EBICS Compendium

Electronic Banking Internet Communication Standard

Document version:	7
Status:	Approved
Date:	20/04/2020

Version management for document **2020-04-20 EBICS 3.0 Compendium V7.0_EN.docx**

Name	Date	Docu-ment version	Remarks
Rolf Münster	01/03/2006	1	Initial version
….			
Michael Lembcke	20/04/2020	7	Additions: ■ Section 6.7: Description of real-time notifications added ■ Section 6.8.4: Reference to delta document on the one-step, message-based use of EBICS 3.0 in the RT1 service added ■ Section 9.5: Description of TRAVIC-Push-Server added

Table of contents

Foreword

At the CeBIT fair in 2006, the German *Central Credit Committee* (ZKA – renamed *German Banking Industry Committee* (DK)) presented an extension of the DFÜ Agreement (remote data transfer agreement) to the general public known as EBICS (Electronic Banking Internet Communication Standard). Today, this standard has been firmly established not only on the German market but also in France and Switzerland. In many other countries, too, EBICS has a good chance to become the European payment standard in the corporate-customer segment and in the interbank business.

Since 1st of January 2008 the EBICS has been binding for German financial institutions in the corporate-customer segment and since the beginning of 2011 it has completely replaced the old FTAM procedure. In France the migration from the ETEBAC standard to EBICS is complete as well.

On 17 November 2010, EBICS SCRL was founded with headquarters in Brussels as a company which holds the trademark rights and develops the standard. Members of EBICS SCRL are the umbrella organisations of the German credit sector which are joined together in the DK, the French financial institutions represented by the Comité Français d'Organisation et de Normalisation Bancaire (CFONB), the Swiss financial institutions and the SIX.

The current EBICS specification in version 3.0 is a milestone in the evolution of the standard. With the collective business transaction formats (BTF) a standardisation of the different national EBICS formats has been realised. Other features like certificates and electronic distributed signatures are now also available for all countries. The new EBICS 3.0 specification is valid as of 27 November 2018. Regardless of this date, however, the EBICS countries have specified different launch dates and conditions for the EBICS versions and their application.

In addition to the basic functions, i.e. the "internet communication" in the corporate customer segment in its broadest sense, EBICS offers many other features like the distributed signature or the authentication signature, and enables the use of certificates. Apart from that, EBICS is also being used successfully in the interbank sector. Currently EBICS' customer and interbank segments are being prepared for the support of instant payments.

The aim of this compendium is to offer the reader insight into the functions of EBICS. We begin by explaining the requirements which were decisive for the development of the standard from which the basic features of EBICS are derived. This is followed by a structured description of the functions of EBICS, including an analysis of the positioning of the standard in relation to other standards such as FinTS or SWIFT. Finally we examine the implementation of EBICS using the example of the TRAVIC product family.

If after working your way through these pages you, the reader, have gained a clear idea of what the transition to EBICS means for you and your company, the purpose of this document will have been fulfilled. We have attempted to

present the indeed highly complex connections as comprehensibly as possible. In any event, we hope you enjoy reading this compendium!

PPI AG, April 2020

1 Introduction

1.1 EBICS requirements

The term which captures the essential objective underlying the creation of the EBICS standard in 2006 is "evolution instead of revolution". Version 3.0 introduces the important topic of harmonisation since different dialects have emerged after the creation of the EBICS Company together with France and Switzerland.

Right from the beginning this key principle of evolution was applied to the EBICS specification which has meanwhile been implemented in market products. For all the innovative energy of the involved parties, one indispensable property had to be preserved: the multi-bank capability. This is evidenced by the current application scenarios in Germany, France and Switzerland. It is no surprise therefore that the specification concentrates precisely on the communication sector, on cryptographic functionalities for security and a number of necessary and particularly attractive new application functions such as the electronic distributed signature (EDS). Nor is it surprising that from the start EBICS was treated in Germany under the legal cover of the DFÜ Agreement as will become clear in the structure of the specification. The loss or mere restriction of the multi-bank capability would have been tantamount to a fragmentation of the market which would not have been in anyone's interests, especially that of corporate clients.

The new EBICS 3.0 specification is valid since 27 November 2018. With the help of EBICS 3.0, various EBICS dialects are now merging.

EBICS offers the following features:

Requirement	Description
Internet	EBICS is consistent in its focus on internet technologies. This aspect, which formerly had only applied to the communication sector, is a continuous thread working its way through the specification, and affects not only communication standards such as HTTP and TLS but also standards such as XML or XML signatures.

Requirement	Description
Security	Nowadays no reference can be made to the internet without mentioning the issue of security. Any departure from the safe haven of the quasi closed networks, in which the previous standards were used, must not be at the expense of security. This concerns a number of areas of implementation, i.e. firewall structures (also accounted for in the concept) and the area of signatures and encryption, as well as the fact that a security concept was drawn up and accepted in parallel to the standardisation.
Bandwidth	One of the greatest advantages is the decoupling of the communication protocol from the physical network so as to exploit the advantages of flexibility and, most notably, the higher line speeds.
Performance & profitability	At first sight the impression is easily gained that aspects such as performance or resources had nothing to do with the subject-specific specifications. However a closer inspection shows these to be decisive for the way in which a communication protocol is structured and implemented given that the order processing is also aligned to this. Therefore the protocol has been tailored to process large volumes of data and to help settle them quickly, securely and profitably. A further point is the use of standards in their original form. In this way, market products and components which are already in widespread use (e.g. the ZIP compression) can be deployed in the platform area. They also serve as a guarantee for optimum and profitable processing.
Technical knowledge	A number of new functions have also been introduced with EBICS, e.g. the electronic distributed signature (EDS). By now this function has become established among German customers via market products and can now be deployed with EBICS in a multi-banking context. With EBICS 3.0 this function is also available in other countries.
Migration	For the further dissemination of EBICS, the migration idea is essential. National forms exist in many European countries and almost everywhere there is a desire first, to ensure parallel operation of old and new systems and second, to create as little overhead as possible on the customer and institution side. Due to the intended harmonisation in the 3.0, a greater focus is put on the topic of migration.

Requirement	Description
Obligation	A task of the organisations which Germany had demanded right from the start was that EBICS be developed under the auspices of the DK (today the EBICS Company). Based on this, concrete obligations have been defined concerning the deadlines for implementing EBICS nationwide and for disconnecting the old standards. These obligations apply as much to Germany as to France.

1.2 Structure of the specification

To conclude this introduction we provide an overview of the structure of the specification and of the other agreement and specification texts accompanying it. The new EBICS 3.0 specification is in effect since 27 November 2018. At the same time the previous version 2.5 is also still valid.

As this version differs not only in its content but also in its structure from the previous one, both versions are to be described below.

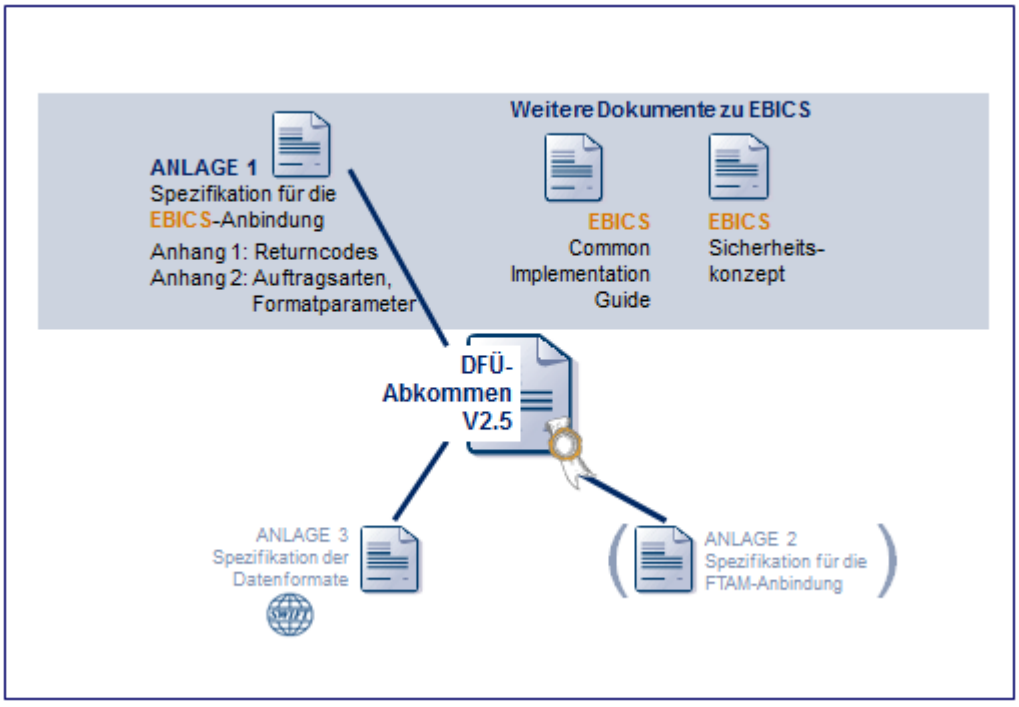


Figure 1: Structure of the EBICS specification 2.5 and embedding in the German DFÜ Agreement

The EBICS Company is responsible for editing annex 1 "EBICS" incl. the two appendices, and for publishing the documents under *ebics.org*. As a consequence of this, the specification itself will be edited in the original English text

and will be translated back into German and French. These documents can be accessed via *ebics.de* and *cfonb.org*.

In addition to the specification in annex 1, an Implementation Guide on EBICS is also available and in Germany a security concept may be obtained on request from the DK. Version 2.5 of the Implementation Guide was compiled once again from the German and French Versions and merged into a common document, In Switzerland, Six Payment Services has defined how to use EBICS in an implementation guide for the Swiss Banking Industry that can be found under *ebics.ch*. Moreover, business rules describing how to use ISO20022 payments in Switzerland were defined in another document. Thereby the demands for simple implementation and migration as well as a secure operation can be met.

Annex 3 of the DFÜ Agreement on the specification of data formats such as SWIFT or SEPA remains a German standard and has no relevance for the international EBICS activities.

Annex 2 on the specification of the FTAM procedure is meanwhile obsolete and has only been mentioned here to complete the picture.

