



# **EBICS 3.0**

Recommendations for implementing the EBICS standard  
in the Swiss financial services sector

"Swiss Market Practice Guidelines EBICS"

**General note**

Any suggestions or questions relating to this document should be addressed to the financial institution in question or to SIX at the following address: [billing-payments.pm@six-group.com](mailto:billing-payments.pm@six-group.com).

**Amendment control**

All the amendments carried out on this document are listed in an amendment record table showing the version, the date of the amendment, a brief amendment description and the valid from date.

The latest version of this document can be downloaded from the SIX Interbank Clearing website at the following address: <http://www.ebics.ch>

## Amendment control

---

<i>Version</i>	<i>Date</i>	<i>Comment</i>	<i>Comment:</i>
1.0	01.06.2020	First edition	15.11.2021

---

# Table of contents

<b>1</b>	<b>Introduction</b> .....	<b>5</b>
1.1	Purpose of the document, and its target group .....	5
1.2	Scope .....	5
1.3	Reference documents .....	6
1.4	Links to the relevant Internet pages .....	7
<b>2</b>	<b>Use of EBICS in the Swiss financial services sector</b> .....	<b>8</b>
2.1	EBICS basic principles .....	8
2.2	Applicable EBICS specification .....	8
2.2.1	EBICS timeline .....	8
<b>3</b>	<b>Security</b> .....	<b>9</b>
3.1	Security aspects under the EBICS security concept .....	9
3.2	TLS version and cypher .....	9
3.3	Electronic signature .....	10
3.4	Key management .....	10
<b>4</b>	<b>Order types</b> .....	<b>11</b>
4.1	Administrative order types .....	11
4.2	Banking order types .....	11
4.2.1	"fileName" attribute .....	11
4.2.2	EBICS service .....	11
4.2.3	SignatureFlag .....	11
4.2.4	"requestEDS" attribute .....	12
4.2.5	DateRange .....	12
<b>5</b>	<b>BTF parameters</b> .....	<b>13</b>
5.1	ServiceName .....	13
5.2	Scope .....	14
5.3	ServiceOption .....	14
5.3.1	Swiss issuer code .....	15
5.3.2	Standard values .....	15
5.4	MsgName .....	15
5.4.1	"version" attribute .....	15
5.4.2	"variant" attribute .....	15
5.4.3	"format" attribute .....	15
5.5	Container .....	15
<b>6</b>	<b>EBICS procedure</b> .....	<b>16</b>
6.1	Initialization using pairs of keys .....	16
6.2	Blocking participants .....	16
6.3	Customer protocol .....	16
	<b>Appendix A: Table of tables</b> .....	<b>17</b>

# 1 Introduction

---

The EBICS working group commissioned by the PaCoS (Payments Committee Switzerland) has produced Swiss Recommendations for implementing the EBICS standard in the Swiss financial services sector. This is documentation of the EBICS configuration settings and parameters used by the financial institutions for the Swiss financial services sector. The document is intended to provide assistance to software partners and users and provides relevant recommendations according to best practice. The use of EBICS is optional for institutions in Switzerland.

With the EBICS standard, there is now an industry standard for financial services in the European area that has established itself across all sectors. In Germany, it has been mandatory for financial institutions to support this standard since January 2008.

Following the foundation of the Franco-German company EBICS SCRL in June 2010, this standard has become even more widespread in versions since 2.4 because it is used in both Germany and France. In particular, the publication of joint Implementation Guidelines has led to wider distribution of the standard.

## 1.1 Purpose of the document, and its target group

---

This document supplements documentation published by EBICS SCRL (see references [1] – [5]) and is intended primarily for software developers and system administrators.

It is intended to document the specific conventions relating to the use of EBICS in the Swiss financial services sector.

## 1.2 Scope

---

This document describes the use of the EBICS standard in Switzerland.

Since, in some respects, the EBICS standard allows for different implementation options, the Swiss financial services sector has decided to agree on certain options and apply them consistently.

The document describes only these implementation decisions which have been agreed upon.

Financial institutions are also free to support other variants provided for under the standard and these will then be regulated in the financial institution's own documentation.

