EBICS Compendium

Electronic Banking Internet Communication Standard

Document version: 5

Date: 20.06.2016

Further information: Michael Lembcke
michael.lembcke@ppi.de

PPI AG

Foreword

At the CeBIT fair in 2006, the German Central Credit Committee (ZKA– renamed into the German Banking Industry Committee [DK]) presented an extension of the DFÜ 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 in 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 1 January 2008, EBICS has been compulsory for German financial institutions and has completely replaced the previous FTAM variant since the beginning of 2011. In France, the migration from the ETEBAC standards to EBICS has meanwhile been completed. The current EBICS specification is available in version 2.5.

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

Additional to the basic functions, i.e. internet communication in the corporate customer business in the broadest sense, EBICS also offers new features such as the distributed signature or authentication signature, and also allows the use of certificates. The definitions for structuring a PKI infrastructure (Public Key Infrastructure) lie at the centre of current implementations.

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 render what are indeed highly complex connections as comprehensible as possible. At all events we hope you enjoy reading this compendium!

PPI AG Informationstechnologie, June 2016

Document version 5 dated 20.06.2016

Table of contents

1 Introduction

1.1 EBICS requirements

The term which captures the essential objective underlying the creation of the EBICS standard is "evolution instead of revolution".

Right from the beginning this key principle 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 two current application scenarios in Germany and France. 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 distributed electronic signature (VEU). 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 multi-bank capability would have been tantamount to a fragmentation of the market which would not have been in anyone's interests.

Below we highlight the requirements for the extension of the BCS Standard (Germany) and the ETEBAC Standard (France), referred to throughout this compendium as EBICS:

Requirement	Description
Internet	EBICS is to be based throughout on internet technologies. This aspect which formerly had only applied to the communication sector is now 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. Use is to be made of all stable and suitable internet standards.
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, e.g. firewall structures (also accounted for in the concept) as much as the area of signatures and encryption not to mention the security concept which was drawn up and accepted parallel to the standardisation.

Requirement	Description
Bandwidth	One of the greatest advantages is to be 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. Ideally the protocol should be tailored to process large volumes of data and 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 can be deployed in the platform area which are already in widespread use (e.g. the ZIP compression). They also serve as a guarantee for optimum and profitable processing.
Technical knowledge	A number of new functions are also to be introduced with EBICS, e.g. the distributed electronic signature (VEU). In the meantime this function has become established among customers via market products and is now to be deployed in a multibanking context.
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.
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 were to be 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.

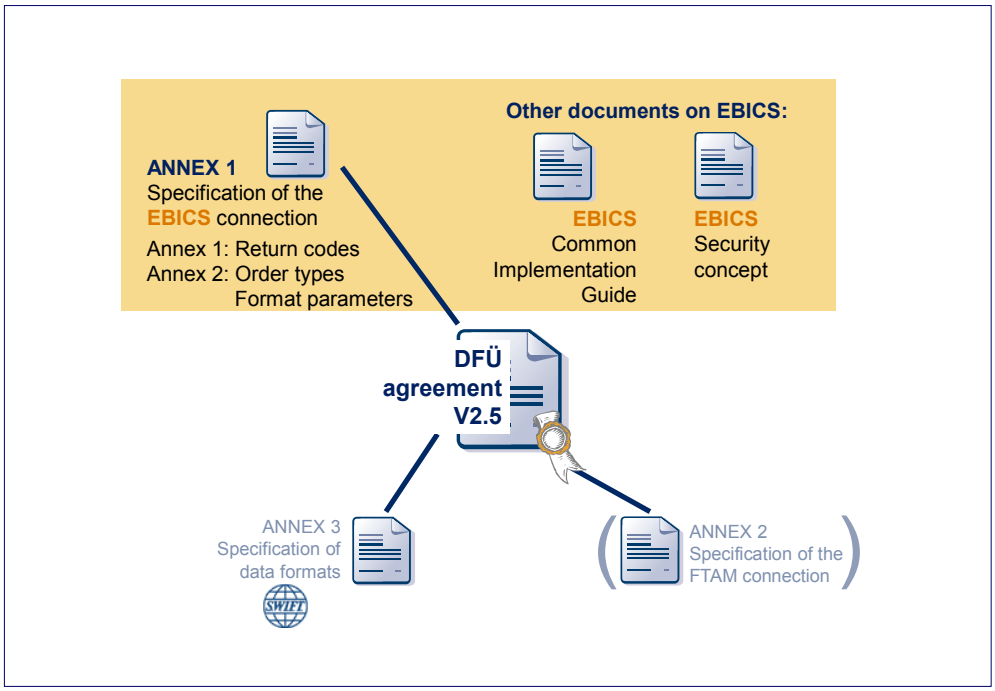

Figure 1: Structure of the EBICS specification and embedding in the German DFÜ Agreement

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 English original text and will be translated back into German and French. These documents can be accessed under ebics.de and cfonb.fr.

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 in an implementation guide for the Swiss Banking Industry how to use EBICS. Moreover, business rules describing how to use ISO20022 payments in Switzerland were defined in another document thereby accommodating demands for simple implementation/migration and secure operation.