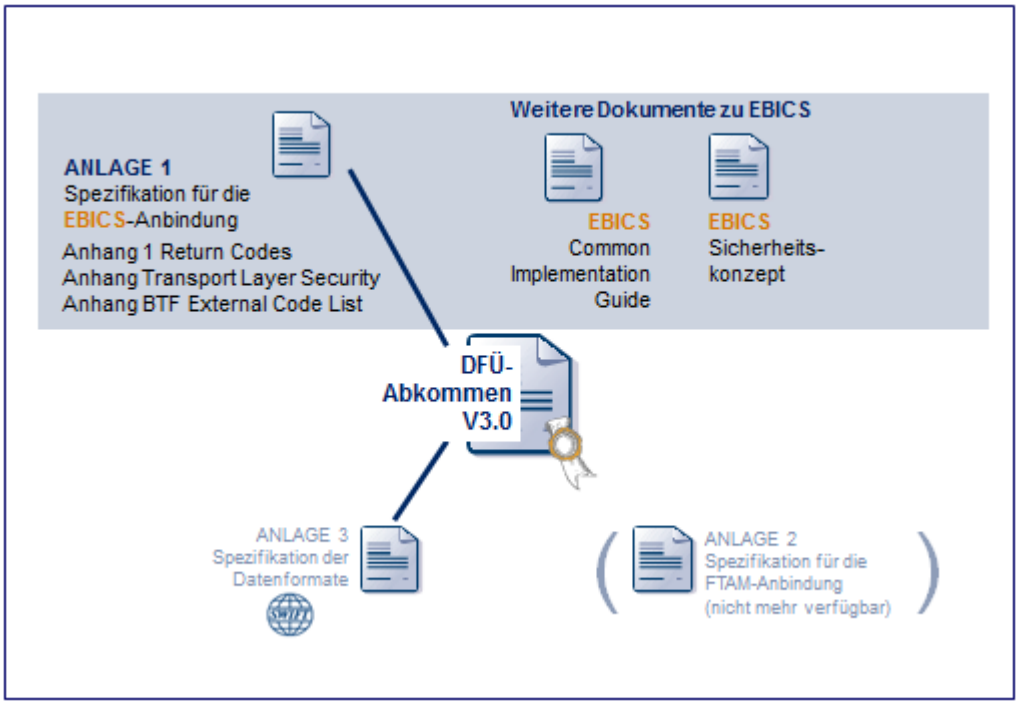


Figure 2: Structure of the EBICS specification 3.0 and embedding in the German DFÜ Agreement

At first glimpse the structure of the EBICS specification 3.0 hardly differs from that of the version 2.5. As was expected, the list of BTF codes replaces the old list of order types, with reference lists for both conversions available under *ebics.de*.

An important step is the outsourcing of Transport Layer Security. This also indicates that the focus of the basic EBICS specification is on the user-specific protocol content.

1.3 Complimentary documents

In addition to the official EBICS specification, other complimentary documents for the varying application scenarios are available.

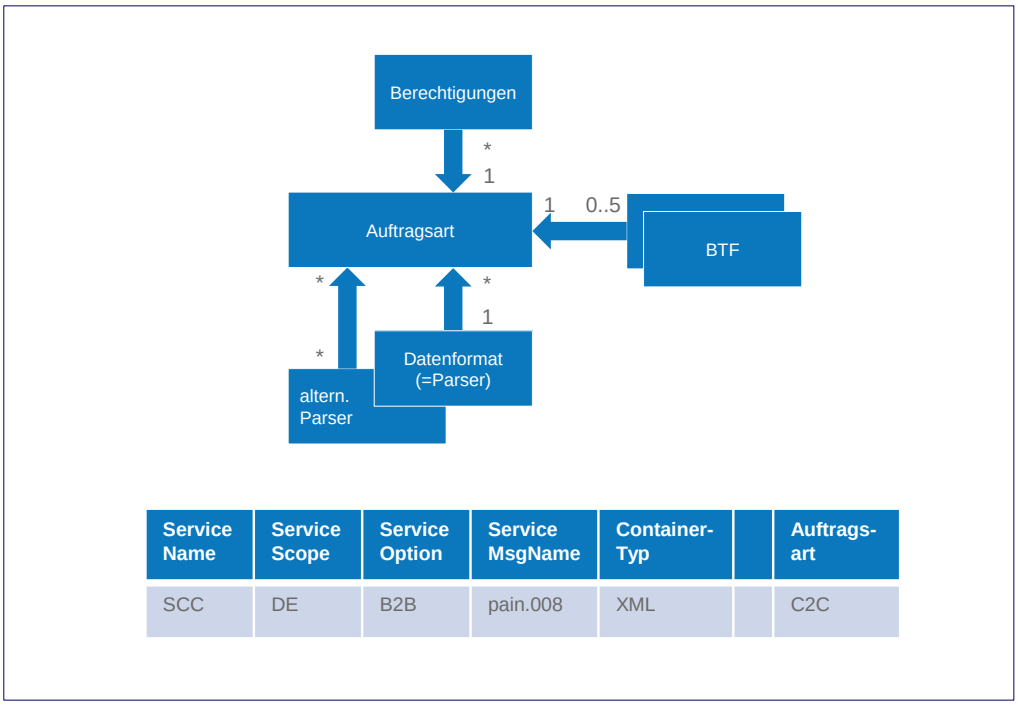
Author	Document
Bundesbank	„EBICS procedural rules“ ■ Hash value ■ Fingerprint ■ Implementation guide freely available on the internet
EBA Clearing	EBA STEP2 EBICS Procedural Rules
EBA Clearing	RT1 System - SCT Inst Service Network Interfaces
Berlin Group	EBA Cards Clearing (ECC)
German Banking Industry Committee	Guidelines on SDC procedure (German: SRZ-Verfahren)
CFONB	Implementation Guide Version 2.1.5 www.cfonb.org
SIX Group	SIX Implementation Guide https://www.six-interbank-clearing.com/de/home/standardization/ebics.html

2 EBICS overall scenario

In this section, we present an exemplary overall scenario. The objective is to create an understanding of the intricate manoeuvrings involved in the smooth and uninterrupted migration of a stable existing infrastructure and an already established internet platform based on market products to an EBICS target system.

2.1 Interplay of EBICS 3.0 and previous versions

Certain requirements have to be met for the implementation of EBICS 3.0 because customers can also use the EBICS 2.5 during the transition period. The primary goal for the implementation has to be the compliance with all requirements according to the EBICS specification 3.0, to realise a step-by-step harmonisation. Thereby, the impact on the customer contracts and the conversion effort for institutions and manufacturers should be kept as low as possible.



Service Name	Service Scope	Service Option	Service MsgName	Container-Typ		Auftrags-art
SCC	DE	B2B	pain.008	XML		C2C

Figure 3: Interplay/Mapping between BTF and order types

In general, the following topics are relevant for the interplay:

- Unified certificate format
- Version compatibility included in the contract
- National BTF mappings
- Special case EDS and signature flag
- Retention of interfaces

- Cryptographic requirements

Unified certificate format

With EBICS 3.0 the only permitted certificate format will then be X.509. This means that at least the X.509 syntax as part of the H005 schema has to be supported. Due to the missing PKI infrastructure, for a certain transition period, CA-based certificates are not checked against the issuing CA if the DK profile is used. Regardless, the validity date of the certificate is checked locally against the current date.

Version compatibility included in the contract / BTF mappings

BTF is introduced in addition to the already known order types and file formats. For an institution this presents the situation that, according to the customer's installation, orders can be submitted in the two different EBICS versions 2.5 and 3.0. If certain requirements are met, a mapping between BTF and order type allows you to create BTF orders with the existing authorisation structure based on order types and thus ensures version compatibility.

Special case EDS and signature flag

VEU-Steuerung

Kundenvertrag	Auftrag	VEU?
erlaubt	erlaubt	ja
erlaubt	nicht erlaubt	nein
nicht erlaubt	erlaubt	nein
nicht erlaubt	nicht erlaubt	nein

Signatur-Flag

Auftragsartkonfiguration	Auftrag	Verarbeitung
O-Datei	Flag vorhanden	EU-Prüfung
O-Datei	Flag nicht vorhanden	ablehnen
nur D-Datei	Flag vorhanden	ablehnen
nur D-Datei	Flag nicht vorhanden	alternative Freigabe

Figure 4: EDS control and signature flag

As seen in the figure above, the customer contract, the order and the signature flag affect whether a submitted order without sufficient authorisation is rejected or send for EDS processing.

Maintaining the interfaces

The EBICS specification 3.0 opens the door for a wide harmonisation of Europe's EBICS landscape and also makes the standard more attractive for other countries.

Conversely, when introducing EBICS 3.0 into existing implementations, we have to make sure that the existing interfaces for application systems can be retained in order to enable a resource-efficient migration.

Cryptographic requirements

As you will see in later sections, some cryptographic procedures can no longer be supported by EBICS 3.0. This affects the authentication signature X001, the order signature A004 and the encryption procedure E001.

In addition, only RSA keys with at least 2048 bits shall be used.

After this description of the different versions' interplay, the following sections will only consider the current EBICS 3.0.

2.2 Inclusion of products

Anyone reading the EBICS specification for the first time quickly realises that it was not devised on the drawing board but that it optimally maps the scenarios encountered in practice. This is also attributable to the fact that before the specification was developed, products had already existed on the market which offered what might be termed as proof of concept. The common feature of all products was that they all showed possibilities of mapping mass payments for corporate customers on internet platforms. Furthermore, each product realised its own ideas for application extensions. Thus, thanks to this portfolio the optimal solutions were able to find their way into the EBICS standard, thereby avoiding the familiar round of beginner's mistakes. This also explains why at the time of introducing EBICS problems such as segmenting large messages had already been solved or why the concept for the electronic distributed signature already existed in a mature and proven form and therefore did not require supplementing or optimising in the course of its first practical application.

2.3 Portals

For some years now every institution has been offering browser-based corporate customer portals as part of their general offer. As EBICS is also based on internet technologies, it is fair to assume that these two worlds can be harmoniously merged. And this is indeed the case as long as we are dealing with an institution's own portal.

3 Communication and safeguarding the infrastructure

This section deals with the centrepiece of the EBICS standard, i.e. communication via the internet.

Introductory literature on the internet as communication protocol always attempts to force the TCP/IP protocol into the OSI stack to create historical comparability. To some extent this is possible and is also justifiable, but it is of no relevance for an analysis of the EBICS standard. The decisive point is that by making this step towards an internet platform, use can be made of infrastructures available on both the customer and the institution side, the efficiency of these infrastructures is many times greater than that offered by the former solution.

The use of internet technology also makes it possible for EBICS to line up more closely with other applications. As the corporate customer business in addition to mass payments also has many application areas in the transaction- or dialog-oriented field, an interplay with other services which are based, for example, on the second significant DK standard FinTS (Financial Transaction Services) is indispensable. This is greatly simplified by the use of shared platforms.

3.1 HTTPS and TLS – Transport Layer Security

While the TCP/IP protocol deals with tasks such as dynamic routing in the event of a sectional default, HTTP controls the session between two partners. The only version used for EBICS is the secured version HTTPS which is indicated in the browser by a lock in the lower corner. The responsibility for this security lies with TLS (Transport Layer Security) which replaces the former SSL (Secure Socket Layer).

