



SWIFTNet Interface Qualification for a SWIFTNet RMA Interface

STeP Relationship Manager Conformance
Statement



Legal Notices

Copyright

Copyright © S.W.I.F.T. SCRL ("SWIFT"), avenue Adèle 1, B-1310 La Hulpe, Belgium, or its licensors, 2008 All rights reserved.

You may copy this publication within your organisation. Any such copy must include these legal notices.

Confidentiality

This publication may contain SWIFT or third-party confidential information. Do not disclose this publication outside your organisation without the prior written consent of SWIFT.

Disclaimer

SWIFT supplies this publication for information purposes only. The information in this publication may change from time to time. You must always refer to the latest available version.

Translations

The English version of SWIFT documentation is the only official version.

Trademarks

SWIFT, S.W.I.F.T., the SWIFT logo, Sibos, SWIFTNet, SWIFTAlliance, SWIFTStandards, SWIFTReady and Accord are trademarks of S.W.I.F.T. SCRL. Other SWIFT-derived service and product names, including SWIFTSolutions, SWIFTWatch and SWIFTSupport are tradenames of S.W.I.F.T. SCRL. SWIFT is the trading name of S.W.I.F.T. SCRL. Other product or company names in this publication are tradenames, trademarks, or registered trademarks of their respective owners.

Table of Contents

1	General Information	4
1.1	Supplier	4
1.2	Product Information.....	4
1.3	Conformance Testing Environment.....	4
1.4	Operational Environment	4
1.5	Customer Implementation Environment	5
1.6	Packaging Statement.....	5
1.7	Integration support.....	5
2	Conformance Requirements.....	6
2.1	Protocol related	7
2.2	Data Store related	7
2.3	Sending authorisations	8
2.4	Receiving authorisations	8
2.5	Sending revocations.....	8
2.6	Receiving revocations.....	9
2.7	Export authorisations in file.....	9
2.8	Import authorisations from file	9
2.9	Housekeeping functions on authorisations	9
2.10	BIC file integration.....	10

1 General Information

1.1 Supplier

Full name of the organisation that has registered this SWIFTNet Interface product and the name of the author of this Conformance Statement.

Organisation	SunGard AvantGard Payments and SunGard STeP
Author	Eitan Biran
Date	18th December 2007

1.2 Product Information

The name and version numbers of the SWIFTNet Interface product to which this qualification and conformance claim applies.

Product Name	STeP Relationship Manager
Product Version Number	1.0

1.3 Conformance Testing Environment

The hardware platform and software environment in which this SWIFTNet Interface product's conformance is validated.

Hardware Platform on which product was tested	Sun
Software Platform on which product was tested	Solaris 10

1.4 Operational Environment

If the environment for which you want to claim and guarantee conformance is not identical to the environment in which conformance was validated, please specify the hardware platform(s) and/or software platforms for which this SWIFTNet product's performance is guaranteed.

Hardware Platform on which product is guaranteed	Sun, IBM, Microsoft
Software Platform on which product is guaranteed	Solaris 10, AIX 5.3, Windows 2000/2003/XP

1.5 Customer Implementation Environment

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

Hardware Platform on which product was implemented	Sun Fire V440, 4 CPUs, 8GB memory
Software Platform on which product was implemented	Solaris 10, STeP Relationship Manager 1.0 SAG/RA 6.0

1.6 Packaging Statement

Explains how this product is packaged.

The main possibilities are:

The SWIFTNet RMA Interface is stand-alone and runs on its own platform.

The SWIFTNet RMA Interface is integrated on the same platform as a SWIFTNet FIN Interface and a SWIFTNet Communication Interface

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

Other variations are possible. If used they are described below.

Product is stand-alone	Yes
Product is integrated with another (which)	

1.7 Integration support

If not integrated how does this product link to user client or server products? Does it use the Message Queue Host Adapter or Remote API Host Adapter as specified by SWIFT? Does it use a proprietary or other industry standard solution?

MQHA	
RAHA	Yes
Other	Own gateways, local and remote

2 Conformance Requirements

The conformance requirements for a SWIFTNet RMA Interface for SWIFTNet release 6 are specified in the SWIFTNet Interface Product Standard. A SWIFTNet RMA Interface for SWIFTNet release 6 must support the mandatory items referred to in the Product Standard and any of the additional optional items.

The tables below identify the mandatory and optional features that a SWIFTNet RMA Interface product may support. They indicate for each of the features whether the qualified application supports and/or requires the elements, by a Yes or No in the respective columns on the right.

Column 1 identifies the feature.

Column 2 contains references to notes which describe the feature in more detail and where possible 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 is also subject to qualification if present.*

Column 4 indicates support of the feature (“Y” or “N”).

The qualification 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 SWIFTNet RMA product is standalone but optional if it is integrated with a SWIFTNet FIN product.

2.1 Protocol related

Handle set of 8 protocol elements supporting RMA	A.1	M	Y
Export and Import authorisation records	A.2	M	Y
Support local update of the RMA data store	A.3	M	Y
Follow state table for authorisations held in data store	A.4	M	Y
Pull mode is supported	A.5	O	N
Push mode is supported	A.6	O	Y
Vendor identification is supported	A.7	M	Y
Mixed XML Canonicalization must be used	A.8	M	Y

Notes

- A.1 The product must be capable of handling the 8 different cases of the RMA protocol. Either push mode or pull mode may be used.
- A.2 The product must be capable of importing and exporting authorisations in the correctly structured XML document. The authentication and integrity rules must be supported. (If import and export are supported).
- A.3 The product must be capable of deleting a previously accepted authorisation from the RMA data store.
- A.4 The product must be capable of controlling the status of RMA authorisations.
- A.5 The product may use Pull mode to fetch authorisations from its queues, or
- A.6 The product may use Push mode to receive authorisations from its queues automatically.
- A.7 The Vendor Name (PIC) and Vendor Product name should appear in each RMA request.
- A.8 The XML document must be canonicalized using the Mixed XML Canonicalization algorithm published in the SWIFTNet Link Interface Specification.

