EBICS

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

"Swiss Market Practice Guidelines EBICS"

Version 1.3 – 20.12.2019

General note

Any suggestions or questions relating to this document should be addressed to the financial institution in question or to SIX Interbank Clearing at the following address: 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.

Amendment control

Version	*Date*	*Comment*	*Valid from:*
1.3	20.12.2019	Section 1.1: Address corrected. Section 1.4: Reference documents updated. Section 1.5: Links updated. Section 2.2: Note on TLS version added. Section 2.5.3: New order types for external batch booking breakdown (QR-bill) using camt.054 added. Sections 2.5.4 and 2.5.5: Newly added.	01.01.2020
1.2	28.11.2017	Change in section 2.5.1, Payment types CH-DD COR1/B2B Note added about messages being delivered in ZIP containers in sections 2.5.2 and 2.5.3	01.01.2018
1.1	16.12.2016	Changes in sections 2, 3 and 4	01.01.2017
1.0	10.04.2015	First edition	01.01.2016

Table of contents

1 Introduction

A working group commissioned by the PaCoS (Payments Committee Switzerland) has produced Swiss Recommendations for implementing the EBICS standard in the Swiss financial services sector. These are recommendations that have been agreed among the financial institutions. The use of EBICS is not mandatory 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 Amendment control

This document is subject to the amendment authority of

SIX Interbank Clearing Ltd
Hardturmstrasse 201
CH-8021 Zurich

and reflects the recommendations of Swiss financial institutions. Any future amendments and additions will be made by SIX Interbank Clearing.

The latest version of this document can be downloaded from the SIX Interbank Clearing website at the following address:

http://www.ebics.ch

1.2 Purpose of the document, and its target group

This document supplements documentation published by EBICS SCRL (see references [1] - [4]) 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.

1.3 Scope

This document describes the use of the EBICS standard in Switzerland. It derives from the EBICS Specification [1] based on Version 2.5 of the Franco-German EBICS Implementation Guidelines.

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.

This 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.

1.4 Reference documents

Ref	Document	Title	Source
	Base documents		
[1]	EBICS_Version_2.5_Final-16-05-2011.pdf	Appendix 1 of the interface specification for data transmission between the customer and the credit institution according to the DFÜ Agreement "Specification for joining EBICS" Version 2.5	DK (ZKA)
[2]	EBICS_Annex2_OrderTypes-FileFormats-04-07-2019.pdf	Order types – Annex 2 of the EBICS specification	DK (ZKA)
[3]	EBICS_Common_IG_based_EBICS_2.5.pdf	Common Integrative Implementation Guide to Supplement the EBICS Specification V2.5	DK (ZKA)
[4]	ebics_xml_schema-12-07-2011.zip	EBICS schema files (.xsd) listing schema types, types of order, data structures and functions	EBICS
	Additional documents		
[5]	EBICS Security Concept	Can be requested at info@ebics.de	EBICS
[6]	EBA guidelines on the security of internet payments	Final Guidelines on the Security of Internet Payments	EBA
[7]	EU guidelines on security for payments initiated electronically	Payment Service Directive 2	EU

Table 1: Reference documents

1.5 Links to the relevant Internet pages

Organization	Link
DK (ZKA)	www.die-deutsche-kreditwirtschaft.de/dk/zahlungsverkehr/electronic-banking/dfue-verfahren-ebics.html
EBICS	www.ebics.de (German) www.ebics.org (English)
SIX	www.iso-payments.ch www.sepa.ch www.six-group.com/interbank-clearing
European Banking Authority (EBA)	www.eba.europa.eu/-/eba-issues-guidelines-to-strengthen-requirements-for-the-security-of-internet-payments-across-the-eu
European Union (EU)	http://ec.europa.eu/finance/payments/framework/index_en.htm

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 is based on the EBICS specification [1] version 2.5 and will be valid for implementation by banks from January 2017.

However, where EBICS has already been implemented in Switzerland, this is based on EBICS specification version 2.4 and can continue to be offered unchanged by the financial institutions, especially with regard to the points listed below. Nevertheless, it is recommended that new customer connections are implemented on the basis of the specifications in this document.

It must be taken into consideration that at least TLS version 1.2 must be mandatory used for secure file transfer on the Internet from 2020.

2.3 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 personalised 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 personalised signature is appropriate or distributed digital approval is given via the institution's online system. Since 2017, this approach has been 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.

2.4 Key management

The following variations relating to electronic signature procedure and key length are supported in Switzerland (version "H004" 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 EU procedures and key lengths offered by each financial institution should be agreed with the institution.

