Interface Certification for a RMA Interface

CGI RMA

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	**CGI IT UK Ltd**
Author	**Bruce Stevens**
Date	**December 2012 (Renewal 2020)**

1.2 Product Information

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

Product Name	**CGI RMA**
Product Version Number	**RMA_3.3.0**

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 p-Series (POWER-PC, POWER6 and POWER7, POWER8) RHEL on x86
Software Platform on which product is guaranteed	AIX7.1 Linux – Red Hat 7.3 or higher Oracle 12.2.0 / 19c IBM Websphere MQ Server 9.0.x.x IBM MQ Client 9.0.x.x Tomcat 8.5.x / 9.0.x, JWS 5.0, Websphere Application Server 9.0.0 Internet Explorer 11.0, Chrome 76+ SAG 7.2.0 / 7.3.0 / 7.4.0

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	IBM p-Series POWER7, RHEL on x86
Software Platform on which product was implemented	AIX 7.1, RHEL 6.5

1.5 Packaging Statement

The main possibilities are:

- The RMA Interface is stand-alone and runs on its own platform.
- The RMA Interface is integrated on the same platform as a SWIFTNet Messaging Interface and a SWIFTNet Communication Interface

- The RMA Interface is integrated on the same platform as a SWIFTNet Messaging Interface but requires a separately packaged SWIFTNet Communication Interface to access SWIFTNet.

Other variations are possible. If used, these should be described below.

Product is stand-alone	Yes
Product is integrated with another (which)	No

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	Yes
RAHA	Yes
Other	No

2 Conformance Requirements

An RMA interface for SWIFTNet release 7 must support the mandatory items referred to in the messaging interface specifications and any of the additional optional items.

The tables below identify the mandatory and optional features that an RMA 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.

The certification of some items as mandatory or optional can depend on the context.

For example support of item D.2 is mandatory for use with a bilateral service such as FIN but optional otherwise, or support of the Export feature is mandatory if the RMA product is standalone but optional if it is integrated with a SWIFTNet Messaging

2.1 Relationship Management Protocol

2.1.1 Commonalities

Feature	Note	Mand. / Optional	Support (Y/N)
Handle set of 8 protocol elements supporting RMA in all their defined versions	A.1	M	Y
Follow state table for authorisations held in data store	A.2	M	Y
Import the RMA application service profile	A.3	M	Y

Notes

A.1 The product must be capable of handling the 8 different cases of the RMA protocol

A.2 The product must be capable of controlling the status of RMA authorisations

A.3 The RMA service profile defines the details on using the RMA service.

2.1.2 Sending Authorisations

Authorisations have to be created and sent over SWIFTNet according to the specifications.

Feature	Note	Mand. / Optional	Support (Y/N)
Create the authorisation	B.1	M	Y
Off-line creation of authorisations	B.2	O	Y
Audit log of sent authorisations	B.3	O	Y
Using the application service profiles	B.4	M	Y
Check for authorisations reaching end of validity period	B.5	O	Y
Generate multiple authorisations	B.6	O	N

Notes

B.1 The product should be capable of creating and sending an authorisation according to the application service profile for a given service, being FIN, InterAct or FileAct.

B.2 The product may support off-line creation of authorisation. These authorisations will be transmitted to SWIFTNet when the connectivity is established.

B.3 An audit log may be kept of sent authorisations

B.4 The application service profile defines the usage of the service, especially which requests are subject to authorisations and when authorisations are mandated.

B.5 A warning could be issued near the end of a validity period to allow prolongation and avoid unexpected rejections.

B.6 When several services are available for which authorisations can be exchanged, the RMA interface can propose to send multiple authorisations in one go for the different services.

2.1.3 Receiving Authorisations

Authorisations have to be received from SWIFTNet, safely stored in the Data Store and handled accordingly.

Feature	Note	Mand. / Optional	Support (Y/N)
Process received authorisation	C.1	M	Y
Generate matching authorisation to send	C.2	M	Y
Off-line processing of received authorisations	C.3	O	Y
Audit log of received authorisations	C.4	O	Y
Automatic acceptance of authorisations	C.5	O	Y

Notes

C.1 The product should be capable of processing a received authorisation.

C.2 The product should be capable of responding with a matching authorisation in bilateral business relationships.

C.3 Received authorisations may be manually verified rather than automatically accepted.

C.4 An audit log may be kept of received authorisations.

