



Interface Certification for a Communication Interface

ACI Money Transfer System™

Conformance Statement

Table of Contents

Title Page	1
1 General Information	3
1.1 Supplier.....	3
1.2 Product Information.....	3
1.3 Operational Environment.....	3
1.4 Customer Implementation Environment.....	3
1.5 Packaging Statement.....	3
1.6 Integration Support.....	4
2 Conformance Requirements	5
2.1 SWIFTNet Security Administration Related.....	5
2.2 SWIFTNet Link Interface Related.....	5
For any service the basic set of primitives are:.....	5
2.3 Local Authentication.....	7
2.4 Event Handling.....	8
Legal Notices	9

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	ACI Worldwide
Author	Lisa Avery
Date	November 2010 (Renewal 2019)

1.2 Product Information

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

Product Name	ACI Money Transfer System™
Product Version Number	3.0 and 4.0 and 5.0

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 pseries
Software Platform on which product is guaranteed	AIX 6.1 and AIX 7.1 (ACI Money Transfer System ("MTS") operates on AIX 6.1 operating system. MTS contains processes (SnIclientadapter and SnIserveradapter) and they may reside on the same CPU as MTS or the same CPU as the SNL or Alliance Gateway)

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	
Software Platform on which product was implemented	

1.5 Packaging Statement

The main possibilities are:

- The communication interface is stand-alone and runs on its own platform.
- The communication interface is integrated on the same platform as a FIN interface with its own security administration.
- Other variations are possible. If used they are described below.

Product is stand-alone	The ACI Money Transfer System (MTS) Communications Interface (CI) is stand-alone and 1. may co-reside on the same platform with the SNL or SAG, or;
-------------------------------	--

	2. may be implemented on a stand-alone platform, or; 3. may be implemented on the same platform with the MTS FIN application
Product is integrated with another (which)	

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	
RAHA	Supported adapter
WSHA	
Other	

2 Conformance Requirements

The conformance requirements for a communication interface for SWIFTNet release 7 are specified in the corresponding interface specifications. A communication interface for SWIFTNet release 7 must support the mandatory items referred to in the communication 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 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 certification if present.
- Column 4 indicates support of the feature ("Y" or "N").

2.1 SWIFTNet Security Administration Related

Feature	Note	Mand. / Optional	Support (Y/N)
Certify or recover nodes	A.1	O	N
Change password of a security profile	A.2	O	N
List available certificates	A.3	O	N
List detailed information of certificates	A.4	O	N
Support of more than 250 certificates	A.5	O	N
Renewing certificates	A.6	M	Y

Notes

- A.1 Certify a new node in the directory or recover a previously certified node.
- A.2 Change the password for a given security profile.
- A.3 Return a list of available certificates according to some search criteria.
- A.4 Return detailed information about the certificates within a given profile.
- A.5 The product may support handling of more than 250 certificates.
- A.6 The renewal of certificates is automatically performed by SWIFT but only if they are actually used within their validity lifetime. The product should contain a facility to initialise and destroy a security context for each DN to trigger automatic renewal

2.2 SWIFTNet Link Interface Related

For any service the basic set of primitives are:

Initialisation Primitives

Feature	Note	Mand. / Optional	Support (Y/N)
Sw:Init	B.1	M	Y
Sw:Term	B.2	M	Y
Sw:HandleInit	B.3	M	Y
Sw:HandleTerm	B.4	M	Y

Security Primitives

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

SwSec:CreateContext	B.5	M	Y
SwSec:DestroyContext	B.6	M	Y
SwSec:SignEncrypt	B.7	O	N
SwSec:VerifyDecrypt	B.8	O	N

Request/Response Primitives

Feature	Note	Mand. / Optional	Support (Y/N)
SwInt:Exchange	B.9	O	Y
SwInt:Send	B.10	M	Y
SwInt:Wait	B.11	M	Y
SwInt:Handle	B.12	M	Y

Miscellaneous Primitives

Feature	Note	Mand. / Optional	Support (Y/N)
Sw:GetDateTime	B.13	O	N
Sw:SMAGetStatus	B.14	O	N
Sw:SMACommand	B.29	O	N

