# Interface Certification for a FIN Interface

BOX Messaging Hub (formerly known as BOX For SWIFTNet)

Conformance Statement

## Table of Contents

# 1 General Information

## 1.1 Supplier

Full name of the organisation that has registered this interface product and the name of the author of this conformance statement.

| | |
|---|---|
| **Organisation** | **Intercope International Communications Products Engineering GmbH** |
| **Author** | **Jens Huser** |
| **Date** | **June 2012 ( Renewal 2016 )** |

## 1.2 Product Information

The name and version numbers of the interface product to which this certification and conformance claim applies.

| | |
|---|---|
| **Product Name** | **BOX Messaging Hub (formerly known as BOX For SWIFTNet)** |
| **Product Version Number** | **314 and above** |

## 1.3 Operational Environment

The hardware platform(s) and/or software platforms for which this product's performance is guaranteed.

| | |
|---|---|
| **Hardware Platform on which product is guaranteed** | IBM System z<br>SUN<br>IBM p_series<br>PC |
| **Software Platform on which product is guaranteed** | Solaris<br>AIX<br>Windows<br>Linux<br>z/Linux<br>z/OS_USS |

## 1.4 Customer Implementation Environment

The hardware platform and software environment in which this interface product's customer implementation is defined (as required to achieve full certification after an interim certification).

| | |
|---|---|
| **Hardware Platform on which product was implemented** | System Model: IBM,9119_FHA<br>Machine Serial Number: 65180BC<br>Processor Type: PowerPC_POWER6<br>Processor Implementation Mode: POWER 6<br>Number Of Processors: 1<br>Processor Clock Speed: 4208 MHz<br>CPU Type: 64_bit<br>Kernel Type: 64_bit<br>LPAR Info: 21 B4SAQL1<br>Memory Size: 6144 MB<br>Good Memory Size: 6144 MB<br>Platform Firmware level: EH350_049<br>Firmware Version: IBM,EH350_049 |
| **Software Platform on which product was implemented** | AIX: 6100_04_05_1015/64Bit<br>DB2: DB2Client V9.7<br>WAS: V7.0.0.11/64bit<br>MQ: V7 |

## 1.5 Packaging Statement

The main possibilities are:

- The FIN interface is realised on one platform with an integrated Relationship Management interface, and another platform hosts the communication interface with its own security administration.
- The FIN interface is integrated with an RMA interface and a communication interface on one platform.
- Other variations are possible. If used they are described below.

| **Product is stand-alone** | |
|---|---|
| **Product is integrated with another (which)** | Communication Interface Alliance Gateway;<br>Alliance Web Platform for Security Administration<br>BOX Messaging Hub includes Relationship Management<br>BOX Messaging Hub includes Backoffice integration capabilities |

# 1.6 Integration Support

The table describes if the product uses the Message Queue Host Adapter or Remote API Host Adapter as specified by SWIFT, or if it uses a proprietary or other industry standard solution.

| | |
|---|---|
| MQHA | To SAG |
| RAHA | No |
| Other | Internal Interface/Protocol to BOX Messaging Hub |

# 2 Conformance Requirements

The conformance requirements for a FIN interface for SWIFTNet release 7 are specified in the corresponding Interface Product Standard. A FIN interface for SWIFTNet release 7 must support the mandatory items referred to in the messaging interface specifications (as referenced in the Product Standard) and any of the additional optional items.

For clarity reasons the conformance statement only lists these functionalities that are still relevant to a FIN Interface after its migration to SWIFTNet release 7. Therefore all functionalities that were proper to the migration have been removed from this version of the conformance statement.

The tables below identify the mandatory and optional elements that a Store-and-forward InterAct messaging interface product may support.

- Column 1 identifies the feature.
- Column 2 contains references to notes which describe the feature in more detail and where appropriate gives reference to the specification source.
- Column 3 describes whether the feature is Mandatory or Optional.
  - A Mandatory feature must be available for all users of the product.
  - An Optional feature, if implemented, is also subject to certification.
- Column 4 is ticked “Y” or “N” to indicate support of the feature.