C.5 Received authorisations may be automatically accepted based on certain criteria such as BIC-8.

2.1.4 Sending revocations

The RMA interface must be able to send revocation messages to SWIFTNet, based on the status of its underlying authorisation.

Feature	Note	Mand. / Optional	Support (Y/N)
Create revocation PDU	D.1	M	Y
Off-line creation of revocation PDU	D.2	O	Y
Audit log of sent revocations	D.3	O	Y

Notes

D.1 The product should be capable of sending a revocation.

D.2 The product may support off-line creation of revocations. These revocations will be transmitted to SWIFTNet when the connectivity is established.

D.3 An audit log may be kept of sent revocations.

2.1.5 Receiving revocations

The RMA interface must be able to receive revocation messages from SWIFTNet, match it to its underlying authorisation and take appropriate actions on the authorisation.

Feature	Note	Mand. / Optional	Support (Y/N)
Process received revocation PDU	E.1	M	Y
Off-line processing of revocation PDU	E.2	O	Y
Audit log of received revocations	E.3	O	Y

Notes

E.1 The product should be capable of receiving a revocation.

E.2 Received revocations may be manually processed rather than automatically accepted.

E.3 An audit log may be kept of received revocations.

2.1.6 Usage of InterAct Store-and-forward

The RMA interface can support the InterAct store-and-forward protocol or connect a messaging interface supporting this protocol.

Feature	Note	Mand. / Optional	Support (Y/N)
Exchange messages over InterAct store-and-forward. At least one of the following has to be supported:	F.1	M	Y
Pull mode is supported	F.2	O	N
Push mode is supported	F.3	O	Y
Supplier identification is supported (*ProductInfo*)	F.4	M	Y
Configure the reception queue	F.5	O	Y
Support multiple reception queues for service segregation	F.6	O	N
Configure the delivery notification queue	F.7	O	N
Support multiple delivery notification queues for service segregation	F.8	O	N
Processing of received store-and-forward delivery notifications	F.9	O	Y

Notes

F.1 InterAct store-and-forward is the only SWIFTNet messaging supporting the exchange of RMA messages.

F.2 The product may use Pull mode to fetch messages from its queues.

F.3 The product may use Push mode to receive messages from its queues automatically.

F.4 The Supplier Name (PIC) and Supplier Product name should appear in each RMA request *ProductInfo* section.

F.5 Allow configuration of the reception queue. It allows service segregation.

F.6 Segregated services could be supported by using multiple reception queues.

F.7 Segregated services could be supported through configuration of different notification queues (delivery monitoring).

F.8 Allow configuration of the delivery notification queue. It allows service segregation.

F.9 Delivery notification indicates when an RMA message was delivered to the correspondent or if it was not.

2.2 Import/Export Authorisations from/to File

Import and Export functions are very important in order to restore a complete set of authorisations to a secondary instance or to propagate authorisation to subscriber application performing the message filtering.

Feature	Note	Mand. / Optional	Support (Y/N)
Export all authorisations to a file (complete file)	G.1	M/O	Y
Export authorisations (partial). Single criteria is mandatory, but it may combine several of the following:	G.2	M/O	Y
Received or issued authorisations	G.3	O	Y
For a specific service	G.4	O	Y
For a specific BIC-8 mask	G.5	O	Y
Since a specific date/time	G.6	O	Y
Audit log of export	G.7	O	Y
Export file are secured with an local authentication	G.8	M	Y
Import authorisations from a file (complete file)	G.9	M	Y
Import authorisations from a file (partial file)	G.10	M	Y
Check import file for relevance (without import)	G.11	M	Y
Audit log of import	G.12	M	Y
Validate the local authentication value before importing file	G.13	M	Y

Notes

G.1 The product must be able to issue a distribution file of authorisations either for all services or for a specific service. If the data store is shared between the RMA interface and the subscriber application, this test is optional.

G.2 The product must be able to issue a partial distribution file of authorisations. Several criteria are possible, which are left to the implementer. If the data store is shared between the RMA interface and the subscriber application, this test is optional.

G.3 The product may be able to issue a partial distribution file of authorisations send or issued.

G.4 The product may be able to issue a partial distribution file of authorisations for a specific set of services.

G.5 The product may be able to issue a partial distribution file of authorisations for a specific BIC-8 mask.

G.6 The product may be able to issue a partial distribution file of authorisation modified since a date/time.

G.7 An audit log may be kept of exportations.

G.8 A valid Local Authentication must be computed and added to the export file.