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.

2 EBICS overall scenario

In this chapter we present an exemplary overall scenario, the objective being 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.

At the time of publishing this compendium the migration of FTAM to EBICS had already been completed in Germany. But this example can still impressively illustrate how to migrate from a national standard to EBICS.

2.1 Interplay of procedures

To migrate from old procedures to the EBICS standard, the institution must be able to ensure at least tandem operation of old standards (e.g. BCS-FTAM) and EBICS over a longer period of time. The figure below illustrates a possible configuration:

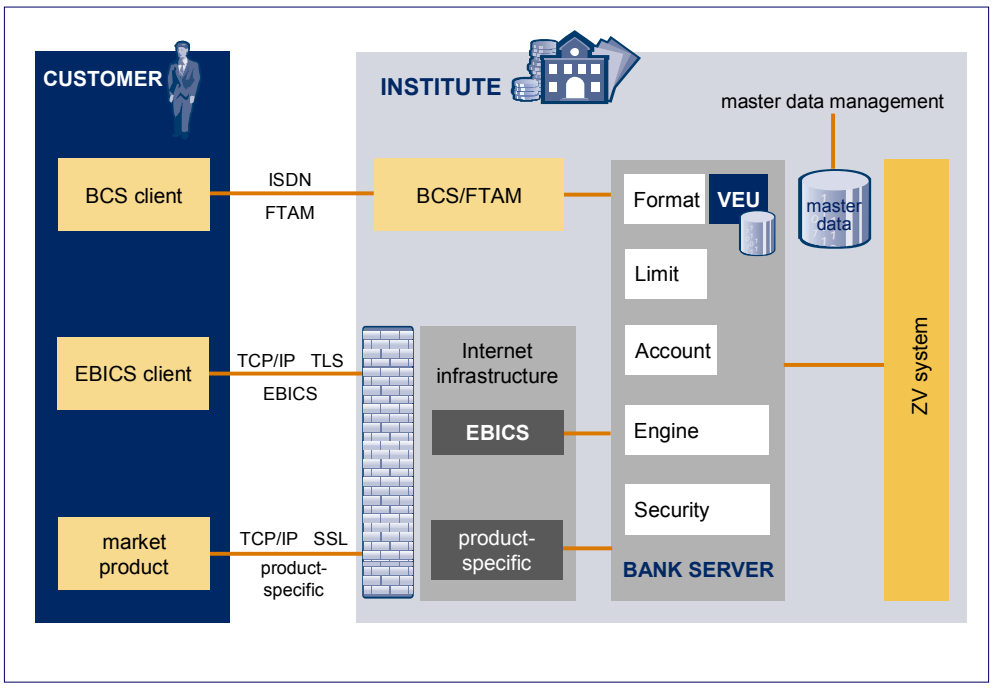

Figure 2: BCS/EBICS overall scenario as example of migration from a national standard to EBICS

The configuration above reveals that, in addition to the access components, a large number of components can be used jointly. As no separation of systems is necessary thanks to the identical A004 security procedure and the same formats, an overall scenario of this kind can be operated over a longer time

period if we leave aside the higher operating costs caused by the duplicate components. However, as a result of the road map stipulated by the German DFÜ Agreement, this overall time period had in any case been restricted to the end of 2010.

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 large scale 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 distributed electronic 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 institute's own portal. However, for the integration of legally independent third parties a number of problems have yet to be solved under EBICS as at the moment no provisions exist for a portal operator to be ascribed a role of its own.

2.4 Migration

This section concentrates on the tasks of a typical BCS to EBICS migration on the customer side. There is no need to discuss the institution side here as since 1 January 2008 an obligation already exists on the part of the banks to support EBICS, at least as far as Germany is concerned.

Note:

The following migration considerations are based on the assumption that the BCS customer product being used is at the current release status.

The current infrastructure should support signatures according to A004 so as to avoid the necessity of having to introduce a new security procedure in addition to the renewal/supplementation of the

communication infrastructure. Thus the assumption is also made that the conversion to the new security procedure A005 or A006 acc. to EBICS version 2.5 is made separate from the migration.

A further assumption is that a functioning internet infrastructure already exists as is also obligatory for other internet applications.

In an ideal case, the migration on the customer side should be restricted to an update of the current customer product if the administrative conditions have been created. Although the general master data such as customer or subscriber (cf. section on the data model) is retained, the communication data changes. The parameters required for the selection are contained in the BPD (bank parameter data) and are provided by the institution.

After installing an appropriate update and after all the necessary settings have been undertaken, it should now be possible to establish connection with the institute via the internet.

A factor which should not be underestimated is the need to understand a number of new processes, such as the preliminary check if this is reflected in the settings and sequences of the customer product. And the use of new functions by EBICS such as the distributed electronic signature also requires in-depth understanding of connections. The corresponding chapters in this compendium could certainly prove helpful in this context.