2.5 Types of technical banking order

In Switzerland, order type codes are used to identify different types of technical banking order.

Depending on what the financial institution can offer, the codes listed in Appendix 2 of EBICS 2.5 are available for use.

In addition, Swiss financial institutions also offer the relevant codes for identifying CH-specific order types.

The codes for these order types have X or Y as the first letter (for uploads to the financial institution) or Z (for downloads from the financial institution).

Swiss financial institutions all provide lists of the order types that they support and the corresponding codes.

2.5.1 Codes for submitting ISO 20022 messages to Swiss financial institutions

The following table shows the codes used in Switzerland to identify the technical banking order types for submitting messages to Swiss financial institutions (codes shaded in grey are not offered by all financial institutions):

Transaction type	Swiss payment type	EBICS 2.5 order type code	Message type
Mixed submission within one message, all payment types	all	XE2	pain.001.001.03.ch.02
Domestic payments in CHF and EUR	01 - 04	YE1	pain.001.001.03.ch.02
SEPA transfer	5	YE5	pain.001.001.03.ch.02
Foreign payments , all currencies	6	YE6	pain.001.001.03.ch.02
Domestic payment order in CHF	7	YE7	pain.001.001.03.ch.02
Bank check/Postcash domestic and abroad, in all currencies	8	YE8	pain.001.001.03.ch.02
Customer Direct Debit Initiation for Swiss direct debits with right of objection, for the banks' LSV+ procedure	CH-TA	XL3	pain.008.001.02.ch.03
Customer Direct Debit Initiation for Swiss direct debits with no right of objection, for the banks' BDD procedure	CH-TA	XL4	pain.008.001.02.ch.03
Customer Direct Debit Initiation for Swiss basic direct debit procedure (COR1) – PostFinance procedure	CH-DD	XL5	pain.008.001.02.ch.03
Customer Direct Debit Initiation for Swiss business direct debit procedure (B2B) – PostFinance procedure	CH-DD	XL6	pain.008.001.02.ch.03
SEPA transfer Direct Debit Initiation, CORE	SDD CORE	XE3	pain.008.001.02.chsdd.02
SEPA transfer Direct Debit Initiation, B2B	SDD B2B	XE4	pain.008.001.02.chsdd.02

Table 3: Codes for submitting ISO 20022 messages

Note: The message types in the above table can be submitted with either the ISO Namespace or the Swiss Namespace.

2.5.2 Codes for collecting ISO 20022 status messages from Swiss financial institutions

The following table shows the codes used in Switzerland to identify technical banking order types for collecting status messages from Swiss financial institutions (codes shaded in grey are not offered by all financial institutions):

Transaction type	EBICS 2.5 order type code	Message type
Status report mixed payment/direct debit/CHTA/SDD	Z01	pain.002.001.03.ch.02
Status report transfers (response to CH pain.001)	Z02	pain.002.001.03.ch.02
Status report Swiss direct debits (response to CH pain.008)	Z03	pain.002.001.03.ch.02
Status report SEPA direct debit orders (response to CH pain.008 SDD)	Z04	pain.002.001.03.ch.02

Table 4: Codes for collecting ISO 20022 status messages

Note: Messages are always delivered in a ZIP container.

2.5.3 Codes for collecting ISO 20022 account statements and associated batch booking breakdowns from Swiss financial institutions

The following table shows the codes used in Switzerland to identify technical banking order types for account statement messages and associated batch booking breakdowns from Swiss financial institutions:

Transaction type	EBICS 2.5 order type code	Message type
Account statement at the end of the reporting period	Z53	camt.053.001.04
Debit or credit advice, general	ZS2	camt.054.001.04
Batch booking breakdown (grouped by the FI)	Z54	camt.054.001.04
Other batch booking breakdown to account statement camt.053 (grouped by the FI)	ZS8	camt.054.001.04
Batch booking breakdown of QRR payments to account statement camt.053 (grouped by the FI)	ZQR	camt.054.001.04
Batch booking breakdown of ISR payments to account statement camt.053 (grouped by the FI)	ZE1	camt.054.001.04
Batch booking breakdown of SCOR payments to account statement camt.053 (grouped by the FI)	ZRF	camt.054.001.04

Transaction type	EBICS 2.5 order type code	Message type
Batch booking breakdown of Swiss direct debits to account statement camt.053 (grouped by the FI)	ZS3	camt.054.001.04
Batch booking breakdown to account statement camt.053 (grouped by the customer)	ZS4	camt.054.001.04

Table 5: Codes for collecting ISO 20022 reporting messages

Note: Messages are always delivered in a ZIP container.

