	Signing, encrypting	Checking, decrypting	Signing, encrypting	Checking, decrypting
Authentication	BASs	KAp	KAs	BASp
Encryption	-	BVSs	BVSp	-
Electronic signature	-	KEp	KEs	-

Table 5: 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. In live operations, use of standard port 443 is mandatory for secure communication with the Deutsche Bundesbank via https.

Transactions are initialised in accordance with the EBICS standard. As no payment service provider public signature keys with the administrative 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.

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

The data are delivered with the order attribute "OZHNN" only. The following keys are used:

Scenario 1: payment service provider uses separate keys

	Deutsche Bundesbank		**Payment service provider**	
	Signing, encrypting	Checking, decrypting	Signing, encrypting	Checking, decrypting
Authentication	BACs	KASp	KASs	BACp
Encryption	KVSp	-	-	KVSs
Electronic signature	BECs	-	-	BECp

Table 6: Separate keys for deliveries

Scenario 2: payment service provider uses combined keys

	Deutsche Bundesbank		**Payment service provider**	
	Signing, encrypting	Checking, decrypting	Signing, encrypting	Checking, decrypting
Authentication	BACs	KAp	KAs	BACp
Encryption	KVp	-	-	KVs
Electronic signature	BECs	-	-	BECp

Table 7: 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 administrative order types are implemented as download transactions:

Order identification	Description
HPB	Collect the Deutsche Bundesbank's or payment service provider's public keys
HPD	Collect bank parameters
HAC	Access customer protocol (XML format)
HKD	Collect customer and participant information
HTD	Access customer and participant information

Table 8: Order types for collections from the EBICS system

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

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

5.2.5 Customer protocols

Customer protocols are made available for download using administrative order type “HAC”.

Access to customer protocols with administrative order type “HAC” must 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, i.e. through the addition of the administrative order type “HAC”.

The Deutsche Bundesbank's customer protocol is EBICS-compliant according to section 10 of the Specifications for the EBICS connection (HAC).

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 orders for the BIC specified in the tag `<SndgInst>` of the file header, the order will be rejected with the participant-related error code DS0H “NotAllowedAccount” (unauthorised signatory). Customer protocols can be accessed for a maximum of ten business days.

A receiving payment service provider, meanwhile, has to create an EBICS customer protocol for the data delivered by the Deutsche Bundesbank in accordance with the EBICS specifications. It must likewise ensure that a customer protocol file notification is created for each order. The file notification should be structured in line with the descriptions of the Deutsche Bundesbank customer protocol (tables 9 to 12).

For submissions to the Deutsche Bundesbank's technical applications, a file notification is displayed in the customer protocol.

The file notification for submissions to the SEPA-Clearer and cheque processing service 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` [3]
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` = „IQF":
		`NumCNRBlk + NumRMPBlk + NumROQBlk + NumSRBlk`

Sender's file reference	File reference	`FileRef`

Table 9: Structure of the customer protocol file notification for submissions to the RPS SEPA-Clearer and the RPS cheque processing service