FileAct Primitives

Feature	Note	Mand. / Optional	Support (Y/N)
Sw:ExchangeFile	B.15	O	Y
Real-time	B.15A	O	Y
Store-and-forward	B.15B	O	N
Sw:HandleFile	B.16	O	Y
Real-time	B.16A	O	Y
Store-and-forward	B.16B	O	N
Sw:FetchFile	B.17	O	N
Sw:GetFileStatus	B.18	O	N
Sw:ListFileStatus	B.19	O	N
Sw:AbortFile	B.20	O	N
Sw:SubscribeFileEvent	B.21	O	Y
Sw:HandleFileEvent	B.22	O	Y
Sw:GetFileDigest	B.23	O	N

Store-and-forward Primitives

Feature	Note	Mand. / Optional	Support (Y/N)
Sw:ExchangeSnF	B.24	O	N
Sw:Handle	B.25	O	N
Sw:PullSnF	B.26	O	N
Sw:GetSnFStatus	B.27	O	N

Return SNL Information

Feature	Note	Mand. / Optional	Support (Y/N)
Sw:HandleResponseInfo	B.28	O	N

Notes

- B.1-B.6 Refer to the SWIFTNet Link Interface Specification.
- B.7, B.8 Refer to the SWIFTNet Link Interface Specification. Mandatory for FIN.

B.9-B.12	The exchange may be asynchronous or synchronous. For SWIFTNet FIN, asynchronous mode is recommended.
B.14	Sw:SMAGetStatus may be used to obtain HSM status.
B.15, B.16	These primitives are used for real-time and store-and-forward.
B.15-B.23	Refer to the SWIFTNet Link Interface Specifications.
B.24-B.27	Refer to the SWIFTNet Link Interface Specifications.
B.28	Only required for specific services.
B.29	Sw:SMACommand may be used to issue commands on the HSM

2.3 Local Authentication

Feature	Note	Mand. / Optional	Support (Y/N)
Each message is signed for authentication	C.1	M	Y
Authentication achieved by non-reversible algorithm	C.2	M	Y
Each interface owns an authentication key	C.3	M	Y
Keys to be stored securely	C.4	M	Y
Confidentiality achieved by middleware	C.5	O	N
Authentication independent of middleware	C.6	M	Y
Messages failing authentication to be blocked	C.7	M	Y
Other traffic can be authenticated	C.8	O	N

Notes

- C.1 Each InterAct message must be authenticated between a SWIFTNet Communication Interface and any other SWIFTNet FIN Interface.
- C.2 The algorithm to be used is HMAC based on SHA-256.
- C.3 Each SWIFTNet Interface must possess at least one key.
- C.4 Authentication keys must be protected against disclosure.
- C.5 Encryption may be performed by middleware; the authentication protocol does not include encryption.
- C.6 Authentication does not depend on middleware used between SWIFTNet interfaces.
- C.7 Messages which fail authentication must not be allowed to continue and an event should be logged.
- C.8 InterAct traffic other than SWIFTNet FIN traffic, is recommended to be authenticated. Authentication is only mandated (C1) for SWIFTNet FIN traffic.

2.4 Event Handling

Feature	Note	Mand. / Optional	Support (Y/N)
SwSubscribeEvent	D.1	O	N
Sw:HandleEvent	D.2	O	N

Notes

- D.1 At initiation, a server application can use the event subscription primitives to be notified with events through a given endpoint.

- D.2 The server application that has previously subscribed to the event endpoint receives the events through an SwCallback

Legal Notices

Copyright

SWIFT © 2019. All rights reserved.

Restricted Distribution

Do not distribute this publication outside your organisation unless your subscription or order expressly grants you that right, in which case ensure you comply with any other applicable conditions.

Disclaimer

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 and binding version.

Trademarks

SWIFT is the trade name of S.W.I.F.T. SCRL. The following are registered trademarks of SWIFT: the SWIFT logo, SWIFT, SWIFTNet, Accord, Sibos, 3SKey, Innotribe, the Standards Forum logo, MyStandards, and SWIFT Institute. Other product, service, or company names in this publication are trade names, trademarks, or registered trademarks of their respective owners.