2.2 Data Store related

Access control protected	B.1	M	Y
Access control by 4-eyes	B.2	O	Y
Access control per service	B.3	O	N
Access control limited by BIC	B.4	O	Y
Issued authorisations not deleted, only revoked	B.5	M	Y
Re-verify signature	B.6	O	N
Audit log of failed logins, and important updates	B.7	M	Y
Warning when export is needed (including revocation)	B.8	O	N
Availability in line with service description	B.9	M	Y
Ability to update configuration data	B.10	O	Y
Support of testing facility	B.11	O	Y
Support of service deployment facility	B.12	O	N

Notes

- B.1 The product must secure the user access to its data store
- B.2 The product may rely on 2 secure users to deal with data store access.
- B.3 The product may segregate access on a service basis.
- B.4 The product may segregate access on an owning BIC basis.
- B.5 Sent authorisations may not be deleted only revoked.
- B.6 Signatures must be able to be verified up to 6 months after an authorisation or revocation has been sent.
- B.7 Audit logs of all important events should be made.
- B.8 User should be warned of an incoming revocation or of new updates.
- B.9 Availability requirements of the RMA service (for subscriber and manager) should meet the SWIFTNet Service Description.

- B.10 RMA configuration data such as new service schema should be able to be integrated in the local configuration data.
- B.11 Testing facilities should be available for customers.
- B.12 New service deployment should be supported.

2.3 Sending authorisations

Create the authorisation	C.1	M	Y
Off-line creation of authorisations	C.2	O	Y
Audit log of sent authorisations	C.3	O	Y
Check for authorisations reaching end of validity period	C.4	O	N
Configure the notification queue(s)	C.5	O	Y

Notes

- C.1 The product should be capable of creating and sending an authorisation.
- C.2 The product may support off-line creations in support of a dial-up facility.
- C.3 An audit log may be kept of sent authorisations.
- C.4 A warning could be issued near the end of a validity period to allow prolongation and avoid unexpected rejections.
- C.5 Segregated services could be supported through configuration of the notification queue.

2.4 Receiving authorisations

Process received authorisation	D.1	M	Y
Generate matching authorisation to send	D.2	M	Y
Off-line processing of received authorisations	D.3	O	Y
Audit log of received authorisations	D.4	O	Y
Configure the delivery queue	D.5	O	Y
Support multiple queues	D.6	O	N
Automatic acceptance of authorisations	D.7	O	Y

Notes

- D.1 The product should be capable of receiving an authorisation.
- D.2 The product should be capable of responding with a matching authorisation in bilateral business relationships such as FIN. For other relationships this feature is optional.
- D.3 Received authorisations may be manually verified rather than automatically accepted.
- D.4 An audit log may be kept of received authorisations.
- D.5 Segregated services could be supported through configuration of the delivery queue.
- D.6 Segregated services could be supported by using multiple delivery queues.
- D.7 Received authorisations may be automatically accepted based on certain criteria such as BIC-8.

2.5 Sending revocations

Create revocation PDU	E.1	M	Y
Off-line creation of revocation PDU	E.2	O	Y
Audit log of sent revocations	E.3	O	Y

Notes

- E.1 The product should be capable of sending a revocation.
- E.2 The product may support off-line creations in support of a dial-up facility.
- E.3 An audit log may be kept of sent revocations.

2.6 Receiving revocations

Process received revocation PDU	F.1	M	Y
Off-line processing of revocation PDU	F.2	O	Y
Audit log of received revocations	F.3	O	Y

Notes

- F.1 The product should be capable of receiving a revocation.
 F.2 Received revocations may be manually processed rather than automatically accepted.
 F.3 An audit log may be kept of received revocations.

2.7 Export authorisations in file

Export all authorisations issued for a service	G.1	M	Y
Export all received authorisations for a service	G.2	M	Y
Export partial: all authorisations issued since a date	G.3	M	Y
Export partial: all authorisations issued for a BIC-8	G.4	M	Y
Audit log of export	G.5	O	Y

Notes

- G.1 The product should be able to issue a full distribution file of authorisations issued.
 G.2 The product should be able to issue a full distribution file of authorisations received.
 G.3 The product should be able to issue a partial distribution file of authorisations issued since a certain date.
 G.4 The product should be able to issue a partial distribution file of authorisations issued by a certain BIC-8.
 G.5 An audit log may be kept of exportations.

2.8 Import authorisations from file

Import all authorisations issued for a service	H.1	M	Y
Check import for relevance	H.2	M	Y
Audit log of import	H.3	M	Y

Notes

- H.1 The product should be able to import authorisations from file.
 H.2 The product should be able to report on the contents of the import file prior to import.
 H.3 An audit log may be kept of importations.

2.9 Housekeeping functions on authorisations

Report on the content of authorisations in the data store	I.1	O	Y
Remove stale authorisations from the RMA data store	I.2	M	Y

Notes

- I.1 Reports could detail the content and nature of authorisations.
 I.2 Removing authorisations (under controlled access) must be possible.

2.10 BIC file integration

Expand BIC	M.1	O	Y
Validate BIC	M.2	O	Y

Notes

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

M.2 BICs can be verified on entry.