Sample content of an INPUT CREDIT 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>
…
```

[3] The BIC of the SEPA-Clearer is entered here as the sending institution (in live operations: MARKDEFF).

<u>For MA files (interim transaction volume and balance enquiry), the file notification is structured as follows:</u>

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

The protocols are to be kept available for access by the Deutsche Bundesbank for at least ten business days.

Key management and the other administrative order types must be logged in accordance with the EBICS specifications. These protocols will be kept by the Deutsche Bundesbank for ten business days and should also be kept available by the payment service provider for ten business days.

6 Test requirements

Please consult the "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" for further information on the testing procedure.

Annex

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 3
1 General 3
2 Registering for the test 3
3 Testing 3
4 Initialising the EBICS connection 4
4.1 Payment service provider ⇨ Deutsche Bundesbank 4
4.2 Deutsche Bundesbank ⇨ payment service provider 4
4.3 Download transactions (in both directions) 4
5 Exchanging data via the EBICS connection – sample test scenarios 4
6 Test definition and contents 4
7 Initial certification and renewal of the test certificate 5

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 401
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
- 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 Test 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.

The scope of the certification refers exclusively to test cases carried out 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.

Changes to EBICS access (hardware, software, or change of provider) or extensions to the range of services (e.g. Addition of another service) require a further acceptance test by the customer test center prior to the start of production. To this end, a test procedure must be agreed with the customer test center at an early stage. Formal registration is also carried out via the online registration form on the Bundesbank’s website. The scope of the tests required for the follow-up certification is to be agreed individually between the participant in question and the Bundesbank’s customer test center.

Purely technical parameter changes, such as the URL or the host ID, must be coordinated directly with the Deutsche Bundesbank, Central Office, Z 201-2 (ebics-stammdaten@bundesbank.de).

Order type	U/D	Brief description	Service/ name	Service/ scope	Service/ option	Service/ msg. name	Container type (container flag)
SEPA and XML formats							
QC1	U	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)	SCT	BBK		icf	
QC4	U	INPUT INQUIRY FILE FOR SCT (IQF) Claim of non-receipt (camt.027) Request for value date correction (camt.087) Resolution of investigation (camt.029) Payment status request (pacs.028)	SCT	BBK		iqf	
QD5	U	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)	SDD	BBK	COR	idf	
QD6	U	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 returns/refund (pacs.004 SDD)	SDD	BBK	B2B	idf	

Order type	U/D	Brief description	Service/ name	Service/ scope	Service/ option	Service/ msg. name	Container type (container flag)
QK1	U	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)	SCC	BBK		idf	
QS1	U	SVV BSE INPUT DEBIT FILE BSE cheque (pacs.003 SVV) BSE reversal (pacs.004 SVV)	CHQ	BBK	0BSE	idf	
QS2	U	SVV ISE INPUT DEBIT FILE ISE cheque (pacs.003 SVV)	CHQ	BBK	0ISE	idf	
QS3	U	SVV ISR INPUT DEBIT FILE ISE reversal (pacs.004 SVV)	CHQ	BBK	0ISR	idf	

EKI

QMA		MA file, interim transaction volume and balance enquiry	OTH	BBK		mt920bbksw	

Order type	U/D	Brief description	Service/ name	Service/ scope	Service/ option	Service/ msg. name	Container type (container flag)
SEPA and XML formats							
QC2	U	CREDIT VALIDATION FILE (CVF) SEPA reject credit transfer by the SEPA-Clearer (pacs.002 SCLSCT)	SCT	BBK		cvf	
QC3	U	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)	SCT	BBK		scf	
QC5	U	INQUIRY VALIDATION FILE FOR SCT (QVF) SEPA reject credit transfer by the SEPA-Clearer (pacs.002 SCLSCT)	SCT	BBK		qvf	
QC6	U	OUTPUT INQUIRY FILE FOR SCT (OQF) Claim of non-receipt (camt.027) Request for value date correction (camt.087) Resolution of investigation (camt.029) Payment status request (pacs.028)	SCT	BBK		oqf	
QK2	U	SCC DEBIT VALIDATION FILE (SCC DVF) SCC reject card clearing collection by the SEPA-Clearer (pacs.002SCLSCC)	SCC	BBK		dvf	
QK3	U	SCC DEBIT NOTIFICATION FILE (SCC DNF) Interbank card clearing collection (pacs.003 SCC) Supplementary data field (supl.017)	SCC	BBK		dnf	