One problem which has yet to be solved is the EBICS initialisation of an existing subscriber which prior to this had already been initialised via FTAM. The subscriber is obviously already in possession of a private key to sign orders, but not of any key pairs for authentication or encryption. For a case of this kind, the order type HSA exists in EBICS which allows a subscriber with the status `Neu_FTAM` to submit his new – EBICS-specific - key signed with his ES activated for FTAM. This optional procedure enables subscribers to be smoothly taken over into EBICS without new initialisation using INI letter.

2.4.1 Migration status in France

In France, the X.25 network has been switched off. This means that the widespread ETEBAC -3 standard could no longer be used, and a migration to EBICS had to be completed by then.

Although in theory, the TCP/IP-based ETEBAC 5 could be used as an interim solution, this did not pose a problem for the EBICS introduction. The certificate-based ETEBAC-5 standard is far less widespread with only a few thousand registered customers.

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 the internet platform, use can be made of infrastructures available on both the customer and the institute side and that the efficiency of these infrastructures is many times greater than that offered by the present solution. The transmission medium used in the old BCS standard was, for example, ISDN which nowadays would be unthinkable for transmitting payment transaction files of today's magnitude.

The use of internet technology also makes it possible for EBICS to line up more closely with other applications. As the corporate customer business with the exception of large scale payments also has many application areas in the transaction or dialogue 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.

Finally, components as well as products have become more widely available as a result of using this widespread technology than was ever the case with the original standard BCS or ETEBAC.

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 previous SSL (Secure Socket Layer).

TLS ensures secure transmission between the customer system and the first HTTP or better web server in the institute. 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 chapter easier to understand, we provide an explanation of the XML standard. In the case of BCS it was 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 and an XML envelope. In other words it is a kind of hybrid system, with the bank technical DTA, SEPA or SWIFT formats remaining the centrepiece while being supplemented by XML structures. The overhead caused by this technology is minimal when considering the large scale payments usually being handled here and the vast size of the payment transaction file compared to the XML envelope.

The figure 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/.

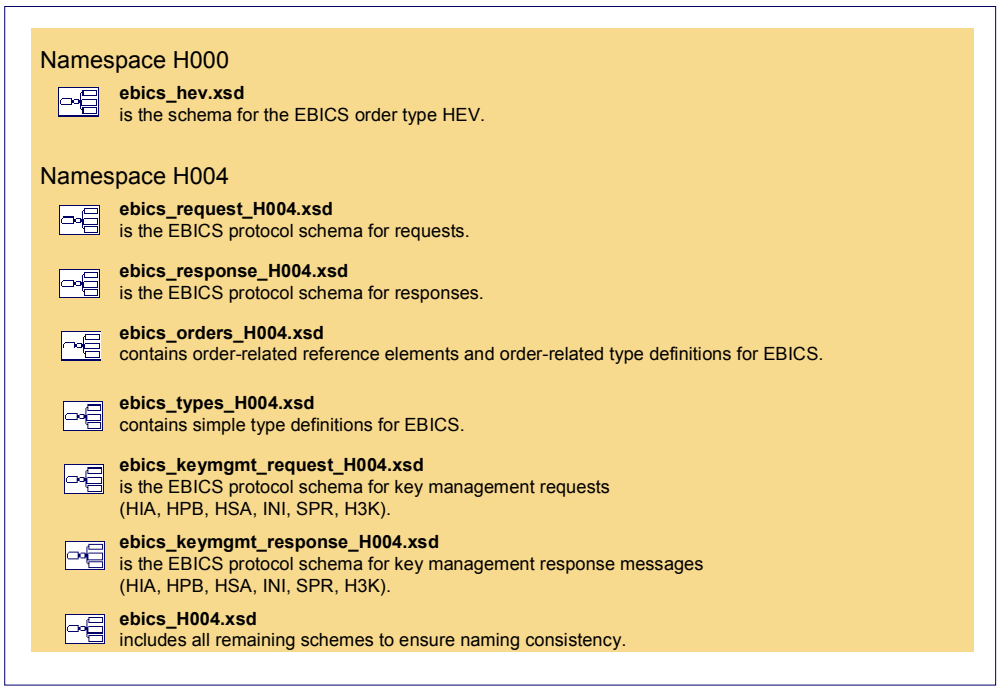

Figure 3: EBICS XML schema

As can be seen, the schema 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 institute supports.

The figure 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 institute side.

Thanks to the – optional – recovery capability of this protocol, it is also possible to intelligently retrieve a transaction if 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 institute 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 chapter deals specifically with the data model used by EBICS. It can be found in the master data management of the respective products and, as already mentioned in the section dealing with migration, is more or less identical for both standards.

Broadly speaking the following entities exist in the data model:

- Customer
- Account
- Subscriber
- Order type

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 institute 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	First signature At least one signature of class B required.
Signature class B	Second signature The order must already have one signature from class A.
Signature class T	Transport signature Designation that this is an authentication signature, e.g. 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 institute side.