G.9 The product should be able to replace the content of its Data Store by importing authorisations from a complete distribution file (may be limited to a single service).

G.10 The product should be able to import authorisations from a partial distribution file.

G.11 The product should be able to report on the contents of the import file prior to import to validate if the import is worth doing.

G.12 An audit log must be kept of importations (if the product supports import).

G.13 The Local Authentication value must be validated before importing the file. The file is processed only if the validation succeeds.

2.3 Local RMA Update

Sometimes, it is necessary to manually take some actions on the RMA Data Store. This is important for bootstrap records and stale records.

Feature	Note	Mand. / Optional	Support (Y/N)
Report on the content of authorisations in the data store	H.1	O	Y
Delete stale authorisations from the RMA data store	H.2	M	Y
Delete bootstrap authorisation from the RMA data store	H.3	O	Y
Add bootstrap records within RMA Data Store	H.4	M	Y
Import the application service profile of that service	H.5	M	Y

Notes

H.1 Reports could detail the content and nature of authorisations.

H.2 Deleting authorisations for correspondent which no longer exist (under controlled access) must be possible.

H.3 Deleting bootstrap authorisations for services in migration period. The migration period is specified in the application service profile.

H.4 Bootstrap records are authorisation to send or authorisation to receive, created without an exchange over SWIFTNet. A bootstrap authorisation cannot be added if the application service profile forbids it.

H.5 The application service profile contains important parameters on how to use the service, including the list of messages subject to authorisation, the activation date and the bootstrapping options.

2.4 Data Store Security

This section covers the minimum security requirements related to the RMA Data Store.

Feature	Note	Mand. / Optional	Support (Y/N)

Access control protected	I.1	M	Y
Audit log of failed logins, and important updates	I.2	M	Y
Access control on part of the RMA Data Store. Criteria may contain one or more of the following:	I.3	O	Y
list of BIC	I.3	O	Y
list of services	I.3	O	Y
Environment (live, pilot, development)	I.3	O	Y
Access control by 4-eyes	I.4	O	Y
Warning when export is needed (including revocation)	I.5	O	Y
Issued authorisations not deleted, only revoked	I.6	M	Y
Received authorisations cannot be added or modified other than through SWIFTNet	I.7	M	Y
Re-verify signature	I.8	O	N
Availability in line with service description	I.9	M	Y

Notes

I.1 The product must secure the user access to its data store.

I.2 Audit logs of all important events should be made.

I.3 The product may segregate access on BICs, services and environment basis.

I.4 The product may rely on 2 secure users to deal with data store access.

I.5 User should be warned of an incoming revocation or of new updates.

I.6 Sent authorisations may not be deleted only revoked.

I.7 Received authorisations cannot be added or modified unless there is a Request delivered by SWIFTNet, signed by the organisation of the Requestor and related to the Issuer.

I.8 Signatures must be able to be verified up to 6 months after an authorisation or revocation has been sent.

I.9 Availability requirements of the RMA service (for subscriber and manager) should meet the SWIFTNet Service Description.

2.5 Supporting Message Generating Applications

Not all message generating applications are aware of RMA Data Store authorisations. This is typically true of legacy applications. The check of the RMA Data Store could be performed by a SWIFTNet Interface application on behalf of the message generating application.

Feature	Note	Mand. / Optional	Support (Y/N)
Provide support for filtering functionally	J.1	O	Y
Trial run of application against RMA data	J.2	O	N

Notes

J.1 Application generating message could request the RMA interface to check the presence of an authorisation based on service, request type, sender and receiver.

J.2 The application may have a mode, where it checks the presence of valid authorisation and report on mismatch. This is possible when the deployment of RMA within the service is in a trial stage.

2.6 BIC file integration

The RMA Interface uses BIC for identifying correspondents. BIC can be integrated or uploaded from the BIC directory.

Feature	Note	Mand. / Optional	Support (Y/N)
Expand BIC	K.1	O	Y
Validate BIC	K.2	O	Y

Notes

K.1 BICs can be expanded in reports and displays.

K.2 BICs can be verified on entry.

2.7 Supportability

Adhering to the same terminology in RMA products allows easy communication between users when they are using products from different Suppliers.

Feature	Note	Mand. / Optional	Support (Y/N)
Adhere to common terminology	L.1	M	Y

Notes

L.1 Adhering to RMA vendor specification terminology ease communication between parties

Legal Notices