2.5.4 Codes for collecting ISO 20022 balance reports and associated batch booking breakdowns from Swiss financial institutions

Some financial institutions also provide balance reports on intraday account movements.

The following table shows the codes used in Switzerland to identify technical banking order types for collecting balance report messages from Swiss financial institutions:

Transaction type	EBICS 2.5 order type code	Message type
Balance report, Intraday account movements	Z52	camt.052.001.04
Batch booking breakdown to balance report camt.052 (grouped by the FI)	ZS5	camt.054.001.04
Batch booking breakdown to balance report camt.052 (grouped by the FI)	ZS9	camt.054.001.04
Batch booking breakdown of QRR payments to balance report camt.052 (grouped by the FI)	ZQ2	camt.054.001.04
Batch booking breakdown of ISR payments to balance report camt.052 (grouped by the FI)	ZE2	camt.054.001.04
Batch booking breakdown of SCOR payments to balance report camt.052 (grouped by the FI)	ZR2	camt.054.001.04
Batch booking breakdown of Swiss direct debits to balance report camt.052 (grouped by the FI)	ZS6	camt.054.001.04
Batch booking breakdown to balance report camt.052 (grouped by the customer)	ZS7	camt.054.001.04

Table 6: Codes for collecting ISO 20022 balance report messages

Note: Messages are always delivered in a ZIP container.

2.5.5 Codes for institution-specific transaction types from Swiss financial institutions

The following table shows the code ranges reserved in Switzerland for the identification of institution-specific order types for collection from / upload to the Swiss financial institutions:

Transaction type	EBICS 2.5 order type code	Message type
Institution-specific transaction types Upload	XZ*	*
Institution-specific status messages Download	ZZ*	pain.002.*
Institution-specific transaction types Download	ZY*	*

Table 7: Codes for institution-specific transaction types

3 EBICS procedure

3.1 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 EBCIS 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.

3.2 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 initialised 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!

4 EBICS security

4.1 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 producer who integrated the EBICS protocol in their system and the customer are all responsible for implementing these aspects.

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.

4.2 Security aspects of EU guidelines and directives

On 19 December 2014, the EBA (European Banking Authority) issued guidelines on the secure handling of Internet payments: "Final Guidelines on the Security of Internet Payments" (see also reference [6]).

The EBA guidelines in some respects go further than the requirements of the EBICS security concept, partly because of the increasing risks in relation to corporate file transfer. For example, the following explicit requirements are specified for "strong authentication" (reference [6], in section "Specific control and security measures for internet payments", from page 18):

"The initiation of internet payments, as well as access to sensitive payment data, should be protected by strong customer authentication. PSPs should have a strong customer authentication procedure in line with the definition provided in these guidelines."

"Strong customer authentication" is defined as follows (reference [6], "Definitions", page 11):

"Strong customer authentication is, for the purpose of these guidelines, a procedure based on the use of two or more of the following elements – categorised as knowledge, ownership and inherence:

i) something only the user knows, e.g. static password, code, personal identification number;

ii) something only the user possesses, e.g. token, smart card, mobile phone;

iii) something the user is, e.g. biometric characteristic, such as a fingerprint.

In addition, the elements selected must be mutually independent, i.e. the breach of one does not compromise the other(s).

At least one of the elements should be non-reusable and non-replicable (except for inherence), and not capable of being surreptitiously stolen via the internet.

The strong authentication procedure should be designed in such a way as to protect the confidentiality of the authentication data."

These specifications were also included in the EU Payment Service Directive 2 (PSD2), published in December 2015 (see Art.97 and Art.98 in [7]) and will therefore be transferred into EU-wide mandatory law on payments initiated electronically with effect from 2018. In connection with this (in compliance with Art. 98), the EBA document will be transferred into another EU-wide mandatory regulation, "EBA regulatory technical standard (RTS) on authentication and communication" by the middle of 2017.

Regardless of exactly when implementation of this RTS becomes mandatory, procedures for strong customer authentication and for secure order authorisation (via a "separate EBICS or non-EBICS channel") should be put in place now wherever possible.

The EBICS standard supports both the use of hardware token-based certificates for the purpose of stronger authorisation and the distributed electronic signature system via a "separate channel", so financial institutions are already able to offer these already.

Appendix A: Table of tables