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

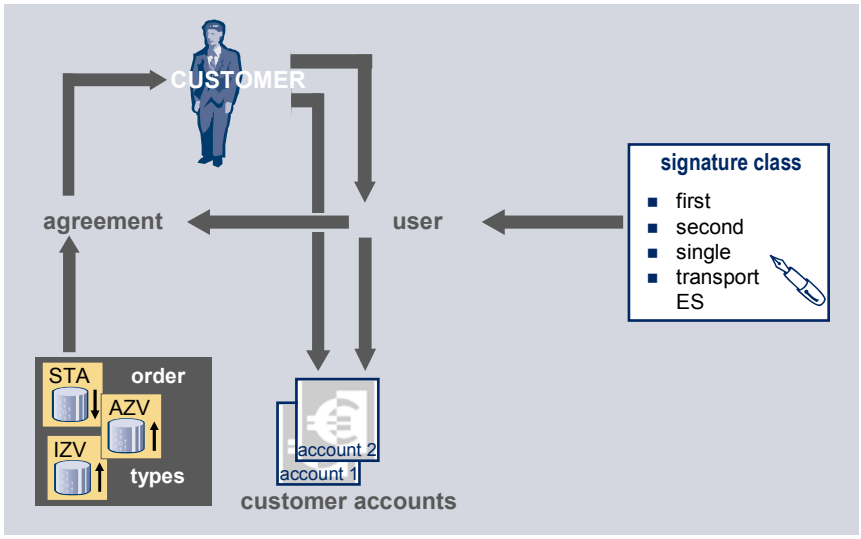

Figure 4: Data model

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

5 Security

New security procedures A005 and A006 as well as X002 and E002 were introduced with the EBICS predecessor version 2.4. Of greater importance, however, are the stipulations governing the obligation to actually implement these procedures - an innovation introduced with the EBICS standard.

No consideration is given to security media as such, 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
- Chipcard
- Other security medium
- Non-removable security medium

France has its special requirements on the TS profile: The Implementation Guide stipulates for the TS profile, that special hardware tokens issued by a certification authority (CA) are used. 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 E001 and E002 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 chapter *EBICS processing steps* on page 32.

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 figure:

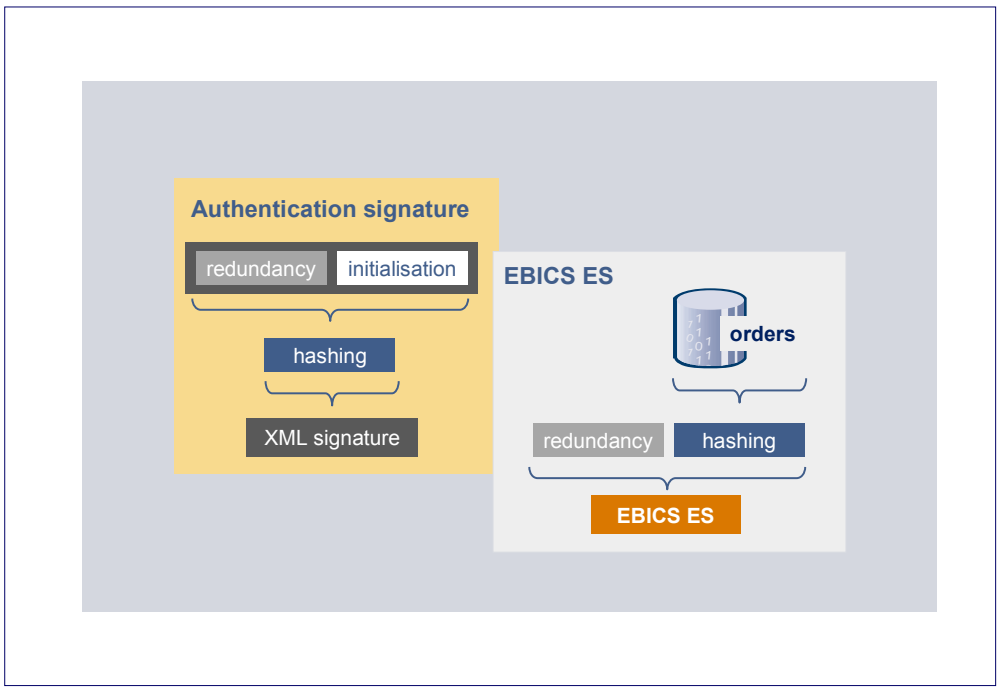

Figure 5: EBICS Signature Procedure

5.2.1 Authentication signature X001 or X002

The purpose of the authentication signature is to unambiguously identify the submitting party. An examination is made of the authentication signature during the initialisation step as well as in every subsequent transaction step, i.e. before transmission of the actual order data (see chapter *EBICS processing steps*, page 32).

Subscribers which 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 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. For this reason, EBICS supports the authentication signature analogous XML signature as standard X001 or 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 institute side) has been carried out since EBICS V2.4 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 variants 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 V2.4, the more robust ES procedures A005 and A006 support the following attributes:

	A005	A006
Key length	1,536 – 4,096 bit	1,536 – 4,096 bit
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.

Single countries (e.g. France and Switzerland) predefine for their financial institutions to use fixed key lengths (2048 bits).