### 1.3 Reference documents

Ref	Document	Title	Source
	<b>Base documents</b>		
[1]	2017-03-29-EBICS_V_3.0-FinalVersion.pdf	EBICS Specification	EBICS
[2]	2017-03-29-EBICS Common IG basierend EBICS 3.0.pdf	Common Implementation Guide EBICS 3.0	EBICS
[3]	EBICS 3.0 schema H005FinalVersion07-08-2017.zip	EBICS 3.0-schema files (.xsd) with types, order types, data structures and functions.	EBICS
[4]	2017-03-29-EBICS Common IG basierend EBICS 3.0.pdf	Common Implementation Guide EBICS 3.0	EBICS
[5]	EBICS security concept	Can be obtained on request at <a href="mailto:info@ebics.de">info@ebics.de</a>	EBICS
	<b>Additional documents</b>		
[6]	EBICS Version 3.0 FinalDE-29-03-2017.pdf	Appendix 1 of the interface specification for remote data transmission between customer and credit institution in accordance with the RDT [remote data transmission] agreement "Specification for the EBICS connection" Version 3.0	DK
[7]	EBICS_Anhang_TransportLayer SecurityDE-29-03-2017.pdf	EBICS Appendix "Transport Layer Security"	DK
[8]	2019-07-04-Mapping_EBICS-BTF-AA-Sortiert_wie_Anlage_3_zzgl_SonstigerThemen.pdf	Mapping_EBICS-BTF-AA (Germany)	DK
[9]	20180808113947EBICS3.0_aid e_a_la_migration_V1.1.pdf	Mapping_EBICS-BTF-FileFormat-Parameters (France)	CFONB
[10]	EBICS_BTF_Parameter_CH.pdf	BTF parameters CH	SIX

Table 1: Reference documents

## 1.4 Links to the relevant Internet pages

Organization	Link
CFONB	<a href="http://www.cfonb.org">www.cfonb.org</a>
DK (ZKA)	<a href="http://www.ebics.de">www.ebics.de</a> (German)
EBICS	<a href="http://www.ebics.org">www.ebics.org</a> (English)
SIX (SIX Interbank Clearing)	<a href="http://www.iso-payments.ch">www.iso-payments.ch</a> <a href="http://www.paymentstandards.ch">www.paymentstandards.ch</a> <a href="http://www.ebics.ch">www.ebics.ch</a>

Table 2: Links to Internet pages

## 2 Use of EBICS in the Swiss financial services sector

---

### 2.1 EBICS basic principles

---

The basic principles of EBICS are documented in detail on the EBICS SCRL website.

### 2.2 Applicable EBICS specification

---

This document regards version 3.0 of the EBICS specification [1].

From November 2021, the Swiss financial institutions that offer EBICS will support version 3.0 server-side.

**Please note:** In order to use version 3.0, co-ordination with the respective financial institution is required.

However, where EBICS has already been implemented in Switzerland, this is based on EBICS specification version 2.5 and can continue to be offered unchanged by the financial institutions. Nevertheless, it is recommended that new customer connections are implemented on the basis of the specifications in this document.

#### 2.2.1 EBICS timeline

---

With the introduction of EBICS 3.0, the mandatory support of EBICS version 2.4 will expire and from this point on will no longer be officially supported by the financial services sector.

Version 2.5, on which the majority of the current EBICS offers of financial institutions in Switzerland are based, will be officially supported by the financial services sector for a further three years (until the end of 2024).

**Please note:** The use of EBICS 3.0 is required for support of the ISO 20022 schema migration to the 2019 version.



## 3 Security

### 3.1 Security aspects under the EBICS security concept

If correctly implemented, the protocol enables end-to-end security, i.e. it is a secure transport channel.

For security to be guaranteed, the EBICS security concept expects that certain conditions will be met at the end points – the financial institution and the customer.

The financial institution, the software manufacturer that has mapped the EBICS protocol in its solution and the customer are responsible for implementing these points.

For use in the Swiss financial services sector, the following points regarding the customer's system from the EBICS security concept must be contractually agreed between the parties before any use.

**The customer is responsible for the following:**

- Internal communication channels for unencrypted technical banking data and unencrypted electronic signatures are protected against interception and manipulation.
- Internal communication channels for EBICS messages are protected against interception and manipulation.
- The customer is solely responsible for protecting the customer's software and internal communication channels and customer-specific solutions must be implemented.

**The software developer is responsible for the following:**

- The participant's private keys are protected from being read or changed by unauthorized parties.
- The bank's public keys are protected from being changed by unauthorized parties.
- The secret symmetric keys are protected against being read or changed by unauthorized parties.
- The certificate that is used as the trust anchor when checking the financial institution's TLS certificate is protected against being changed by unauthorized parties.
- The customer's software is protected against any manipulation which could mislead the participant about the progress of EBICS transactions.

**The financial institution is responsible for the following:**

- Guidelines for the secure storage of private/public keys form part of the financial institution's terms and conditions for customers.

### 3.2 TLS version and cypher

It must be taken into consideration that at least TLS version 1.2 must be mandatory used for secure file transfer on the Internet [7].

### 3.3 **Electronic signature**

---

In Switzerland, approval for instructions sent via a direct submission interface is normally given by means of a single signature which in most cases represents a company and not an individual. This procedure is based on the premise that these instructions are sent by the customer from a secure environment, the greatest possible degree of automation is desirable and personalized signatures have been checked before transmission by the customer's software (e.g. in the customer's ERP system).