The switch from SSL to TLS alludes to the general problem of fusing Internet technologies and their application standards: according to the German Federal Office for Information Security (BSI) by now the versions 1.0 and 1.1 of the TLS protocol are also considered to be obsolete and in need of replacement. Until now the integration of these standards in the EBICS specification did not allow for a lot of flexibility. With the introduction of EBICS 3.0 these security procedures of the transport layer have been transferred into a separate document that can be maintained independently from the business standard.

TLS in the current version 1.2 ensures a secure transmission between the customer system and the first HTTP or rather web server in the institution. It also fulfils this task sufficiently well and securely, although this was deemed insufficient by the EBICS standardisers, as is explained in the section after next.

3.2 XML – Extensible Markup Language

To make the following sections easier to understand, this section provides an explanation of the XML standard. In the case of BCS, it was still possible to

conceal the necessary protocol tasks in the file name, but for EBICS a separate protocol envelope is required due to the abundance of tasks. In the field of internet technology it is more advisable to use the data description language XML – Extensible Markup Language - for this purpose.

With EBICS each request or response consists of an order analogous to the defined order types or the BTF container respectively and an XML envelope. In other words it is a kind of hybrid system, with the bank-technical SEPA or SWIFT formats remaining the centrepiece while being supplemented by XML structures. The overhead caused by this technology is minimal when considering the mass payments usually being handled here and the vast size of the payment transaction file compared to the XML envelope.

The diagram below highlights all the XML schema defined in EBICS. These are stored according to the XML namespace concept under the associated addresses http://www.ebics.de/.

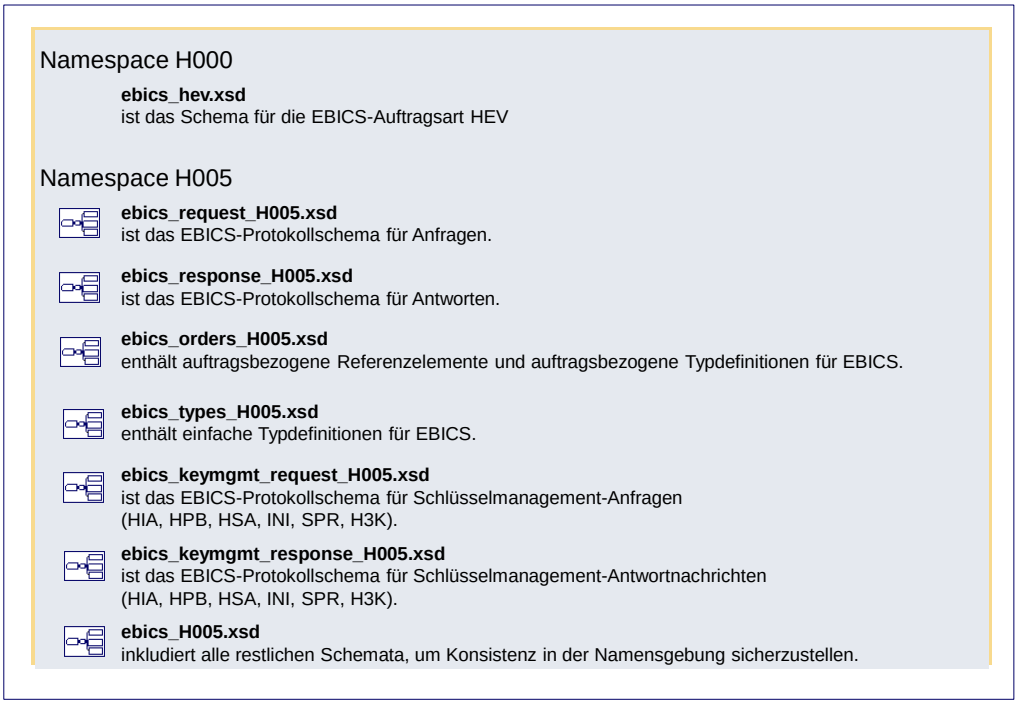


Figure 5: EBICS-XML schema 3.0

As can be seen, the schemas are clearly structured and the type definitions are separated from the subject-specific protocol schema.

The first schema is a special case. H000 is responsible for version administration and allows the customer product to be scanned to determine which protocol version the institution supports.

The diagram does not show the namespace S001, which contains the EBICS signature schema. You can find the latest versions of the EBICS schema on the official websites ebics.org and ebics.de.

3.3 Optimisation of communication

As a result of optimisation in the communication area, account could be taken of the special features of the internet.

EBICS offers the possibility of compressing transfer data. To do this, EBICS makes use of the license-free and widespread ZIP algorithm.

Large data volumes can be segmented in the EBICS protocol so as not to block the capacities of the internet instances on the institution side.

Thanks to the optional recovery capability of this protocol, it is also possible to intelligently retrieve a transaction if the data transmission was interrupted. This eradicates the need for duplicate transmission of segments transmitted once already.

EBICS also provides a procedure involving `nonce` and `timestamp` which makes it possible to recognise replays. A customer product generates a random nonce (i.e. an "ad hoc value") and inserts it together with a timestamp into the EBICS envelope. On the institution side, a list is drawn up of the nonces and timestamps already used by the subscriber to prevent duplicate submission of orders.

4 Data model

This section deals specifically with the data model used by EBICS. It can be found in the master data management of the various products and, as already mentioned with the migration process, scarcely differs from the original EBICS model.

Broadly speaking the following entities exist in the data model:

- Customer
- Account
- Subscriber
- Business transaction

The entry point in the nomenclature is the `customer`. This is the umbrella term e.g. for a company which on the one hand maintains several accounts at an institution while on the other hand granting several subscribers access to these accounts.

A `subscriber` could be, for example, an employee of a company acting on behalf of the customer. He is allocated a signature class which determines whether this subscriber may authorise orders, alone or jointly with other subscribers.

The following signature classes are supported:

- Signature class E Single signature

  No further signature required to authorise the order.

- Signature class A Single signature

  At least one other signature of the signature class B is needed. It does not matter in which order the signatures of the different classes are made.

- Signature class B Second signature

  At least one other signature of the signature class A is needed. It does not matter in which order the signatures of the different classes are made.

- Signature class T Transport signature

  Indicates that this is an authentication signature, e.g. of a technical subscriber.

A subscriber with signature class E, A or B is granted signature rights for certain accounts of the company, and order types are allocated to him for which he is specifically authorised.

In this way a flexible authority system can be established which is then mapped in the respective products on the customer and institution side.

The following diagram illustrates a simple form of the data model:

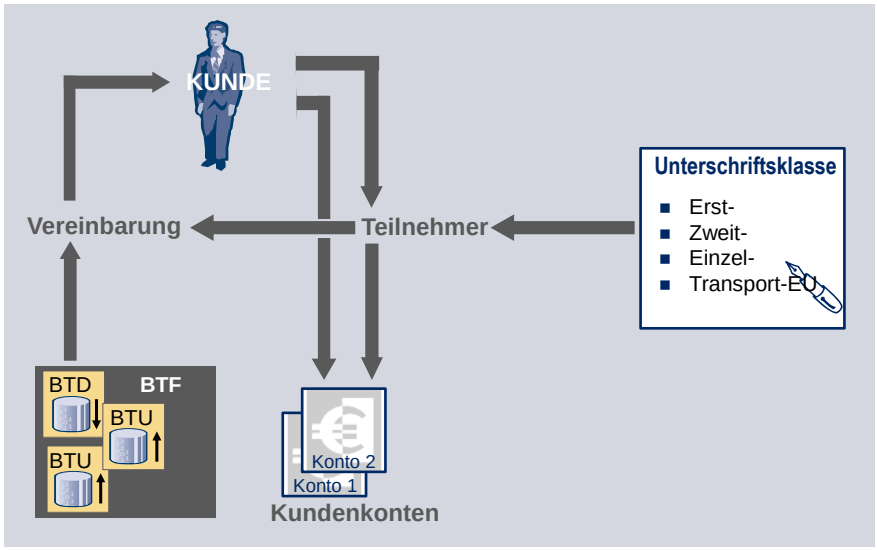


Diagram 6: Data model

When discussing the data model, reference should also be made to the bank parameter data and the user data. All the information for accessing the institution are contained in the bank parameter data, which can be retrieved from the EBICS server, along with the optional functions offered by the institution. These include, for example, the communication address (URL). The user data that is optionally offered by the institution contain customer- and subscriber-specific information such as authorised accounts, order types or message names.

5 Security

Already with the EBICS predecessor version 2.5 new security procedures A005 and A006 or X002 and E002 were introduced. Of greater importance, however, are the stipulations governing the obligation to actually implement these procedures - an innovation introduced with the EBICS standard.

Not considered are security media itself, e.g. smartcard, disk or, as is more common today, the USB flash drive. EBICS makes no stipulations here and leaves the choice of such media up to the customer or the manufacturers of the customer products. However, with the aid of the following classification the customer system can informally communicate which type of security medium the customer has used:

- No specification
- Disk
- Smartcard
- Other security medium
- Non-removable security medium

France makes high demands for the TS profile: the implementation guide dictates the use of special HW tokens for the TS profile, these need to be issued by a certification authority (CA). The tokens are implicitly transferred using the X.509 certificate (see below).

5.1 Infrastructure security

A key aspect for attaining a high level of infrastructure security is the consistent concept for signature and encryption in EBICS. Customer signatures are mandatory for EBICS. Provisions exist for bank signatures and they will be specifically defined once the legal implications have been regulated (i.e. the issue of person-related bank signature vs. company stamp). There is also the additional authentication signature X001 and X002.

EBICS is equally thorough when it comes to encryption: besides the obligatory encryption with TLS on the transport level, EBICS's own encryption procedure E002 (or E001, obsolete) is also compulsory so as to ensure end-to-end security.

In a special initialisation step in which preliminary checks can be optionally carried out, a transaction ID is also granted for the entire transaction. This enables the formation of a transaction bracket and is a precondition for segmentation when transmitting large volumes of data.

By making these stipulations, a level of security is reached which is appropriate to operations in the internet, the strength of which is also examined and attested in a corresponding security concept.

More details on the protocol features themselves can be found in the section *EBICS processing steps* on page 39.