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 V2.5 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.

5.3.1.1 The submitting party profile T based on certificates

Only signature class T is required as entry point in France, i.e. the order is submitted via EBICS and then authorised by fax. This corresponds to the procedure for the older but more widespread standard ETEBAC 3.

The initialisation does not have to be carried out compulsorily via a listed certificate authority (CA), with self-signed certificates of the institute also possible with INI letter.

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

5.3.1.2 Authorisation profile TS

Use is made of electronic signatures for Transport and Signature. The procedure corresponds roughly to 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.

5.3.1.3 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.

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 authentication signature or for the encryption) to the institute. 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 institute 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 from 2009.

5.4.1 TLS – Transport Layer Security

TLS is the successor to 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 institute 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 institutes are used as server certificates (i.e. those certified via VeriSign).

Encryption takes place in both directions. The only procedures supported are the strong encryption procedures or Cybersuites. Four Cybersuites are named in the standard, and all four must be supported by each EBICS partner.

5.4.2 Encryption E001 and E002

E001 and E002 are 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 Bit long encryption key and the padding algorithm PKCS#1.

E002 was deployed as the next development in EBICS V2.4. 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

The business functionalities of EBICS are not substantially different from that of the predecessor standards (BCS-FTAM or ETEBAC). For example, the order types defined in Germany are also available in EBICS. In France, on the contrary, file format parameters are added to the upload and download order types providing information on the business order type.

In many places, EBICS goes beyond the predecessor standards and opens up new fields of application for the customer.

6.1 Order types

The following application areas are supported in the DFÜ Agreement through operative order types:

- SEPA payment transactions
- German foreign payment transactions with DTAZV
- Securities trading
- Documentary credit business
- Information on daily account statements with MT940/MT942 or camt XML for transactions booked and notifications of account movements

6.1.1 SEPA payment transactions

EBICS supports order types for SEPA payment transactions customer-bank and bank-bank (German Central Bank 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 are reflected in the corresponding EBICS order types, with account also to be taken of the following feature.

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

- SEPA Standard Format

  Use of the SEPA standard format subject to the restriction that the only orders possible are those for a submitting party account. To process or-

ders from several submitting party accounts, several orders must be submitted in the SEPA standard format for this option.

- SEPA Container

  DK-specific protocol extension to enable several SEPA standard formats to be submitted for several submitting party accounts in the framework of one order type.

- Extended Grouping Options

  SEPA standard formats which offer the possibility of submitting orders for several submitting party accounts while exploiting 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 SRZ procedure.

To give the full picture it is worth mentioning that the SWIFT formats MT940 and 942 were adjusted to enable the SEPA-relevant data to be conveyed in the context of the SWIFT daily statements via 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.

6.1.2 Foreign payments and daily statements

The following list gives an overview of some formats of standardised order types used in Germany:

AZV	send AZV order in disk format
AZ2	send AZV in magnetic tape format (record length field 2 bytes)
AZ4	send AZV in magnetic tape format (record length field 4 bytes)
STA	download SWIFT daily statements (SWIFT MT940)
VMK	short-term acknowledgement slips (SWIFT MT942)
VML	long-term acknowledgement slips (SWIFT MT942)
ISR	download of ISR information (Switzerland)

6.1.3 Standard order types for upload (FUL) and download (FDL)

Up to now, these order types are mainly used in France and are intended for the transparent file transfer using 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 V2.4. 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.

6.1.4 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 VEU
- Other system-induced orders types being supported

  e.g. 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 VEU transaction details

6.2 Distributed electronic signature (VEU)

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

The distributed electronic 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:

1. A subscriber submits an order, e.g. with order type IZV, and if necessary adds a banking ES of its own with signature class A.
2. On the institute side, the order is checked to ascertain whether further signatures are required. If this is the case, the order is cached in the institute along with the hash value.
3. 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 institute 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 institute supplies information upon subscriber inquiries, such as individual transactions of the order, remittance information right through to the entire order.

4. After analysing the orders the subscriber now has one of the following possibilities:
   - Sign them with order type HVE
   - Cancel them with order type HVS

The following figure which is similar to that in the *Specification for EBICS* [1], gives an overview of the complex interrelations:

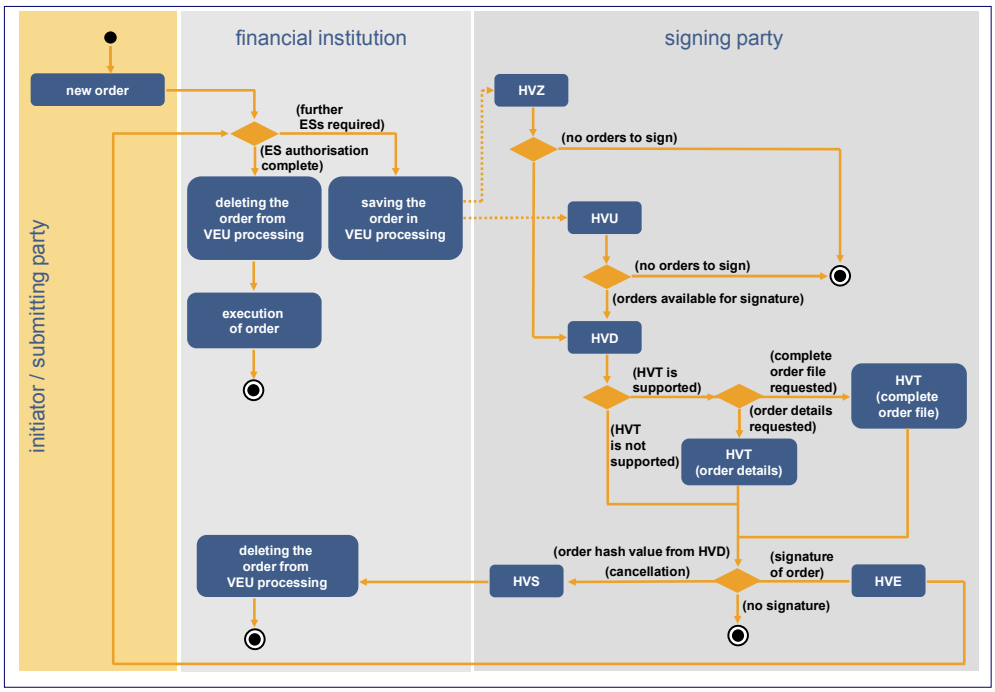

Figure 6: Sequences for the VEU procedure

While the VEU is well circulated and used in Germany, it has not taken root in France until now.

In France, it is still common to send the signature with the completed 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. This is also where the decision is made as to whether, for example, the order is to be executed if one of the two signatures lacks authorisation.

One signature on the order, second signature dependent 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.

6.3 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.

6.4 Optional functions

In preceding chapters there was already frequent reference to the fact that certain functions such as recovery or detailed inquiries at VEU have optional character. A number of special functions from this portfolio are now to be briefly presented here.

6.4.1 Preliminary check

As described in greater detail in chapter *EBICS processing steps* on page 32, 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 institute 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.

6.4.2 User data

The following set of order types enables the customer product to download information from the institute 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 institute name conveyed but also the optional functions which are supported by the institute, 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.

6.5 EBICS in interbank operations

Another form of EBICS implementation is its deployment in interbank operations and to link to STEP2.

6.5.1 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 institutes to the German Central Bank. The German Central Bank offers only two interfaces with SEPA:

- EBICS with SEPA pacs messages
- SWIFT FileAct

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

6.5.2 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 will also provide this access via EBICS to connected banks 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.

6.5.3 Bilateral interbank exchange („garage clearing“)

No stipulations are laid down in the EBICS specification for the direct bilateral exchange between banks. In principle, the partners make agreements on a bilateral basis. 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.

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 institute 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 institute.

The following figure illustrates the sequence of an EBICS transaction:

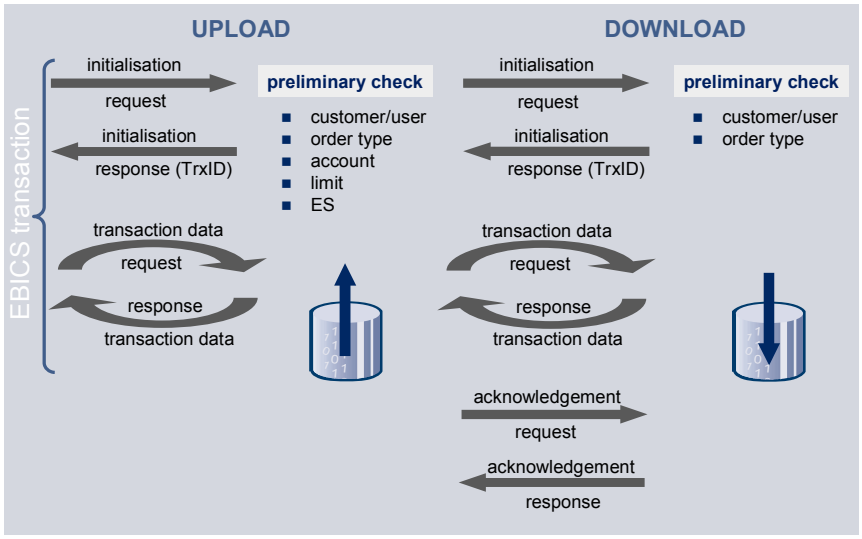

Figure 7: Sequence of an EBICS transaction

After having completed this admittedly somewhat dry section on the EBICS transaction sequences, the next section of our compendium deals with the positioning of EBICS in the national and international environment.

8 Positioning in the international environment

As an extension to the German RDT Agreement, EBICS defines the communication and security definitions for large scale 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.

This chapter concludes with an assessment of the expected significance and development of the standard.