In practice, combined versions are also used, where, for example, a personalized signature is appropriate or distributed digital approval is given via the institution's online system (sometimes also by means of written approval or via fax). This approach is supported on the server side by supporting the VEU (distributed electronic signature) system.

Whether the VEU can be used depends on the contractual arrangement between the customer and the financial institutions, and on what the financial institution offers.

### 3.4 **Key management**

---

The following variations relating to electronic signature procedure and key length are supported in Switzerland (version "H005" of the EBICS protocol envisages the use of the following procedures):

- "X002" for the authentication signature
- "A005" or "A006" for the electronic signature
- "E002" for the encryption
- Key length: 2048 Bit

The electronic signature procedures and key lengths offered by each financial institution should be agreed with the institution.

## 4 Order types

---

In EBICS 3.0, a distinction is made between administrative and (bank) technical order types.

While the administrative order types in all EBICS versions (2.x and 3.x) and variants (DE, FR) have uniform order type codes, the classification used to identify the technical order types is dependent on the EBICS version or variant used.

With the introduction of EBICS version 3, however, the country-specific classification for identifying technical order types was standardized (BTF coding).

### 4.1 Administrative order types

---

The administrative order types are used, inter alia, for the administration of the EBICS channel and include tasks such as fetching the transmission protocol, key exchange or retrieving the BTF parameters supported by the server.

The administrative order types are exhaustively documented in the EBICS Standard [1], [2].

### 4.2 Banking order types

---

The following order types are available for sending banking-related files to the financial institution or for collecting banking-related files from the financial institution:

- BTU (upload to the financial institution) and
- BTD (download from the financial institution)

#### 4.2.1 "fileName" attribute

---

In addition to the specification of the technical properties of the file using the BTF parameters of the EBICS service in question, the local file name on the customer system can optionally also be specified *exclusively* for the **BTU** order type.

This information can make troubleshooting and support easier.

#### 4.2.2 EBICS service

---

The EBICS service requested by the client is specified using the corresponding BTF parameters.

The general structure and functionality of the BTF parameters is clarified in section 5 "BTF parameters".

#### 4.2.3 SignatureFlag

---

If the SignatureFlag is used, the EBICS server checks whether the transmitted file has been fully delivered by the sender with the required combination of electronic signatures.

If the SignatureFlag is missing, the file must be released by the customer for further processing by the financial institution outside the EBICS channel (e.g. e-banking).

**4.2.4 "requestEDS" attribute**

---

When using the optional requestEDS attribute, files with incomplete electronic signatures are not rejected by the server, but placed in the wait queue for the distributed electronic signature.

**Please note:** There must be a corresponding contractual agreement with the financial institution for the use of the distributed electronic signature.

**4.2.5 DateRange**

---

By specifying a date range, the request for the collection of files from the financial institution can only be limited in time for the BTD order type (creation date, account statement date).

**Please note:** This feature is not supported by all financial institutions.

## 5 BTF parameters

The technical characteristic of a file and the desired EBICS service are specified in EBICS 3.0 by indicating BTF parameters.

<b>ServiceName</b>	<ul style="list-style-type: none"> <li>• Use of the existing globally defined service name code list</li> </ul>
<b>Scope</b>	<ul style="list-style-type: none"> <li>• Use of the globally defined scope</li> </ul>
<b>ServiceOption</b>	<ul style="list-style-type: none"> <li>• Use of the global EBICS service option rules</li> <li>• Definition of the CH service options</li> <li>• Definition of the bilateral service options used in Switzerland with assignment of an owner code</li> </ul>
<b>MsgName</b>	<ul style="list-style-type: none"> <li>• Message name</li> </ul>
<b>Container</b>	<ul style="list-style-type: none"> <li>• Container according to EBICS code list</li> </ul>

In addition to the name of the service and the message designation (message standard) the “scope” (= the issuer of the technical set of rules used for the message) must also always be specified.

Further optional parameters can be specified for a fine-granular identification of the file to be transmitted.

The BTF parameters are used both for the specification of files for the transmission to the financial institution as well as for the collection from the financial institution and in administrative order types.

The EBICS BTF parameters currently used in CH and LI (depending on the institution) can be found in the document BTF parameters CH [10].

### 5.1 ServiceName

The ServiceName parameter is the central parameter within BTF. It identifies the corresponding EBICS service of the financial institution using a standardized code list.

The services include banking services such as the submission of payment orders or the provision of account statements and reports.

These services can be used with messages in different message standards, versions and according to different sets of rules.

The available codes for ServiceName are defined in the EBICS standard and thus guarantee a consistent, cross-market designation.

## 5.2 Scope

---

The scope parameter defines the set of rules according to which a message file was created.