## 2.1 FIN Application related

| Feature | Note | Mand. (M/O) | Support (Y/N) |
|---|---|---|---|
| Support of FIN message features | A.1 | M | Y |
| Make use of the list of messages defined in the ASP file | A.2.a | O | Y |
| Support of current message standards version | A.2 | M | Y |
| Support of FIN system messages | A.3 | M | Y |

### Notes

A.1 The definitions of FIN message structure and syntax must be followed.

A.2.a The application service profile (ASP) file for the swift.fin services contains the list of all MTs that are supported for a standards version. The FIN messaging interface can use this data as definition of the supported MTs.

A.2 The current message standards version must be supported (see Interface Policy for ongoing support of new versions).

A.3 All the FIN system messages must be supported.

## 2.2 Session Layer Protocol related

| Feature | Note | Mand. (M/O) | Support (Y/N) |
|---|---|---|---|
| FIN Session Layer protocol version 3 | B.1 | M | Y |
| Support batching features | B.2 | M | Y |
| Select preferred user batching timeout | B.2.a | O | Y |
| Select preferred user max batch count | B.2.b | O | Y |
| Select user maximum batch size | B.2.c | O | Y |
| Accept overruled user batching timeout | B.2.d | M | Y |
| Accept overruled user max batch count | B.2.e | M | Y |
| RP User Synch | B.3 | M | Y |
| Session Layer Retry protocol (client) | B.4 | M | Y |
| Session Layer Retry protocol (server) | B.5 | M | Y |
| Return of PKI signature to back-office application | B.6 | O | Y |

### Notes

B.1 Only protocol version 3 is allowed for login.

B.2 The batching features of pv3 must be supported.

B.2.a A user batching timeout value may be specified (otherwise default is accepted).

B.2.b A user maximum batch count may be specified (otherwise default is accepted).

B.2.c A user maximum batch size may be specified (otherwise default is accepted).

B.2.d SWIFT may overrule selected timeout value and require another value.

B.2.e SWIFT may overrule selected batch count value and require another be used.

B.3 RP User Synch applies during a session using a specific protocol version. It does not apply if different protocol versions are used before and after a break in communication.

B.4 The retry of an InterAct request in the absence of a response is mandatory.

B.5 The ability to receive and process a duplicate InterAct response is mandatory.

B.6 The signature calculated by the communication interface may optionally be delivered to the back-office application for audit purposes.

## 2.3 Login/Select related

| Feature | Note | Mand. (M/O) | Support (Y/N) |
|---|---|---|---|
| Login and Select using PKI signatures in pv3 | C.1 | M | Y |
| Alarm if bad SignDN in login ACK in pv3 | C.2 | O | Y |
| Support change of window size | C.3 | O | Y |
| Support of user vendor code | C.4 | M | Y |
| Support of multiple destinations (BIC-8s) | C.5 | O | Y |
| Support of multiple LTs per BIC-8 | C.6 | O | Y |
| Support of synonyms | C.7 | O | Y |
| Support of multiple T&T destinations per BIC-8 | C.8 | O | Y |

### Notes

C.1 This is the standard way to login and select.

C.2 The login ACK is signed by SWIFT, and the corresponding DN should refer to SWIFT. If not, an alarm event should be made. (This also applies to the other SWIFT originated messages).

C.3 The user should have the possibility to change the default window size (after agreement with SWIFT).

C.4 The user vendor code must occur in the OPEN PDU.

C.5 The product may be configured to support multiple BIC-8 destinations; each destination requires its own certificate.

C.6 The product may be configured to support multiple LTs.

C.7 Master destinations may login on behalf of several branch synonym destinations. Each synonym requires its own certificate. The SignDN must be different from the AuthContextDN in this case.

C.8 One BIC-8 may have several test destinations associated.

## 2.4 Test and Training related

| Feature | Note | Mand. (M/O) | Support (Y/N) |
|---|---|---|---|
| Support system wide authorisation bypass for T&T | D.1 | M | Y |
| Optional use of lite certificate in T&T | D.2 | O | Y |
| SignDN used in signing login/select requests, belongs to owner BIC | D.3 | M | Y |

### Notes

D.1 T&T traffic can completely bypass authorisation process.

