Use of EBICS for the Clearing & Settlement of Instant Payment Transactions
(Delta - Concept)

(Electronic Banking Internet Communication Standard)

www.ebics.org

Date: October, 30th 2019
## Contents

1. Motivation.................................................................................................................................................. 3
2. Preparatory Considerations for an “Instant Request” schema........................................................... 4
3. Proposal for the ebics_inst_request_H005.xsd.................................................................................... 7
1 Motivation

EBICS has been successfully used between bank and CSMs for the clearing of SEPA payments for many years - changes in the specification of the procedure were not necessary for this use case / case of application.

However, to allow the clearing of instant payments according to the SCTinst rulebook of the European Payments Council the EBICS process has to be adjusted to fulfil the necessary performance requirements.

The present "delta concept" describes which adjustments are necessary to the existing standard for the clearing of instant payments. However, these deviating rules only apply to this scenario.

In particular, a variation of the schema ebics_request_H005.xsd is specified which takes the requirements of an "instant clearing" into consideration. Under the name ebics_inst_request_H005.xsd, this variation represents an modification of EBICS version 3.0, dedicated to the clearing of instant payments.

Apart from the modified structure of the request-xsd, the usual H005 schema set is used in this scenario. This means that the new schema is applicable within the framework of the EBICS version 3.0 instead of the existing request schema.

In practice, this means that in CSMs for instant payments, the new xsd must be added in a top-schema dedicated for this use case, i.e. ebics_inst_H005 contains both the standard request (for administrative transactions of an instant CSM) and the new instand request.

All other parts of the specification and schema H005 remain unchanged.

It is also important to note that the proven EBICS procedure for the standard scenarios "customer to bank communication" and "interbank communication without special performance requirements" remains completely unchanged.
Preparatory Considerations for an “Instant Request” schema

The current ebics_request_H005 is as follows:

- **Diagram 1: EBICS-Request (Version 3.0, schema version H005)**

The three element groups `<header>`, `<AuthSignature>` and `<body>` are always present. The header of the EBICS-request contains static and mutable header entires. Its specifications depend on whether you are in the initialization phase or in the transfer phase of the request. The specification of the body depends on the phase of the request on the one hand but on the other hand also on whether it is an upload or a download request.

For the clearing of instant payments the following conclusion can be drawn from this:

- Payment transaction information are sent from one party to another, i.e. only upload requests occur.
- In order to optimize the speed of data transfer, all information should be transmitted to the receiving party in one single step. Therefore, the initialization phase is extended by the data that normally is only sent in the transfer phase. This must be done while maintaining the appropriate security requirements.
Use of EBICS for the Clearing & Settlement of Instant Payment Transactions
Delta - Concept of October 30th 2019

For the element group <header> the following considerations should be discussed for a one-step "instant request" (grey boxes in the diagram):

Annotation: By this attribute all data of the element group <header> are considered in authSignatur (authenticate = true)

Only one phase (initialization) is used (non choice) - for the unique "link" between request and response the element <Nonce> can be used (with <Timestamp>) to limit the storage time on the server.

Since there is only one phase and no segments are transferred, all information in <mutable> is unnecessary. The element group can be omitted.

Diagram 2: Considerations for the element group <header>
For the element group <body> the following considerations should be discussed for a one-step "instant request" (grey boxes in the diagram):

**Diagram 3: Considerations for the element group <body>**

In addition to the fundamental considerations mentioned above regarding the structure of the "instant request", the following points have to be mentioned:

**Unique linking of the request and the response**

In order to use the standard ebics response also for the clearing of instant payments the following approach is used: The element <Nonce> (data type 16-digit hexBinary, its storage on the server side can be limited by the timestamp provided) and the response element <TransactionID> have the same data type, namely 16-digit hexadecimal coded with binary content. Therefore, the request value from <Nonce> can be returned via <TransactionID> in the response.

**Signature of <OrderData>**

Although both (ES and authentication key) have the same minimum key length and the same cryptography, for security reasons a second certificate (self-signed or issued by a CA, the decision is made by the responsible scope) is used to sign the payment data. This approach is analogous to the EBICS standard procedure.

**Further key information relating to <OrderData>**

A new local data type must be defined for the element group <static>, since it is considerably smaller than the group in the standard request.

Since a new data type must be defined anyway, this opportunity can be used to provide further key information about the transaction in a structured way (e.g. the message ID).
3 Proposal for the ebics_inst_request_H005.xsd

Taking into account the considerations from the previous chapter, the following draft of an “instant request” schema results. In addition to actual adjustments, optional elements/element groups (but superfluous in this use case) are eliminated. This makes the schema more compact and reduces the risk of errors during implementation.

In addition to the changes of the request the top-schema ebics_H005 has to be extended by an include to ebics_inst_H005: To ensure that administrative transactions according to the "normal" ebics standard can also be carried out in this system, both ebics_inst_request_H005 and ebics_request_H005 are included:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<schema xmlns="http://www.w3.org/2001/XMLSchema" xmlns:ebics="urn:org:ebics:H005" targetNamespace="urn:org:ebics:H005"
  elementFormDefault="qualified" attributeFormDefault="unqualified" version="1.0">
  <annotation>
    <documentation xml:lang="en">ebics_inst_H005.xsd includes all schema files (delta for instant payments incuded) in order to enforce unique element and type names in the EBICS namespace.</documentation>
  </annotation>
  <include schemaLocation="ebics_request_H005.xsd"/>
  <include schemaLocation="ebics_inst_request_H005.xsd"/>
  <include schemaLocation="ebics_response_H005.xsd"/>
  <include schemaLocation="ebics_keymgmt_request_H005.xsd"/>
  <include schemaLocation="ebics_keymgmt_response_H005.xsd"/>
</schema>
```
The following adjustments were made in the request xsd:

- In the element group `<header>` the subgroup containing only `<TransactionID>` is removed.
- The hash value of the encryption key is omitted since it occurs again in the element group `<body>`. This leads to the prevention of assigning contradictory data in a request.
- In `<OrderDetails>` only BTF parameters which refer to banking transactions can be used (BTUOrderParams).
- The group `<mutable>` is omitted completely.
In the area <body> only the group <DataTransfer> is needed. However, this group is now mandatory.

- The 'choice' structure is summarized into a sequence group. But not all information is needed (anymore). All that remains is the base-64 encoded and encrypted order data as well as information on encryption.

- The data digest of the order data is omitted since the order data is already delivered in this step.

- It can be discussed whether some key information about the payment transaction may be helpful (e.g. <MsgID> and/or <UETR> ).

- The element <AdditionalOrderInfo> should remain to transport further transaction-related information for which no separate element has been specified (usable only by bilateral agreement).
Use of EBICS for the Clearing & Settlement of Instant Payment Transactions
Delta - Concept of October 30th 2019

Diagram 6: ebics_inst_request_H005 – structure of <body>