8.1 FinTS

FinTS (Financial Transaction Services) is also a DK standard which, however, is focused on online banking with private clients and small and medium enterprises. The roots of FinTS go back to the days of classic screen text systems but had already been fully decoupled from this communication standard by HBCI (Homebanking Computer Interface). Thus, FinTS in its classic form maps dialogs between customer and institute and processes message-oriented individual transactions. FinTS contains functionalities such as bank or user parameter data comparable to EBICS.

In its most recent version 4.0, FinTS also relies consistently on internet standards such as HTTP or XML. Dialog-free datagrammes and the communication Bank → Customer 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 DTA, DTAZV, SEPA and SWIFT – where they are referred to as business transactions. 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 institute. 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 distributed electronic signature (VEU) themselves. The standard is currently lacking all the possibilities of large scale 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:

www.fints.org

8.2 SWIFT

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

- The classic FIN formats in international payment transactions
- The 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 like e.g. 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 methodic 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.

As a result of this international significance, SWIFT is now closely linked to other international standards such as TWIST, IFX or SEPA and is also co-responsible for the development of this so-called payment kernel as generalised payment transactions model under the auspices of OAGi.

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.

The SWIFT standard can therefore be granted a key role as an instance for issuing and managing payment transaction formats; its positioning vis à vis EBICS is thus unambiguously described and can also be expected to remain stable in the years to come.

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. But the notion of SWIFT and EBICS harmoniously existing side by side still persists.

www.swift.com

8.3 ETEBAC

The French ETEBAC (Echange Télématique Banque-Clients) can be viewed as a complementary standard to EBICS. This standard also allows mass payments to be carried out and turnover data to be downloaded. For corporate customers domiciled in France, products are frequently deployed which also have an ETEBAC module.

France has decided to deploy EBICS as successor to the ETEBAC standard when the X.25 network is disconnected at the beginning of 2012. Most French financial institutions have meanwhile switched over to EBICS. EBICS V2.5 contains all extensions required for a migration from ETEBAC to EBICS.

8.4 PeSIT-IP

The French manufacturer-driven PeSIT standard can be considered as a complementary standard to EBICS, particularly in the interbank business but also for big companies. With PeSIT, too, bulk payments may be submitted and turnover data be provided. Corporate customers in France often use products, that do not only consist of an EBICS module but also have a PeSIT IP module.

It remains to be seen how other ES countries position themselves in relation to EBICS in the near future following this first step towards internationality.

8.5 SFTP and FTP(S)

The file transfer protocols based on FTP are sometimes also used in Europe for payment transactions. Contrary to the protocols discussed so far, these protocols only cover the transfer and not any kind of business processing. It is also the security of this protocol which does not meet today's requirements for payment transactions. Due to its broad availability as a system software, SFTP or FTPS is often used in the context of a general file transfer.

8.6 Outlook

This description of standards tells us in no uncertain terms that there are no currently no 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.

All the more important is the fact that a standard extension now exists in the guise of EBICS which eradicates all the weaknesses of old communication standards. This is also evidenced by the fact that EBICS was introduced very quickly and on a widespread scale, not least, because a soft migration concept was taken into account.

Of even greater interest, however, is the question of how the standard will further spread to other European countries or individual banks within the European Union. A number of initiatives are already known to exist, but no concrete information can be given on them at this juncture.

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

9 Implementation

Having completed our explanation of the functionalities of EBICS and a description of the scenario as a whole, the last chapter deals with the topic of implementation to demonstrate that the interplay between old and new can 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 core functionalities on the institute side for handling EBICS and EBICS Interbank and also the channels PeSIT and SFTP/FTP(S).
TRAVIC-Link	Provides a cross-module file transfer portfolio with which, for example, orders can be passed onto an institute via EBICS or other file transfer protocols, bearing bank technical electronic signatures.
EBICS-Mobile	Allows users to release, i.e. to sign, order files of national and international payment transactions which are available in the financial institution while "on the road".
EBICS kernel	API which contains all EBICS functions on the customer side – for supporting customer products.
TRAVIC-Web	Offers a complete EBICS client based on Java in interaction with the TRAVIC corporate components.
TRAVIC-Port	Implements an EBICS portal for processing payment transaction services via a portlet infrastructure
TRAVIC-Retail	Rounds the kit off and provides all core functionalities for an institute-side FinTS system.

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

The functionalities of TRAVIC-Corporate cover both BCS-FTAM and EBICS. As far as possible care was taken to ensure reusability to enable both soft migration as well as shared administration as illustrated in the following figure:

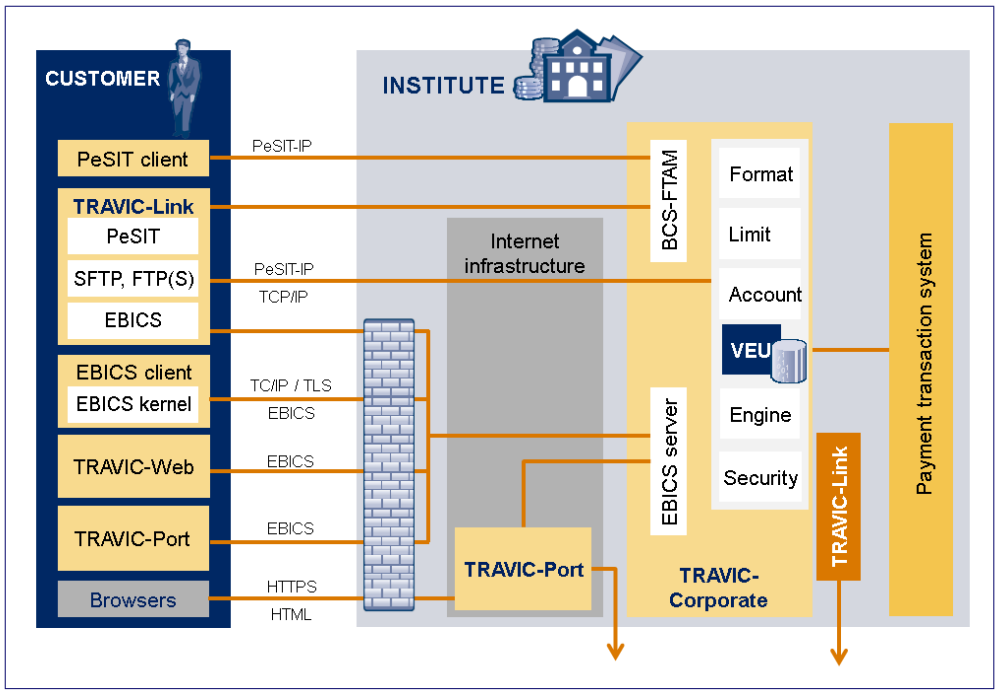

Figure 8: Components of the TRAVIC product family

TRAVIC-Corporate provides all the functions described in EBICS, including the optional components such as key transfer from the BCS environment. Additionally available tools also allow the transfer of master data and cryptographic keys of the BCS implementations of other manufacturers in the framework of migration.

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

9.2 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 or-

ders as well as automatic download and forwarding of account turnover files. Order files to be transmitted to an institute 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 integrable via interfaces
  - rvs (gedas Deutschland GmbH)
  - CONNECT:Direct (Sterling Commerce)
  - UDM (Stonebranch)

9.3 EBICS-Mobile

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

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

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

EBICS-Mobile is

- is suitable for multibanking 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

9.4 TRAVIC-Services-APIs for EBICS

While the established manufacturers of bank server implementations are busily rendering their products suitable 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.

9.5 TRAVIC-Web

For customers requiring a customer product with cash management functions, an implementation exists in the guise of TRAVIC-Web. The function of this Java application is to collect and manage customers, subscribers, institutes and orders for dispatch to the institute via EBICS. It also includes the support of security media such smartcards or disks.

9.6 TRAVIC-Port

In the distributed signature field or in cases of where there is a low number of orders to be collected and submitted, a portal integration with EBICS represents an ideal addition to a bank's range of products and services. No wonder therefore that a growing number of institutes 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 multibanking. 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 institute 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. TRAVIC-Port also has its own portlet-based user interface.

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. By deploying the portlet technology, an attractive and flexible presentation can also be made to the customer.

Bibliography

[1] DFÜ Agreement
Annex 1: Specification for EBICS connection
Version 2.5 of 16th May 2011
Central Credit Committee

[2] DFÜ Agreement
Annex 2: Specification for FTAM connection
Version 2.0 of 3rd November 2005 (obsolete since 1st January 2011)
Central Credit Committee

[3] DFÜ Agreement
Annex 3: Data Format Specification
Version 2.8 of 2014
Central Credit Committee

[4] EBICS Implementation Guide
based on EBICS Version 2.5 of 16th May 2011
Central Credit Committee

[5] EBICS Security Concept
Version 1.4
Central Credit Committee

[6] FinTS V4.0
Version 4.0 of 22nd June 2004
Central Credit Committee

List of abbreviations

BCS	Banking Communication Standard
BPD	bank parameter data
CFONB	Comité Français d'Organisation et de Normalisation Bancaire
DFÜ	remote data transfer
DK	The German Banking Industry Committee (previously ZKA)
DTA	Datenträgeraustausch, data exchange process
EBICS	Electronic Banking Internet Communication Standard
ETEBAC	Echange TElematique BAnque-Clients
ES	Electronic Signature
FIX	Financial Information Exchange
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
FinTS	Financial Transaction Services
FTAM	File Transfer and Access Management
HBCI	HomeBanking Computer Interface
IFX	Interactive Financial Exchange
IT	information technology
ISO	International Standards Organisation
OAGi	Open Application Group
OFX	Open Financial Exchange
OSI	Open Systems Interconnection
SEPA	Single Euro Payments Area
SRZ	data processing service centre
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	distributed electronic signature
W3C	World Wide Web Consortium, internet standardisation body
XML	Extensible Markup Language
ZKA	Central Credit Committee (now DK)

List of figures

PPI AG

Moorfuhrtweg 13
22301 Hamburg
Tel.: +49 40 227433-0
Fax: +49 40 227433-333

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

Document version 5 dated 20.06.2016