5.2 Signature procedure

EBICS uses two different signatures:

- Authentication signatures to identify the submitting party
- Order signatures, electronic signature (ES) for bank-technical authorisation of orders

The two signature types differ fundamentally, as can be seen in the following diagram:

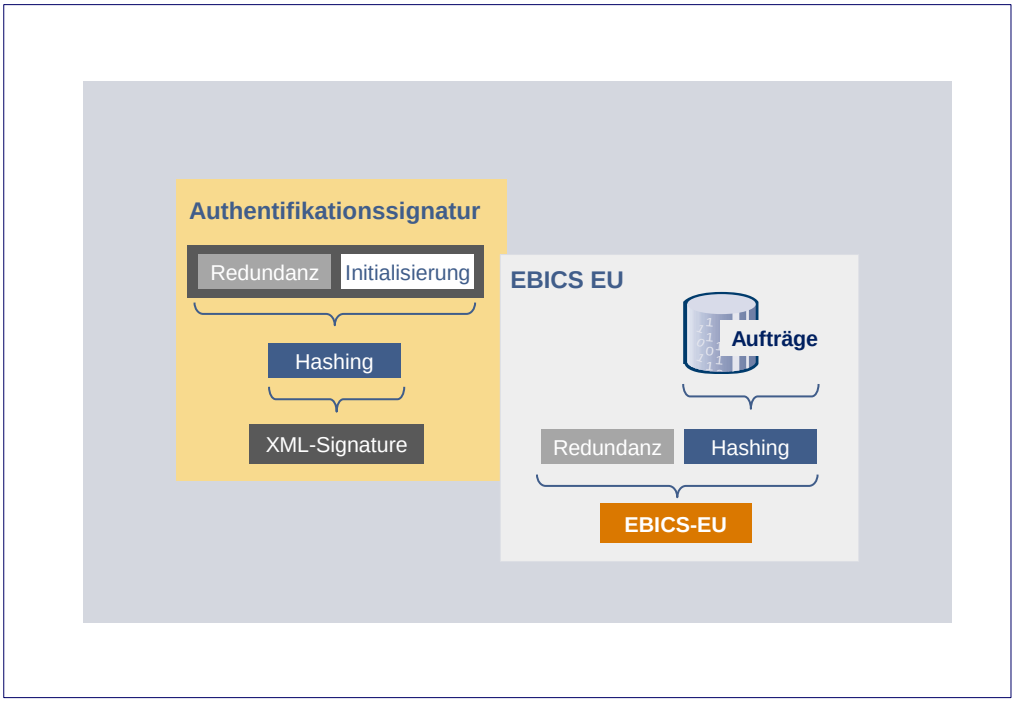


Diagram 7: EBICS Signature Procedure

5.2.1 Authentication signature X001 or X002

The purpose of the authentication signature is to unambiguously identify the submitting party. The authentication signature is checked during the initialisation step as well as in every subsequent transaction step, i.e. before the transmission of the actual order data (see section *EBICS processing steps*, page 39).

Subscribers who submit only orders can hold signature class T. This class also allows purely "technical subscribers" to be set up which are then only entitled to submit orders.

The formation of the authentication signature corresponds to the standard procedure in the transaction area. The orders are supplemented by dynamic information such as session ID, timestamp etc. so that for the same reference data different signatures can be received belonging to the special situation. Cryptologists use the term redundancy for this. Over the entire structure a cryptographic checksum is formed, the hash value. The most important feature of this hash value is its ability to create an exact value based on concrete predetermined data which practically no other data combination is able to create. A 1:1 relation is thus created between data and hash value.

Using this hash value a digital signature is formed with the aid of a signature key. A point that should be mentioned is that, before formation of the hash value, the data is padded up to a specific minimum length according to a predetermined algorithm to allow this mechanism to also function for small data volumes.

As this is a common procedure in the transaction business, it is also supported in the W3C Standard XML signature in this way. That is why analogous to the XML signature, EBICS supports the authentication signature in the standard X002 and X001 (obsolete) and as of EBICS 3.0 only in the standard X002.

5.2.2 Order signatures (ES) according to A004 and A005/A006

The electronic signature (ES) of an order on the customer side (and, in future, also on the institution side) has been carried out compulsory since EBICS 2.4 on the basis of the new procedures A005 and A006. Unlike signature formation for the authentication signature, the redundancy formation and hash value formation steps are interchanged. Due to the use of the hash value file as important, direct representation of the original data, the file is formed directly via the order file without redundancy and can thus be directly checked at any point.

For reasons of migration capability, EBICS demanded the RSA signature according to A004 for entry – with older signature types from the DFÜ Agreement no longer being supported. In procedure terms, A004 had already been customised to the current signature card of the German credit sector with SECCOS as operating system, but as already mentioned it also supported these procedures via disks or USB flash drives.

Of the procedures supported by SECCOS, a profile was supported for A004 comprising the following algorithms:

- RSA signature with key lengths of 1,024 bits
- Padding according to ISO9796-2
- Hash value procedure RIPEMD160

In common use today and also declared compulsory since EBICS 2.4, the more robust ES procedures A005 and A006 support the following attributes:

	A005	A006
Key length	(1.536) – 4.096 bits	(1.536) – 4.096 bits
Hash value procedure	SHA-256	SHA-256
Padding procedure	PKCS#1	PSS

The table reveals that A005 and A006 only differ in respect of the padding procedure.

From the explanation of the security procedure and the reference to the SECCOS smart card operating system, one might deduce that this part of the EBICS specification has a more typical German shaping. However, this is by no means the case. The DK's card strategy which is strictly aligned to the annually published voucherless cheque collection crypto-catalogue and, by extension, to the national shaping of the ES signature directive, guarantees that international standards are being deployed.

In general, for EBICS 3.0 the key length has to be at least 2048 bits. Still existing A004 keys need to be changed to match this criterion.

5.3 Initialisation

Before a key pair can be used, the authenticity of the partners must first be established via a suitable procedure. To achieve this, certificates are used or alternative procedures based on separate channels. While provisions exist in EBICS to support certificates according to X.509, in Germany use is still being made at the moment of the procedure based on the initialisation letter. France is already in possession of a regulated PKI infrastructure for the introduction of the EBICS standard. For this reason, certificates can also be used there for the initialisation process which since EBICS 2.5 has also been continuously supported by the standard.

Both concepts are briefly explained below; however, as evidenced in the fallback scenario in France the possibility still exists of the two worlds becoming intermingled.

5.3.1 Certificates in France

The foundation for a certificate-based procedure is laid by an appropriate Security Policy. This means that it is necessary to regulate which certificate issuer can be deemed as secure and at which level. In France, clear and published definitions exist for the use of certificates in EBICS. The highest security level applies to issuers of qualified certificates according to the European Signature Directive. In France, however, lower security levels are also sufficient for the pure exchange of payment transaction files as illustrated below.

In France use is made of the signature classes T and E. At the moment no distributed ES is supported. Instead two basic profiles exist for submission (T) and authorisation (E).

For the submission of certificates, use can be made of the new order type H3K, valid as of Version 2.5. The remaining processes for initialising a customer remain valid from the EBICS perspective.

- Submitting party profile T based on certificates

  The initialisation must not necessarily be performed by a listed certification authority (CA). Self-signed certificates of the institution with an INI letter are also allowed.

  If, however, the certificate is issued by a CA this authority must be listed on the Trusted List.

- Authorisation profile TS

  Use is made of electronic signatures for Transport and Signature. The procedure corresponds roughly to the ETEBAC 5 standard. In this case the certificate for the signature key must be issued and signed by a CA, and the CA must also be listed in the Trusted List. The certificates for the authentication and encryption key can also be self-signed.

  The certificate check is compulsory for the signature key while the check for certificates for the authentication and encryption key is run against the CA, provided the certificates were issued by a CA.

- INI letter as fall back scenario

  In France, INI letters are a part of the initialisation process when making use of certificates. Regardless of whether certificates are being used, the customer must at all events first send an INI letter.

  Non-CA based certificates are activated exclusively via the INI letter. The CA must permanently check the CA-based certificates. If the CA has successfully checked the certificate, additionally defined certificate specifications must be matched with the conveyed specifications of the submitting party. If the specifications do not match, manual activation is still possible – based on the specifications in the INI letter.

After being successfully checked and activated, the customer's certificate is saved in the application system. Future lock enquiries will be carried out on this basis – thus the customer need only submit the certificate once.

Independent of the authorisation and submission profiles that are common in France, EBICS 3.0 generally uses the certificate format for keys. For the moment, there will still be the different practices, so that the effect of harmonisation is not as pronounced yet.

5.3.2 INI letter procedure in Germany

For the INI letter procedure, a subscriber creates a key pair and conveys its public key with the order type INI (or HIA if the key is a public key for the au-

thentication signature or for the encryption) to the institution. Parallel to this, an initialisation letter is printed out containing administrative data, the public key and associated hash value. This initialisation letter is manually signed by the subscriber and sent by mail or fax to the institution where it is compared with the electronically conveyed data. If the data match, the key is activated and can now be used by the subscriber. The same procedure can be applied in reverse when the bank signature is introduced at a later date. In this case the subscriber will have the task of comparing the key data conveyed electronically and by post and confirming that the data match.

5.4 Encryption procedure

For EBICS use is made of duplicate encryption according to TLS and of EBICS's own procedure E001 and E002 in order to receive both the standard encryption in HTTPS as well as the end-to-end encryption. For E002, use is made of the AES procedure recommended by BSI since 2009.

5.4.1 TLS – Transport Layer Security

TLS is the successor of SSL. Both encryption protocols are able to guarantee authentication as well as encryption on one transport route. Corresponding implementations exist on the customer side e.g. in the internet browser and on the institution side in common web servers.

While setting up a TLS connection, certificates and supported procedures are exchanged between the partners and a session established on the basis of this.

In line with general practice, EBICS only uses the server authentication from TLS and is currently not supporting any TLS client certificates. The internet certificates generally deployed by the institutions are used as server certificates (i.e. those certified via VeriSign).

Encryption takes place in both directions. The only procedures supported are strong encryption procedures or cipher suites. Valid cipher suites can be found on the website of the Bundesbank or at ebics.de.

Here please note again, that with EBICS 3.0 the Transport Layer Security has been transferred into a different document.

5.4.2 Encryption E001 and E002

E001/E002 is a so-called hybrid procedure, i.e. consisting of asymmetric and symmetric algorithms. The basis for this is generally an asymmetric RSA key as encryption key. For performance reasons, the message itself is symmetrically encrypted. A dynamic key is used as key which – secured by the encryption key – is exchanged.

E001 uses a 1.024 bits encryption key and the padding algorithm PKCS#1. At the latest with the introduction of EBICS 3.0, E001 shall no longer be supported by the implementations. The reason for this is, among others, that the last

two EBICS versions have to be supported. With the introduction of EBICS 3.0 and the current 2.5, the old EBICS 2.4 and the E001 procedure (as well as X001 and A004) therefore become obsolete.

E002 was deployed as the next development in EBICS 2.4. Here, the transition from Triple-DES to AES is carried out (2009 recommendation of the BSI - Federal Office for Information Security in Germany).

6 EBICS business functions

EBICS offers new fields of application for the customer.