Since the specification of the message standard used is generally not sufficiently precise for a correct processing of the message file, the scope parameter must always be supplied.

The scope is also specified by codes defined in the EBICS standard

The code values are either:

- 2-digit ISO 3166 country codes (CH, DE, FR,...) or
- 3-digit EBICS defined issuer codes for globally valid sets of rules (GLB for SEPA and SWIFT FIN, CGI), as well as
- the code BIL for bilaterally agreed rules.

The code CH (= SPS, Swiss Payments Standard) is used for payment traffic in CH and LI.

The scope also influences the designation structure of the available service options.

## 5.3 ServiceOption

---

Specific sub-variants of a service can be identified using the optional ServiceOption parameter.

The structure of the ServiceOption code is dependent on the scope used.

ServiceOptions are specified by 3 to 10-digit ServiceOption codes:

- ServiceOption codes for scope = GLB are fixed 3-digit codes and are defined in the EBICS standard.
- ServiceOption codes for scope = ISO 3166 country code are a fixed 4-digit code always starting with an X in CH.

### Example:

XB2B – direct debit submission, without right of objection, single-origin

- ServiceOption codes for scope = BIL have 5 to 10 digits.

In Switzerland and Liechtenstein, ServiceOption codes are always 6 to 10 digits, beginning with the Swiss issuer code (see section 5.3.1) and a maximum of 5 freely assignable characters.

### Example:

CH001COR - PostFinance direct debit submission, only COR1

---

### 5.3.1 Swiss issuer code

---

This code is used in Switzerland for identifying the bilateral ServiceOptions.

The code consists of the character string "CH" and a 3-digit issuer number.

Issuer number 000 is reserved for SPS-defined variants, further numbers are assigned by means of a request to the address [billing-payments.pm@six-group.com](mailto:billing-payments.pm@six-group.com) by the PaCoS EBICS working group.

### 5.3.2 Standard values

---

If the ServiceOption parameter is not specified when using scope = "CH", then the general SPS definitions or the institution-specific standard offer will apply for the corresponding service.

## 5.4 MsgName

---

MsgName contains the technical designation of the message type, e.g. pain.001 or mt940, always in lower case.

### 5.4.1 "version" attribute

---

The optional "version" attribute must always be provided in CH and LI if the document to be transmitted does not correspond to the schema version of the current SPS guidelines for the message type (only for ISO 20022).

### 5.4.2 "variant" attribute

---

The optional "variant" attribute is currently not used in CH and LI.

### 5.4.3 "format" attribute

---

The optional "format" attribute can be used if necessary in order to identify documents such as PDFs or non-standardized lists in csv, json or xml format.

## 5.5 Container

---

The optional container parameter identifies files that are transmitted as a ZIP file or embedded in an XML container.

In CH and LI, e.g. ISO 20022 account statements and reports (camt.053, camt.054, camt.052) as well as PDF documents are always provided by the financial institutions as ZIP files.

---

## 6 EBICS procedure

---

### 6.1 Initialization using pairs of keys

---

Initialization in Switzerland takes place according to the standard (German version), where the procedure is as follows:

1. The customer signs the contract documentation for their financial institution.
2. The financial institution sends the EBICS access data including the hash values for the financial institution to the customer.
3. The customer carries out INI and HIA order types using their EBICS system.
4. The customer sends the signed initialization letter by post, including their hash values, to the financial institution.
5. The financial institution compares the hash values and checks the signatures.
6. The financial institution accepts the keys and gives technical authorization for the contract.
7. The customer carries out the HPB order type using their EBICS system and compares the hash values of the financial institution in the response to HPB with those in the letter giving the EBICS access data.
8. The customer accepts the keys using their EBICS system.

Once all the initialization steps have been successfully completed, the customer and the financial institution can exchange data.

### 6.2 Blocking participants

---

Swiss financial institutions support the administrative order type SPR for blocking an EBICS user.

An EBICS user can also be blocked manually (e.g. by telephone or other means of communication). The procedure is as follows:

1. The event leading to the blocking occurs (e.g. on the basis of a phone call from the customer).
2. The financial institution blocks the contract manually.
3. The contract cannot be used until it is initialized again.

**Important:** Regardless of how the user is blocked (using order type SPR or manually), the block on an EBICS user always applies solely to the EBICS communication channel!

### 6.3 Customer protocol

---

All actions and events that occur when files are sent, fetched and signed are recorded in EBICS and made available to the customer in EBICS and as a machine-evaluable protocol in the ISO 20022 standard (pain 002).

The customer protocol contains all actions and status information on the partner ID (customer ID). This protocol can be fetched by authorized users with the administrative order type HAC.



## Appendix A: Table of tables

---

Table 1:	Reference documents .....	6
Table 2:	Links to Internet pages .....	7