QK4	U	SCC SETTLED DEBIT FILE (SCC SDF) Interbank reversal (pacs.007 SCC) Interbank return/refund (pacs.004 SCC) Supplementary data field (supl.017)	SCC	BBK		sdf	
QK5	U	SCC UNSETTLED DEBIT FILE (UDF) SEPA direct debit (pac.003) SEPA return/refund (pacs.004)	SCC	BBK		udf	

Order type	U/D	Brief description	Service/ name	Service/ scope	Service/ option	Service/ msg. name	Container type (container flag)
QK6	U	SCC RESULT OF SETTLEMENT FIEL (RSF) SEPA reject (pacs.002SCLSCC)	SCC	BBK		rsf	
QR1	U	DAILY RECONCILIATION REPORT FOR CREDIT TRANSFERS (DRC) – not XML format –	REP	BBK		drc	
QR5	U	DAILY RECONCILIATION REPORT FOR SCC (DRR SCC) - not XML format -	REP	BBK		drr	
QR9	U	DAILY RECONCILIATION REPORT FOR SCT INQUIRY (DRQ)	REP	BBK		drq	
QD7	U	DEBIT CORE VALIDATION FILE (DVF) SEPA reject direct debit by the SEPA-Clearer (pacs.002 SCLSDD)	SDD	BBK	COR	dvf	
QD8	U	DEBIT CORE NOTIFICATION FILE (DNF) SEPA direct debit (pacs.003) SEPA payment cancellation request (camt.056 SDD) SEPA reject (pacs.002)	SDD	BBK	COR	dnf	
QD9	U	SETTLED CORE DEBIT FILE (SDF) SEPA return/refund (pacs.004 SDD) SEPA reversal (pacs.007)	SDD	BBK	COR	sdf	
QDA	U	DEBIT B2B VALIDATION FILE (DVF) SEPA reject direct debit by the SEPA-Clearer (pacs.002 SCLSDD)	SDD	BBK	B2B	dvf	
QDB	U	DEBIT B2B NOTIFICATION FILE (DNF) SEPA direct debit (pacs.003) SEPA payment cancellation request (camt.056 SDD) SEPA reject (pacs.002)	SDD	BBK	B2B	dnf	
QDC	U	SETTLED B2B DEBIT FILE (SDF) SEPA return (pacs.004 SDD) SEPA reversal (pacs.007)	SDD	BBK	B2B	sdf	
QDD	U	UNSETTLED DEBIT CORE FILE (UDF) SEPA reject (pacs.002SDD) SEPA direct debit (pacs.003) SEPA return/refund (pacs.004SDD)	SDD	BBK	COR	udf	

Order type	U/D	Brief description	Service/ name	Service/ scope	Service/ option	Service/ msg. name	Container type (container flag)
QDE	U	UNSETTLED DEBIT B2B FILE (UDF) SEPA reject (pacs.002SDD) SEPA direct debit (pacs.003) SEPA return/refund (pacs.004SDD)	SDD	BBK	B2B	udf	
QDF	U	RESULT OF SETTLEMENT CORE FILE (RSF) SEPA reject (pacs.002SCLSDD)	SDD	BBK	COR	rsf	
QDG	U	RESULT OF SETTLEMENT B2B FILE (RSF) SEPA reject (pacs.002SCLSDD)	SDD	BBK	B2B	rsf	
QR3	U	DAILY RECONCILIATION REPORT FOR CORE DIRECT DEBITS (DRD CORE) - not XML format -	REP	BBK	COR	drd	
QR4	U	DAILY RECONCILIATION REPORT FOR B2B DIRECT DEBITS (DRD B2B) - not XML format -	REP	BBK	B2B	drd	
QSD	U	SEPA-Clearer directory provided in the rocs data record format of the European Automated Clearing House Association (EACHA)	REP	BBK		rocs.001	
QS4	U	SVV BSE DEBIT VALIDATION FILE BSE reject by the Deutsche Bundesbank (pacs.002 SVV)	CHQ	BBK	0BSE	dvf	
QS5	U	SVV BSE DEBIT NOTIFICATION FILE BSE cheque (pacs.003 SVV)	CHQ	BBK	0BSE	dnf	
QS6	U	SVV BSE SETTLED DEBIT FILE BSE reversal (pacs.004 SVV)	CHQ	BBK	0BSE	sdf	
QS7	U	SVV ISE DEBIT VALIDATION FILE ISE reject by the Deutsche Bundesbank (pacs.002 SVV)	CHQ	BBK	0ISE	dvf	
QS8	U	SVV ISE DEBIT NOTIFICATION FILE ISE cheque (pacs.003 SVV)	CHQ	BBK	0ISE	dnf	
QS9	U	SVV ISR SETTLED DEBIT FILE ISE reversal (pacs.004 SVV)	CHQ	BBK	0ISR	sdf	
QSA	U	SVV ISR DEBIT VALIDATION FILE ISE reversal reject by the Deutsche Bundesbank (pacs.002 SVV)	CHQ	BBK	0ISR	dvf	

Order type	U/D	Brief description	Service/ name	Service/ scope	Service/ option	Service/ msg. name	Container type (container flag)
QSB	U	SVV BSE UNSETTLED DEBIT FILE (UDF) BSE cheque (pacs.003SVV) BSE reversal (pacs.004 SVV)	CHQ	BBK	0BSE	udf	
QSC	U	SVV ISE UNSETTLED DEBIT FILE (UDF) ISE cheque (pacs.003SVV)	CHQ	BBK	0ISE	udf	
QSE	U	SVV ISR UNSETTLED DEBIT FILE (UDF) ISE reversal (pacs.004 SVV)	CHQ	BBK	0ISR	udf	
QSF	U	SVV BSE RESULT OF SETTLEMENT FILE (RSF) BSE reject by the Deutsche Bundesbank (pacs.002 SVV)	CHQ	BBK	0BSE	rsf	
QSG	U	SVV ISE RESULT OF SETTLEMENT FILE (RSF) ISE reject by the Deutsche Bundesbank (pacs.002 SVV)	CHQ	BBK	0ISE	rsf	
QSH	U	SVV ISR RESULT OF SETTLEMENT FILE (RSF) ISE reversal reject by the Deutsche Bundesbank (pacs.002 SVV)	CHQ	BBK	0ISR	rsf	
QR6	U	DAILY RECONCILIATION REPORT FOR SVV BSE (DRD BSE)	REP	BBK	0BSE	drd	
QR7	U	DAILY RECONCILIATION REPORT FOR SVV ISE (DRD ISE)	REP	BBK	0ISE	drd	
QR8	U	DAILY RECONCILIATION REPORT FOR SVV ISR (DRD ISR)	REP	BBK	0ISR	drd	
QBL	U	Bank Sort Code File (BBkBLEIT)	REP	BBK		bleit	
QBE	U	Bank Sort Code File extended (BBkBLEIT2)	REP	BBK		bleit2	
QBA	U	Interbank tape (BBkINTBA)	REP	BBK		intba	
Payment formats							
EKI							
QMU	U	Interim transaction volume and balance reports	STM	BBK		mt942bbksw	
QMK	U	End-of-day statement	EOP	BBK		mt940bbksw	
QMN	U	M3 file, notification that an MA file could not be processed	REP	BBK		m3bbksw	
Q52	U	Interim transaction volume report Interbank - camt.052 individual message	STM	BBK		camt.052	
Q53	U	End-of-day statement Interbank- camt.053 individual message	EOP	BBK		camt.053	