6.1 Order types

In the German DFÜ Agreement, the Swiss Implementation Guidelines and the format standards of the French CFONB the following fields of application are supported by operative order types and FileFormat parameters with EBICS and by the respective BTF with EBICS 3.0:

- SEPA and other national payments
- Foreign payments
- Securities trading
- Documentary credit business
- Information on daily account statements and other information on transactions booked and notifications of account movements (MT940/MT942 or camt XML and other formats)

In addition, EBICS 3.0 introduces the following new order types for BTF:

- BTD: administrative order type for downloading a file, described in more detail by the BTF structure
- BTU: administrative order type for sending a file, described in more detail by the BTF structure

6.1.1 SEPA payment transactions

EBICS supports order types and FileFormat parameters for SEPA payments customer-bank and bank-bank (Bundesbank and interbank STEP2). At the moment, the following SEPA messages are supported for the customer-bank interface:

- SEPA Credit Transfer Initiation
- SEPA Direct Debit Initiation
- Rejects Prior to Settlement

These messages are reflected in the corresponding EBICS order types, taking into consideration the following specifics.

In the course of implementing the SEPA messages for the DK, it was deemed reasonable to introduce extended formats in addition to the standard SEPA format. The extended formats can be used depending on the financial institution or use case. They relate specifically to collective orders with multiple group formations, such as ordering party accounts or execution dates which can be treated in differing ways (e.g. the treatment of several ordering party accounts):

- SEPA Standard Format

  Use of the SEPA standard format, subject to the restriction that the only orders possible are those for an ordering party account. To process orders from several ordering party accounts, several orders must be submitted in the SEPA standard format for this option.

- SEPA Container

  DK-specific protocol extension to enable the submission of several SEPA standard formats for several ordering party accounts within one order type

- Extended Grouping Options

  SEPA standard formats which offer the possibility of submitting orders for several ordering party accounts when using the extended grouping options in the SEPA format itself.

This breakdown over several forms can be explained by the optimised processing method for the various IT service providers.

The following table lists some of the SEPA order types used in Germany according to different forms:

Option	Order type	SEPA designation
SEPA data formats	CRZ	Payment Status Report for Credit Transfer
	CDZ	Payment Status Report for Direct Debit
Container	ZKA	Credit Transfer Initiation
	CRC	Payment Status Report for Credit Transfer
	CDC	Direct Debit Initiation
	CBC	Payment Status Report for Direct Debit
Extended grouping options	CCT	Credit Transfer Initiation
	CDD	Direct Debit Initiation

In addition to the mentioned SEPA order types, further order types were developed with different format characteristics to process the specific business transactions of the German Banking Industry Committee. These primarily include the order types for processing the national SDC procedure.

To give the full picture it is worth mentioning that the SWIFT formats MT940 and MT942 were adjusted to convey the SEPA-relevant data for SWIFT daily statements via the order type STA.

To map the payment transactions from SEPA orders without any loss of information, new download order types for camt formats (C52, C53 and C54) were introduced as equivalent to the MT94x messages (STA and PFM) and the DTAUS turnover information (DTI).

Details on the SEPA data formats and their application in Germany can be found in annex 3 of the DFÜ Agreement.

Depending on the country, outside of SEPA, different national payment formats with individually defined order types and FileFormat parameters can also be used.

6.1.2 ISO 20022

An important part of the present international electronic payments is the free and open standard "*ISO 20022: Financial Services – Universal financial industry message scheme*". The aim of this standard is to simplify and unify the global communication in the finance sector. Topics of the standardisation are, among others, the used terms, procedures and message formats. This facilitates a global exchange of finance information between different systems. The messages are exchanged between customer and financial institution or between financial institutions are represented as a XML document (Extensible Markup Language).[1] This is different in the former formats like the DTA format.

For this, many message types have been standardised through ISO 20022 and can be found here: https://www.iso20022.org/full_catalogue.page. For every type there is a formal specification of the available elements and structures in the form of XML schema files. For their unique identification each type also has an identifier or a name. In addition, there are various versions of the message descriptions, so that differing versions of the underlying message descriptions can be differentiated. Each message type is suitable for the representation of one or multiple business transactions (for example submission of a SEPA credit transfer).

Below some of the relevant messages for the customer-bank-communication are listed:

Name	Message
pain.001	Credit transfers
pain.002	Status reports
pain.008	Direct debits

[1] See ISO 20022: https://www.iso20022.org/ as a start page and for more information for example https://www.iso20022.org/faq.page

Name	Message
pain.007	Customer return (customer to bank payment reversal)
camt.052	Intraday account turnovers
camt.053	Daily statements
camt.054	Booking information
camt.029	Information on cancellations/returns (Resolution of investigation)
camt.055	Customer payment cancellation request

Table 1: Customer-bank-messages

Respective messages are also available for the interbank-communication (pacs messages, among others). ISO-20022 messages are also used for instant payments.

Thus ISO 20022 establishes a unified form for the exchange of messages in the finance sector. On this global level, initially the total sum of all available elements is described for a message.

By restricting the general requirements and specifying additional usage rules (technical and/or subject-specific), organisations can define their own subforms of the ISO-20022 messages for certain validity scopes.

One organisation that has defined such further specifications and additional rules is the CGI (Common Global Implementation) Group. They put focus on the message exchange for the global and cross-country payments. At the same time many varying payment order types can be represented. There is no specialisation for example on SEPA payments.[2]

Another organisation that has their own specifications for ISO-20022 messages is the European Payments Council (EPC).[3] The EPC publishes specific implementation guidelines which describe messages for SEPA payments like credit transfers (ISO-20022 name pain.001) by use of ISO-20022.[4] The documents present a restriction of the general ISO-20022 specifications, like permitted elements and additional payment-specific rules that need to be considered. That way the EPC format only keeps those elements that are required for SEPA payments. The format descriptions for, among others, the permitted values are only available for the EPC format as a general textual description.

2 See CGI Group / SWIFT: https://www.swift.com/standards/market-practice/common-global-implementation

3 See European Payments Council (EPC): https://www.europeanpaymentscouncil.eu/

4 See European Payments Council (EPC):
https://www.europeanpaymentscouncil.eu/document-library/implementation-guidelines/sepa-credit-transfer-scheme-inter-bank-implementation

On a national level separate manifestations have been defined based on the ISO-20022. In Germany for example the *German Banking Industry Committee* (DK) defined certain specifications on how XML messages have to be structured based on the ISO 20022 and which rules have to be considered for the transported information. They describe different data formats and procedures in detail and publish the respective XML schema files.[5] This is similar with the Swiss financial centre. With the Swiss Payment Standards the SIX (Swiss Infrastructure and Exchange) published the respective stipulations and implementation recommendations for realising ISO-20022 messages. They contain concrete specifications, for example on the exchange of credit transfer orders. Stipulations for Swiss payment orders, like Swiss direct debits, exist as well.[6]

The specifications of the DK as well as of SIX apply various stipulations of the EPC, but they elaborate ISO-20022 specifications in a country-specific way. That way the DK and SIX specifications present more concrete forms of the EPC specifications. Especially the format descriptions are, in contrast to the EPC format, partly more detailed in the form of XML schema components. Many checks can that way be performed directly with the XML schema (for example for the DK format). Same for all is the ISO-20022-based form with a universal XML description.

In addition, the SIX specifications for instance offer a framework for individual configuration to the financial institutions, for example depending on the institution's service portfolio.

Furthermore, in France the CFONB released an implementation for the local ISO-20022-based application of pain.001 payments[7] (SEPA, Non-SEPA,…) or pain.008-SEPA direct debits, among others[8]. The varying manifestations are being differentiated in the documents.

Based on the very general description of the ISO-20022 standard, the varying manifestations are always more concrete and specific or restrictive.

The ISO-20022 messages are then communicated via EBICS as an upload or download transaction (see section *EBICS processing steps*, page 39). This way, for example, the pain.001 message (credit transfer) is sent via EBICS from the customer system to the financial institution (see section *SEPA payment transactions*, page 26). The download order for the respective pain.002 status report is also created via EBICS (see section *SEPA payment transactions*, page 26).

The pain.002 messages can, depending on the manifestation of the ISO-20022 standard, include positive or negative messages to the payment orders.

---

5 See The German Banking Industry Committee, SIZ: http://www.ebics.de/spezifikation/dfue-abkommen-anlage-3-formatstandards/

6 See SIX: https://www.six-interbank-clearing.com/en/home/standardization/iso-payments/customer-bank/implementation-guidelines.html

7 See CFONB: http://www.cfonb.org/Default.aspx?lid=1&rid=122&rvid=144

8 See CFONB: http://www.cfonb.org/Default.aspx?lid=1&rid=122&rvid=143

A financial institution with a pain.002 message can inform the customer system in a machine-readable way about the reasons for rejected credit transfer orders. The customer system can suitably consider these errors. In addition, different status codes can give information on the status of complete orders or single partial transactions. Especially a credit transfer order that consists of various single erroneous or correct transactions can be partially processed. In that case, only the correct transactions are processed, whereas the erroneous transactions are separate from the standard processing and will be reported to the customer. They system can react and give error information in a fine-grained and machine-aided way.[9]

6.1.3 Foreign payments and turnover information

The list below highlights a number of examples of format-dependent, standardised order types used in Germany and Switzerland:

- AZV send AZV order in disk format (DTAZV in Germany)
- STA download SWIFT daily statements (SWIFT MT940)
- VMK short-term acknowledgement slips (SWIFT MT942)
- VML long-term acknowledgement slips (SWIFT MT942)
- C52 download bank-to-customer account report
- C53 download bank-to-customer statement report
- C54 download bank-to-customer debit credit notification
- ESR download ESR information (specific for Switzerland)

Furthermore, in Europe different national formats are used especially for the processing of cross-border payments. Still, the ISO-20022-based formats are gaining more importance here, as well (for example, ISO Global, CGI) (see section *ISO 20022*, page 28).

6.1.4 Standard order types for file upload (FUL) and download (FDL)

Up until now, France has been almost exclusively using the following order types to ensure a transparent transfer of files of any format. It is subject to the provision that the name of the order type does not allow recognition of the format being transported, as has been the case in Germany. Instead, the order type FUL and/or FDL are given a format parameter of greater length which allows for continued control. These order types have been available as of EBICS 2.4. The file upload order type FUL is used for submission and the file download order type FDL is used for downloads. Together with the order types, the structure and the format parameters to be used are documented as appendix to the EBICS specification.