D.2 With Test & Training, either a lite or a business certificate may be used.

D.3 Each T&T BIC is associated with a live BIC; in most cases the first 7 characters are the same, but if not the T&T BIC is registered to belong to a specific live BIC. This BIC code must appear in the SignDN.

## 2.5 PKI and HSM related

| Feature | Note | Mand. | Support |
|---|---|---|---|

| | | (M/O) | (Y/N) |
|---|---|---|---|
| Support HSMs | E.1 | M | Y |
| Support of token HSMs | E.2 | O | Y |
| Support of box HSMs | E.3 | O | Y |
| Support of HSM monitoring | E.4 | O | N |
| HSM performance | E.5 | O | Y |
| Support of PKI verification failure | E.6 | O | Y |

### Notes

E.1 At least one HSM must be supported.

E.2 The token HSMs are small capacity and limited to use on Windows platforms.

E.3 The box HSMs are of medium to very high capacity and are available on all platforms.

E.4 The monitoring of HSM devices is recommended so that a user can be advised of failure or malfunction.

E.5 By using more than one certificate for any BIC, signature processing may be spread over several HSMs.

E.6 In the event of PKI verification failure, a retry feature should be available.

## 2.6 Authentication related

| Feature | Note | Mand. (M/O) | Support (Y/N) |
|---|---|---|---|
| Presence of authentication for all FIN messages requiring authentication | F.1 | M | Y |
| Make use of ASP definition for authentication of messages | F.1.a | O | Y |
| Absence of authentication for any other message types | F.2 | M | Y |
| Single reference element and no object element in signature calculation | F.3 | M | Y |
| Local Authentication (LAU) | F.4 | M | Y |
| Verification of policy id on received messages | F.5 | M | Y |
| Support of Broadcast Digest as introduced for SSI messages | F.6 | M | Y |

### Notes

F.1 The FIN UHB contains a list of message types which require authentication.

F.1.a The FIN messaging interface can make use of the messages authentication definition from the application service profile (ASP) file for the swift.fin services.

F.2 The FIN UHB contains a list of message types which must not be authenticated. Note however that this can be overruled in exceptional cases i.e. MT 971 as decided by some Market Infrastructures.

F.3 The reference element (for standard digest) should be present without an object element (reserved for FINCopy).

F.4 If the FIN interface is not co-located with the communication interface, then local authentication must be applied to data exchanged between the components.

F.5 FIN messages should be signed using a business certificate held on HSM; the policy id identifies this and should be verified on received authenticated messages.

F.6 The New Standing Settlement Instructions (SSI) FIN messages introduce the broadcast digest. FIN messaging interfaces must support the calculation for sending and verification on reception of the broadcast digest.

## 2.7 Authorisation related

| Feature | Note | Mand. (M/O) | Support (Y/N) |
|---|---|---|---|
| Authenticated messages cannot be sent without authorisation | G.1 | M | Y |
| RMA data must be authenticated during import/export | G.2 | M | Y |
| Manual treatment of messages failing authorisation | G.3 | M | Y |
| Import of RMA authorisations | G.4 | M | Y |

| | | | |
|---|---|---|---|
| No modification of RMA authorisations | G.5 | M | Y |
| RMA data must be resiliently protected | G.6 | M | Y |
| RMA document validity must follow the specification requirements | G.7 | M | Y |
| Support of authorisation failures (log) | G.8 | M | Y |
| Support of authorisation controls (exclusions) | G.9 | M | Y |
| Support of ASP for RMA filtering | G.10 | M | Y |

### Notes

G.1 The authorisation rules must always be followed (RMA documents or bypass).

G.2 Unless the FIN interface and RMA interface are located on the same platform, the RMA data must be authenticated using LAU.

G.3 Any messages which fail to be authorised (on output or input) must be set aside for manual intervention.

G.4 RMA authorisations can be imported to the FIN interface if originating in a RMA interface, or made available if the RMA component is integrated with the FIN component. The importation must include support for partial import, priority given to date-time documents, documents referring to FIN only, documents referring to non-licensed BIC-8's.