[9] For example DK standard, see The German Banking Industry Committee, SIZ: http://www.ebics.de/spezifikation/dfue-abkommen-anlage-3-formatstandards/

6.1.5 Other order types

In addition to the standardised order types, the following classification can also be made for use in EBICS:

- System-induced order types – especially for EBICS
  - e.g. order types in connection with the EDS
- Other system-induced orders types being supported
  - e.g. HAC, PTK for downloading customer protocols
- Reserved order types for file transfer between companies
  - e.g. sending FIN for EDIFACT-FINPAY
- Miscellaneous order types reserved in the specification when using non-standardised formats, e.g.:
  - FTB for dispatching/downloading any file
  - FTD for dispatching/downloading free text files
- Optional EBICS order types
  - e.g. retrieving HVT for EDS transaction details

6.2 Business Transaction Format – BTF

BTF translates to business transaction format. With the introduction of EBICS 3.0 BTF unifies the transfer formats in Germany, France and Switzerland. Instead of the old order types and format parameters, now the BTF structure is exchanged during the communication with the bank server and it identifies a business transaction.

To guarantee the compatibility with older versions of EBICS, adjustments from format parameters and order types to BTF standards have been facilitated by match overviews (mappings). On a national level match mappings have been defined for order types and format parameters. The EBICS clients have to consider the mapping. During the transition period mixed forms of the supported EBICS versions might emerge:

- Client side

  Financial institution A, for example, already supports BTF, while financial institution B still only offers EBICS 2.x. The bank accesses of the EBICS client should be adjusted to the respective version of the bank server.

- Server side

  The employees of a customer use different versions of the EBICS clients. While one employee submits an order via the order type of an older version, another employee that has the EBICS client 3.0 signs the order with the EDS via BTF.

6.3 Electronic Distributed Signature (EDS)

The electronic distributed signature (EDS) is probably the most important application function in EBICS. Prompted by available market products, this extension has made its way into the EBICS specification.

The electronic distributed signature makes it possible for the submission of an order – which, if necessary, already bears a first signature – to be disconnected from the actual release. It is possible to submit a signature file that is disconnected from the order in terms of time and location. The connection between two files is made via an order number and an order ID.

The procedure is as follows:

- A subscriber submits an order, e.g. with order type CCT, and if necessary adds an electronic authorisation signature of its own with signature class A.
- On the institution side, the order is checked to ascertain whether further signatures are required. If this is the case, the order is cached in the institution along with the hash value.
- A second subscriber would now like to release the order and has received the required data such as order number and hash value by an alternative channel (the provision of the order number and hash value lies outside EBICS and is not part of the server components on the institution side).

  The subscriber now has the following possibilities:

  - With order type HVU or HVZ he calls up the orders to be signed by him and receives an overview which, among other things, contains the order type, indicates the signatures that have been given and those missing and shows the length of the uncompressed order.
  - For each individual order he can have further details transmitted via order type HVD such as routing slip information or the hash value.

    This step is omitted if the overview was downloaded with order type HVZ as HVZ already provides all the necessary details.
  - With optional order type HVT, the institution supplies information upon subscriber inquiries, such as individual transactions of the order, remittance information right through to the entire order.
- After analysing the orders the subscriber now has one of the following possibilities:

  - Signature with order type HVE
  - Cancellation via HVS

The following figure, which has been modelled after the illustration in the *Specification for EBICS connection* [1], gives a comprehensible overview of the sometimes a little complex related processes:

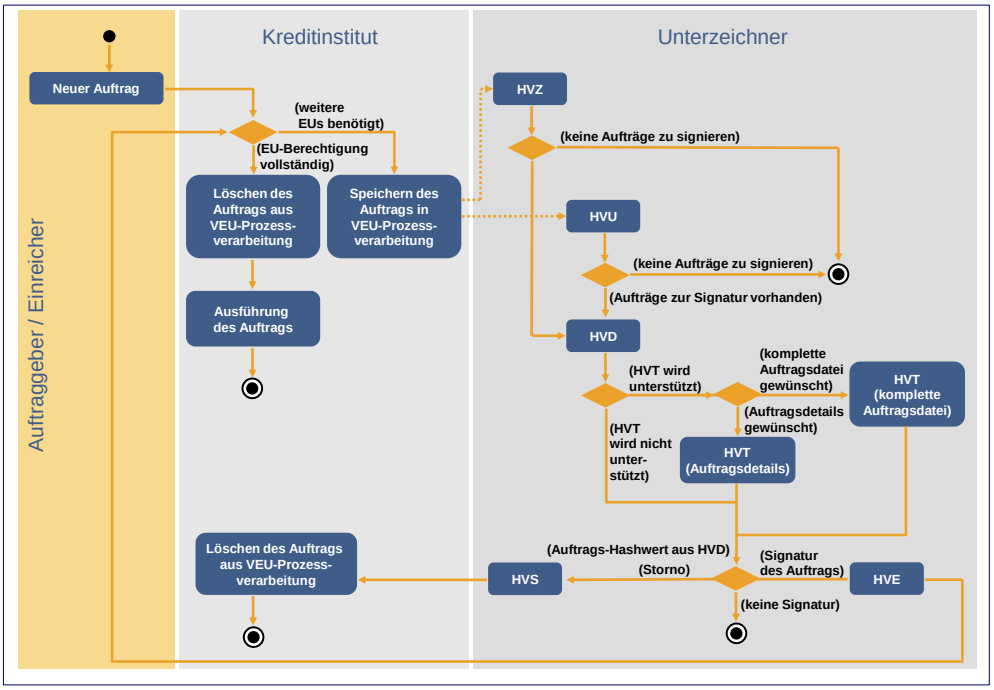


Diagram 8: Processes related to the EDS procedure

Whereas the EDS is in widespread use in Germany, it has not been that common in France and Switzerland. There, it shall also be implemented with EBICS 3.0.

In France the signatures are usually sent with the order. With EBICS Profile TS, depending on the number of signatures, an order is processed as follows:

- One signature on the order: the order is fully authorised with one signature and is executed.
- Two signatures on the order: the decision as to whether the second signature is required and the order is sufficiently authorised is made in the application system. The application system also decides whether the order is still executed even though, for example, one of the two signers has no authorisation.
- One signature on the order, second signature depending on the limit: Whether the order has been sufficiently authorised or a second signature is required, depending on the limit, is decided in the application system.

With the introduction of EBICS 3.0, mixed contracts of order types and BTF might emerge during the migration period. To fit in with existing authorisation models, certain framework conditions have to be applied to BTF orders (here BTU for the submission), for example:

- BTU does not have to match that of the order, but it needs to be configured with the same order type.
- BTU is used for requesting signature folder data.
- According to the specification, empty fields in the BTF filter are wildcards:

  All matching orders from the signature folder are provided (it is not possible to address a certain BTU with an empty field).
- BTU from the HVx is not additionally reported in the order BTU in Exits.

6.4 Portal systems

Although the term portal does not explicitly appear anywhere in the EBICS specification, the possibility exists of involving third parties in the order submission by using the authentication signature. EBICS does not go as far as FinTS which gives portal operators or intermediaries a role of their own – but the separation of submitting party (technical subscriber) and initiator enables simple portal scenarios to be shown. By using signature class T, this transport instance is also given rules appropriate for this.

6.5 Optional functions

The preceding sections have already referenced the fact that certain functions such as recovery or detailed inquiries at EDS have an optional character. A number of special functions from this portfolio are now to be briefly presented here.

6.5.1 Preliminary check

As described in greater detail in the section *EBICS processing steps* on page 39, an EBICS transaction comprises two steps. In the first step preparations are made with the aid of a brief message, the initialisation, for what could well prove to be a substantial file transfer.

In this step the option exists for preliminary checks to be carried out on upload transactions within a certain framework, thereby ruling out the possibility of unauthorised transfer. The following details can be verified in the context of the preliminary check:

- Account rights
- Limit
- ES verification based on the hash value delivered with the file

The possible extent of the preliminary check depends on which checks are actually supported by the institution and which information is or can be supplied

by the customer product. In other words, we are not dealing with a functionality to ward off attacks but with one intended to upgrade operational security and optimise the resource requirement as incorrect file uploads are prevented from being started at all.

6.6 User data

The following set of order types enables the customer product to download information from the institution on the agreements reached:

- HAA download of retrievable order types
- HPD download bank parameters
- HKD download customer data and subscriber data of the customer
- HTD download customer data and subscriber data of the user

These optional order types allow a subscriber to correctly prepare his customer product for access or the customer product can set up an environment locally that suits the subscriber by, for example, only showing the order types supported.

In the course of transmission, not only are the actual access parameters such as URL and institution name conveyed but also the optional functions which are supported by the institution, e.g. preliminary check or recovery.

The customer and subscriber data provide information on the following details of the business agreements:

- Customer information, e. g. address data
- Account information, e. g. account numbers and currencies
- Authorised order types
- Subscriber attributes, such as subscriber ID and signature class

With this very detailed information a customer product can carry out a fully-automatic configuration of the local environment. In the event of error, a targeted analysis is also possible by using the status information also received.

6.7 Real-time notifications

It is becoming increasingly clear that corporate customers also need real-time notifications of incoming payments for their business models. This trend is due not least to the instant payments processes. With EBICS communication, the initiative always comes from the corporate customer (EBICS client). The EBICS server of a financial institution only reacts to incoming requests (inbound), but does not initiate data exchanges on its own. But how should information be transmitted from the financial institution to the customer in a timely manner? To achieve this, the German Banking Industry Committee (DK) has agreed on the implementation of an interface for real-time notifications that can be used by the financial institution to initiate a download process for the customer system while retaining the EBICS role model (see *Specification*

"Real-time notifications" [8]). For outgoing communication (outbound) from the financial institution to the corporate customer, a push service based on WebSocket is used, which functions as a central component for actively sending notifications to EBICS customers and users.

6.8 EBICS in interbank operations

Another area for using EBICS are interbank operations for exchanging mass payments (SEPA payments) as well as for instant payments.

6.8.1 Link to the SEPA clearer of Deutsche Bundesbank

In Germany, the manufacturer-based solutions (e. g. RVS and Connect:Direct) are increasingly being replaced in bilateral clearing by EBICS as open standard.

A scenario in interbank operations is the connection of institutions to the Bundesbank. The Bundesbank offers only two interfaces with SEPA:

- EBICS with SEPA pacs messages
- SWIFT FileAct

The Bundesbank has introduced its own order types in EBICS and determined formats (e.g. for PTKs).

6.8.2 Link to the STEP2 platform of the EBA Clearing

Another scenario in interbank operations for SEPA payments is the connection of banks to STEP2 of EBA Clearing. Since 2013, EBA Clearing also provides this access via EBICS (as of EBICS 2.5) to connected financial institutions as an alternative to the SWIFT access. EBA Clearing has also introduced its own orders types in EBICS and specified formats for data exchange via EBICS.

6.8.3 Bilateral interbank exchange („garage clearing“)

So far no stipulations have been recorded in the EBICS specification for the direct bilateral exchange between banks. In general the partners make bilateral agreements. Apart from the specification on how to handle returns (R transactions), these agreements also cover business policy issues like e.g. the transfer of liabilities or specific SLAs (e.g. regarding maximum file size).

For order types and technical regulations, the EBA clearing regulations for the STEP2 link are adopted in general.

6.8.4 Instant payments

Instant payments, also called ‘immediate’ or ‘real-time’ payments, present the next step for harmonising payments in the SEPA area with the goal of aiding the competitiveness and economic growth in Europe. After the switch to SEPA credit transfers and direct debits is nearly complete and the digitalisation of the

whole economy has created new expectations for customers and retailers, instant payments represent the focus of the European Payment Council (EPC) for the coming years.

Centrepiece is the new SEPA Instant Credit Transfer (SCT^{Inst}) schema. It offers a strong connection to the existing SEPA payments and already established processes and implementations through a special configuration of the standard SEPA credit transfer schema. Even though the schema itself only supports euro, of course debit and target accounts can be kept in other currencies.

Since November 2017, EBA Clearing offers an Instant Payments Service (RT1) based on the SCT^{Inst} on a European level. The ECB plans the introduction of a Target Instant Payments Service (TIPS) for the fall of 2018. Beside these, other local procedures are productive for the respective countries.

One of the main characteristics of instant payments is the time period between the transfer of a validated SCT^{Inst} order of the ordering party's financial institution to the response of the beneficiary's financial institution. As a rule this time period should not exceed 10 seconds. If an exemption timeout occurs, there are rule for the status requests in the rulebook. In every case, until the financial institution gives a negative feedback, it is assumed that the payment has been carried out successfully. This presumes that all involved systems are available 24/7/365.

A single instant payment is limited to 15,000 euros due to security reasons; higher sums can be agreed upon bilaterally. SEPA instant payments exist in 34 countries of the SEPA zone. The support of SCT^{Inst} is currently not mandatory for financial institutions. For the realisation of an instant payment, this function has to be supported by the beneficiary's financial institution.

As an access channel to the RT1 service the EBA Clearing offers SiaNet and EBICS (as of EBICS 2.5). Analogous to the Step2 connection, EBA Clearing offers an Implementation Guide for the connection via EBICS. The instant payments messages are transferred in one step via EBICS and the file-based reports are transferred via EBICS in a process analogous to STEP2. For the one-step, message-based use of EBICS 3.0 in the RT1 service, a separate specification has been created in the form of a delta document (see *Use of EBICS for the Clearing & Settlement of Instant Payment Transactions (Delta - Concept)* [7]) and published on the EBICS website (www.ebics.de and www.ebics.org).

7 EBICS processing steps

Having completed this description of the functionalities contained in EBICS, we now offer an explanation of the actual protocol sequences in this last subject-specific section.

Here, a dispatched processing unit is termed a transaction. EBICS makes a broad distinction between upload and download transactions. The function of upload transactions is, for example, to submit orders and that of download transactions to retrieve account turnover.

Transactions break down into transaction phases and transaction steps. The following transaction phases are possible:

Upload transaction	Download transaction
Initialisation	Initialisation
Data transfer	Data transfer
	Acknowledgement

In turn, several steps can then be contained in the transaction phases comprising in each case of an EBICS request and associated response. While the initialisation phase consists of only one step, the data transfer phase can contain several steps on account of segmenting.

A transaction is initiated by the customer product. The system on the institution side can only intervene in the initiation by, for example, notifying the customer system of a recovery point following a termination.

The individual transaction phases are connected with each other by means of a transaction ID which is generated by the banking system and is notified in the initialisation response.

Every EBICS request and every EBICS response contains the authentication signature of the customer/subscriber or of the institution.

The following diagram illustrates the sequence of an EBICS transaction:

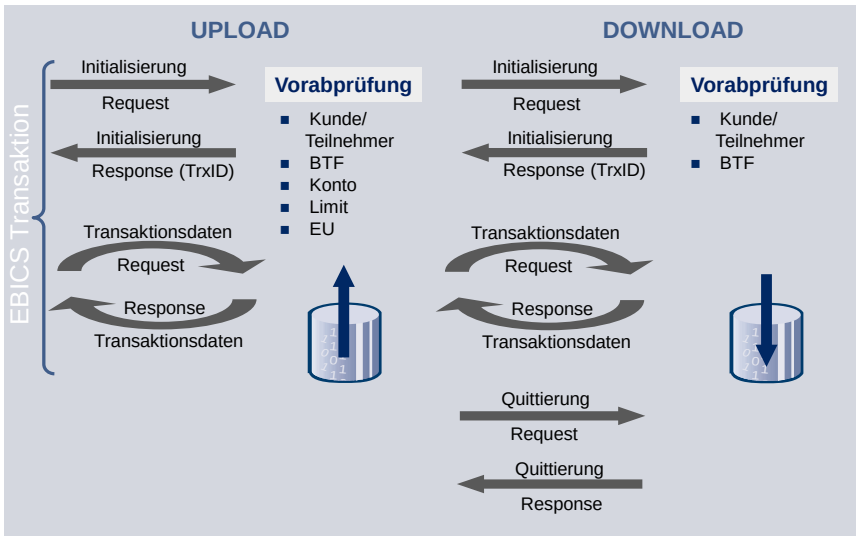


Diagram 9: Sequence of an EBICS transaction

8 Positioning in the international environment

As an extension to the German DFÜ Agreement, EBICS defines the communication and security definitions for mass payments in the corporate customer business. Standards exist in both the national and the international environment which can be viewed as supplementing and overlapping with EBICS. A number of these are briefly described below and placed in relation to EBICS.

8.1 FinTS

FinTS (Financial Transaction Services - formerly Homebanking Computer Interface) is also a DK standard which, however, is focused on online banking with private clients and small and medium enterprises. FinTS in its classic form maps dialogs between customer and institution and processes message-oriented individual transactions. FinTS contains functionalities such as bank or user parameter data comparable to EBICS.

In its most recent version 4.1, FinTS also relies consistently on internet standards such as HTTP or XML. Dialog-free datagrams and the bank-customer communication were also added to the communication protocol.

In the security area, FinTS also supports electronic signatures as well as the PIN/TAN procedure in various forms.

As with EBICS, FinTS also supports the usual financial data formats such as SEPA, camt, DTAZV and SWIFT and refers to them as business transactions. Instant payments are also included in FinTS. In the meantime DK is also ensuring that similar use is being made of the versions and contents of these formats by both standards. However, FinTS also has the possibility of defining a large number of own business transactions, ranging from standing orders across time deposits to free notifications to the institution. These business transactions create (at least) a national standard whenever an international definition is missing.

In the small and medium enterprises segment, apart from the business transactions identical to EBICS, e.g. for collectors or account turnover, FinTS also offers customers the possibility of implementing the electronic distributed signature (EDS) themselves. The standard is currently lacking all the possibilities of mass payments such as segmenting or recovery.

Bearing these various points in mind, FinTS must be positioned as an addition to EBICS. This applies wherever small/medium enterprises or corporate customers have to be viewed as a joint target group as they operate their financial transactions in both worlds, i.e. a company carries out both mass payments and is also active in the investment and securities business. For some business types a crucial point would also be where the transaction is being carried out, i.e. in the bookkeeping department or by a managing director out on business.

Modern customer products have already been geared to this situation and already offer two communication protocols with EBICS and FinTS.

For a more detailed explanation of FinTS it is worth reading the FinTS Compendium which can be downloaded from *fints.org*:

8.2 SWIFT

In the interaction between EBICS and SWIFT the following structures must be mentioned:

- Classic FIN formats in international payment transactions
- XML and ISO activities of SWIFT
- SWIFTNet as the company's own communication standard
- SWIFT FileAct as the company's own file transfer standard

There is not a great deal to mention about the classic FIN formats such as MT940. They are stable, are only subject to statutory amendments and are packed into the protocol of the two relevant German standards EBICS and FinTS in the same way. A degree of independence from SWIFT is thus also created, as the only work carried out is with referencing.

The fact that an XML-based version, SWIFT XML, also exists alters nothing in the clear separation of tasks between the standards. More important here is the fact that SWIFT has taken a very abstract approach in the creation of XML formats and carried out what was in effect a reverse engineering of the existing world. After years of laborious work, process models were produced for international payment transactions using UML which today produce the FIN and XML formats as mere derivations. This methodical approach gave SWIFT the lead in the competition over international payment standards, enabling it to successfully position the core components of these models as ISO Standard 20022.

While SWIFT's ISO efforts are likely to strongly influence the development of payment transaction formats, the associated transport log which offers the foundation for SWIFTNet is of subordinate importance and must be viewed as a proprietary development. SWIFTNet doubtless has a stable diffusion rate in the interbank business, but it plays practically no role at all in the customer-bank relation.

That is why the SWIFT standard constitutes an important instance for publishing and servicing payment formats. Its positioning in relation to EBICS has also unambiguously been established and should continue to be stable in the coming years.

As a result of France's involvement in the SEPA Company, SWIFT's influence has also strengthened as this standard plays a major role in France. SWIFT FileAct is also more frequently encountered as file transfer protocol. Nevertheless, the rule applies that SWIFT (see *swift.com*) and EBICS coexist harmoniously.

8.3 PeSIT-IP

The French manufacturer standard PeSIT can be considered as a complementary standard to EBICS, particularly in the interbank business but also for big companies. PeSIT can also be used to submit mass payments and download turnover data. Corporate customers in France often rely on products that apart from EBICS also have the PeSIT-IP module.

8.4 SFTP and FTP(S)

The file transfer protocols based on FTP are also occasionally used in Europe for payment transactions. Contrary to the protocols discussed so far, these only cover the transfer and not any kind of business processing. The security of the protocols also does not match the current requirements for payment transactions. Due to its widespread availability as a system software, SFTP or FTPS is often used for the general file transfer.

8.5 Outlook

This description of standards tells us in no uncertain terms that there are no currently comparable industrial standards available – not even in the international sector.

This makes it clear that EBICS will become the future key standard for bulks payments in Europe and far beyond that. It is strengthened by the fact that next to the partners of the EBICS Company (Germany, France and Switzerland), other countries like Austria, Spain, Italy, Portugal and the Republic of Ireland are also increasingly supporting the EBICS on the part of the financial institutions. This development is facilitated by the introduction of EBICS 3.0 and the harmonisation that goes comes along with it.

Another motivator for the implementation of EBICS in other EU states can be instant payments, as here a unified European processing would bring advantages for all involved parties.

The final section now offers an example of an EBICS implementation and migration based on an actual product family.