G.5 The FIN interface user may not add or modify RMA documents manually or otherwise. Only the RMA interface may modify documents prior to export.

G.6 The RMA documents must be stored resiliently such that no major loss can occur, necessitating complete reconstruction of the data store by new authorisation requests.

G.7 If a message is subject to RMA authorisation, it must pass all checks as specified.

G.8 Authorisation failures should be logged in the audit trail and set aside for manual intervention.

G.9 Authorisation controls should include checks on time validity as well as MT category or type exclusions and inclusions.

G.10 The FIN interface must base the RMA filtering on the information provided in the Application Service Profile (ASP).

## 2.8 FINCopy related

| Feature | Note | Mand. (M/O) | Support (Y/N) |
|---|---|---|---|
| FINCopy for end-user | H.1 | O | Y |
| FINCopy for Central Institution | H.2 | O | Y |
| FIN Inform | H.3 | O | Y |
| Support of authorisation bypass per service profile | H.4 | M | Y |
| Two reference elements plus random value in signature calculation | H.5 | M | Y |
| Presence of two digests for double authentication FINCopy messages | H.6 | M | Y |
| Support of ASP for FINCopy | H.7 | M | Y |

### Notes

H.1 The support of FINCopy is optional for a FIN interface.

H.2 The support of FINCopy for use in a Central Institution is optional for a FIN interface.

H.3 The support of FIN Inform is optional for a FIN interface.

H.4 A service profile may be specified with authorisation bypass. If the FIN interface supports FINCopy it should include support of this feature.

H.5 In calculating a PKI signature for a FINCopy message, two reference elements (for two digests) should be present plus a random value if double authentication is required.

H.6 Those FINCopy profiles specifying double authentication must be based on two digests plus a random element.

H.7 The support of Application Service Profiles for FINCopy services is mandatory for a FIN interface.

## 2.9 FIN Cold Start related

| Feature | Note | Mand. | Support |
|---|---|---|---|

| | | (M/O) | (Y/N) |
|---|---|---|---|
| Traffic reporting to identify messages to be re-sent | I.1 | O | Y |
| Re-sending messages (select and re-queue with PDE) | I.2 | O | Y |
| Reconciling MT 011/019 with messages sent | I.3 | O | Y |
| Reconciling MT 082/083 with messages sent | I.4 | O | Y |
| FIN Cold Start documentation | I.5 | M | Y |

### Notes

I.1 Traffic reporting features consist of the criteria to select messages to report upon and the information reported. \

Criteria for selection are**;**•

ISN range**,** •

OSN range**,** •

Date and Time range (sent or received)**,** •

FINCopy Service code (field 103 from User Header)**,** •

Delivery status (undelivered, delivered, unknown, unsent).

Information reported consists of the FIN message and other processing-related information.

I.2 Re-sending messages is done in two steps: 1. Select user-to-user messages to re-send using a subset of the selection criteria as applicable for Traffic Reporting, 2. Re-queue the messages for further processing with a PDE including the MIR returned by SWIFT. Further processing can include some authorisation steps before the messages arere-sent to SWIFT.

I.3 Reconciling MTs 011/019 with messages sent. An MT 011 indicates that the message is delivered and an MT 019 indicates that the message has been aborted.

I.4 Reconciling MTs 082/083 with messages sent. MT 082/083 processing depends on the parameters that were used to generate the undelivered reports. At a minimum, the MT 082 which is the first message queued for each destination subject to coldstart, should be processed.

I.5 The procedure for restarting the operations after a FIN cold start will use the available features of the interface. Accurate documentation is essential to guide the user so that recovery from the FIN cold start is as easy as possible.

## 2.10 FIN Bulk Retrieval

| Feature | Note | Mand. (M/O) | Support (Y/N) |
|---|---|---|---|
| Support of FIN Bulk Retrieval | J.1 | O | N |
| Processing retrieved files | J.2 | O | N |

### Notes

J.1 The FIN Interface supporting the FIN Bulk Retrieval must allow initiation of the Bulk Retrieval request and handle the notification of the Bulk Retrieval completion.

J.2 This feature processes the content of bulk retrieval Detail and Error records.

# Legal Notices