9 Implementation

Following the explanation of the functionalities of EBICS and a description of the scenario as a whole, this final section deals with the topic of implementation to demonstrate that the interplay between old and new can indeed function and how this can be achieved.

We begin by examining the product family TRAVIC (Transaction Services), the individual components of which can be used to set up an overall scenario of this kind.

TRAVIC is made up of the following components which can be combined as required:

Components	Description
TRAVIC-Corporate	Fully encompasses the functionalities on the institution side for mapping EBICS and interbank EBICS and also the channels PeSIT and SFTP/FTP(S).
TRAVIC-Port	Implementation of an EBICS portal for processing payment services.
TRAVIC-Interbank	Offers the possibility of submitting payments via EBICS at the European clearing houses or via EBA Clearing for instant payments.
TRAVIC-Link	Provides a cross module file transfer portfolio with which, for example, orders can be passed fully automatically to an institution via EBICS or other file transfer procedures, bearing electronic authorisation signatures.
TRAVIC-EBICS-Mobile	Allows users to approve, i.e. to sign, order files of national and international payments which are available in the financial institution while "on the road"
TRAVIC-Push-Server	Active information for the customer on his EBICS orders via app, e-mail, WebSocket or via other media
TRAVIC-Retail	Rounds the kit off and provides all core functionalities for an institution-side FinTS system
TRAVIC services APIs for EBICS	The TRAVIC services APIs for EBICS and the EBICS-Kernel help with the implementation of EBICS in the customer's products by offering a complete and readily comprehensible EBICS suite for integration on the customer side
Outlook: TIPS - Tar-	Offers clearing and settlement functions for instant

Components	Description
get IP Settlement	payments

With the exception of TRAVIC-Retail, which has not been considered in this context, the individual components are explained in more detail below.

9.1 TRAVIC-Corporate

TRAVIC-Corporate offers all functions comprised in EBICS, including the optional functions. Additionally available tools also allow the transfer of master data and cryptographic keys of products by other manufacturers within the scope of migration:

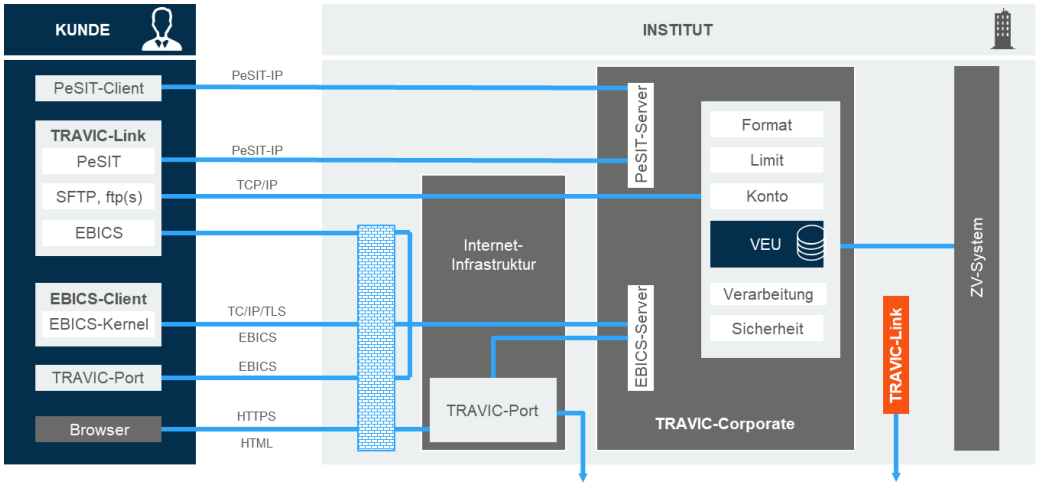


Diagram 10: Components of the TRAVIC product family

TRAVIC-Corporate is available on several UNIX platforms and Linux to enable selection of the best possible environment for each deployment purpose.

9.2 TRAVIC-Port

In the distributed signature field or in cases where there is a low number of orders to be collected and submitted, a portal integration with EBICS represents an ideal addition to a financial institution's range of products and services. It is therefore no surprise that a growing number of institutions are keen to incorporate corporate customer portals into their internet banking portfolio.

TRAVIC-Port uses an EBICS protocol component, the so-called EBICS-Kernel, as the centrepiece for communication suitable for multi-banking. These core functions are supplemented by web services for the subject-specific development of payment transactions and user profile administration which help customers to process administrative tasks.

To facilitate integration into existing internet banking solutions, the portal functions are visualised via web service interfaces, i.e. the presentation can be

made by the institution itself or by its IT service provider. TRAVIC-Port also has a single sign-on functionality which enables portals to be integrated into TRAVIC-Port and vice versa.

With these means it is possible with little implementation work to develop the transaction-dependent part of a corporate customer portal and enrich it by adding further subject-specific functions.

9.3 TRAVIC-Interbank

In the interbank business EBICS stands out especially thanks to enabling homogeneous roles for the two communication partners. Each partner has an EBICS server and an EBICS client. TRAVIC-Interbank offers a component for both roles Authorisations for data exchange are made directly with the data transfer. TRAVIC-Interbank supports the following application scenarios:

- Interbank and Bundesbank operations, the exchange of electronic mass payments with the SEPA clearer of the Bundesbank or STEP2 of EBA clearings via EBICS
- TRAVIC-Interbank for instant payments RT1 of the EBA clearing

9.4 TRAVIC-Link

TRAVIC-Link is a universal file transfer product that can be deployed in various scenarios.

In an environment of electronic payment transactions for the corporate customer business, TRAVIC-Link plays the role of a so-called customer system according to the DFÜ Agreement with customers. In these scenarios, TRAVIC-Link supports the standards BCS and EBICS. Here, TRAVIC-Link supplements financial accounting systems with automatic transmission of orders as well as automatic download and forwarding of account turnover files. Order files to be transmitted to an institution can be given electronic signatures prior to transmission.

The communication protocol ONGUM-IP integrated into TRAVIC-Link allows transmission of files between several TRAVIC Link systems, regardless of content.

Another functionality of TRAVIC-Link is the communication via so-called standard software. TRAVIC-Link offers the necessary interfaces for this.

The following communication protocols or communication modules are currently supported by TRAVIC-Link.

Electronic banking in the corporate customer business field:

- EBICS
- PeSIT-IP

Integrated file transfer procedures:

- ONGUM-IP
- Secure-FTP
- HTTP
- JMS
- FTP(S)

Standard software that can be integrated via interfaces:

- Connect:Direct (Sterling Commerce)
- UDM (Stonebranch)

9.5 TRAVIC-EBICS-Mobile, TRAVIC-Push-Server

TRAVIC-EBICS-Mobile is a mobile application used to sign payment orders which were submitted to financial institutions via the EBICS procedure.

Account information (balances and transactions) continues to be displayed.

The application is intended for financial institutions and large companies that want to offer their customers or employees the possibility to sign payment orders even when outside the corporate environment.

TRAVIC-EBICS-Mobile is:

- Suitable for multi-banking due to its standardised interfaces and consequent usage of the EBICS standard in the gateway server
- Individually configurable
- Secure due to electronic signatures and encrypted message transfers
- Push-enabled by banks which operate TRAVIC-Corporate with the TRAVIC-Push-Server

TRAVIC-Push-Server is used for outgoing communication (outbound) from the financial institution to the corporate customer. It functions as the central component for active sending of notifications via the preferred communication channels of the EBICS customers and users. Aside from the push channels mobile and e-mail, TRAVIC-Push-Server offers the information advice in real time via a WebSocket interface according to the new *Specification "Real-time notifications"* [8].

9.6 TRAVIC services APIs for EBICS

While the established manufacturers of bank servers are busy rendering their products for EBICS, the customer product manufacturers are faced with a problem.

Hundreds of pages of documentation have to be implemented and integrated merely to, for example, add a new transport channel to a payment transaction product. The extent to which the optional EBICS features have to be used in future is still unclear at this juncture, i.e. whether they have to be accounted for from the beginning.

A TRAVIC services API for EBICS, the EBICS-Kernel, offering a complete and readily comprehensible EBICS suite for integration on the customer side proves useful here.

Bibliography

[1] DFÜ Agreement
Appendix 1: Specification for EBICS connection
Version 3.0 from 29 March 2017
The German Banking Industry Committee (DK)

[2] DFÜ Agreement
Appendix 2: FTAM connection
- obsolete -
The German Banking Industry Committee (DK)

[3] DFÜ Agreement
Appendix 3: Data Format Specification
Version 3.1 from 24/04/2017
The German Banking Industry Committee (DK)

[4] EBICS Implementation Guide
based on the EBICS version 3.0 from 29 March 2017
EBICS Working Group

[5] EBICS Security Concept (on request)
Version 1.5 from 1 December 2014
The German Banking Industry Committee (DK)

[6] FinTS V4.1
Version 4.1 from the 23/02/2018
The German Banking Industry Committee (DK)

[7] Use of EBICS for the Clearing & Settlement of Instant Payment Transactions (Delta - Concept)
From 30/10/2019
EBICS Working Group

[8] Specification "Real-time notifications"
The German Banking Industry Committee (DK)
Version 1.0 from 17/07/2019

List of abbreviations

BCS	Banking Communication Standard
BPD	Bank Parameter Data
BSI	German Federal Office for Information Security
BTD	Administrative order type for sending a file, described in more detail by the BTF structure
BTF	Business Transaction Formats
BTU	Administrative order type for sending a file, described in more detail by the BTF structure
CFONB	Comité Français d'Organisation et de Normalisation Bancaire
DFÜ	Remote Data Transfer (RDT) (from German: Datenfernübertragung)
DK	The German Banking Industry Committee (previously →ZKA)
EBICS	Electronic Banking Internet Communication Standard
EDS	Electronic Distributed Signature
ETEBAC	Echange TElematique BAnque-Clients
ES	Electronic Signature
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
FinTS	Financial Transaction Services
FTAM	File Transfer and Access Management
HBCI	Home Banking Computer Interface
IP	Instant Payments
IT	Information technology
ISO	International Standards Organisation
OAGi	Open Application Group
OSI	Open Systems Interconnection

RT1	Instant payments service of the EBA Clearing
SEPA	Single Euro Payments Area
SIX	Swiss Infrastructure and Exchange
SDC	Service Data Center for processing data
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
UML	Unified Modelling Language
TWIST	Transaction Workflow Innovation Standards Team
VEU	Verteilte Elektronische Unterschrift (see also → EDS)
W3C	World Wide Web Consortium, internet standardisation body
XML	Extensible Markup Language
ZKA	Central Credit Committee (now →DK)

List of diagrams

Moorfuhrtweg 13
22301 Hamburg
Tel.: +49 40 227433-0
Fax: +49 40 227433-1333

email: info@ppi.de
Internet: www.ppi.de