



SWIFT Partner Management

SWIFTReady Label –  
Exceptions and Investigations  
Technical Validation Guide 2010

Version 2

January 2010

# Legal Notices

## Copyright

SWIFT © 2010. All rights reserved.

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

## 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 is the trade name of S.W.I.F.T. SCRL. The following are registered trademarks of SWIFT: SWIFT, the SWIFT logo, Sibos, SWIFT, SWIFTRReady, and Accord. Other product, service, or company names in this publication are trade names, trademarks, or registered trademarks of their respective owners.

## Table of content

<b>1</b>	<b>Introduction.....</b>	<b>3</b>
1.1	Purpose and Scope.....	3
1.2	Target Audience.....	3
1.3	Related Documents.....	3
<b>2</b>	<b>Technical Validation Process .....</b>	<b>4</b>
2.1	New Label .....	4
2.1.1	Integration with Alliance Interfaces .....	4
2.1.2	Vendors not having ITB Connectivity.....	8
2.2	Label Renewal .....	9
<b>3</b>	<b>Summary of Technical Validation .....</b>	<b>10</b>
<b>4</b>	<b>FAQ .....</b>	<b>11</b>

# 1 Introduction

SWIFT initiated the SWIFTRReady label programme to help application vendors to offer products that are compliant with the business and technical requirements of the financial industry. SWIFTRReady labels certify third party applications and middleware products that support solutions, messaging, standards and interfaces supported by SWIFT.

SWIFT has mandated Wipro (referred hereinafter as the “Validation Service provider”) for performing the Technical Validation of the products applying for a SWIFTRReady Label.

## 1.1 Purpose and Scope

The certification for the SWIFTRReady Exceptions and Investigations label is based on a set of pre-defined qualification criteria which will be validated by means of a technical, functional and customer validation process.

The set of pre-defined qualification criteria is defined in the SWIFTRReady Exceptions and Investigations Label Criteria 2010 ([2]).

This document focuses on the approach that a vendor application must follow to complete the technical validation certified against SWIFTRReady Exceptions and Investigations criteria.

In this document a distinction is made between New Application (for products that apply for the label for the first time) and for Application Renewal (for products that are already labelled the previous year and are applying for renewal of the label).

## 1.2 Target Audience

The target audience for this document is application vendors considering the certification of their middleware suite / business application for SWIFTRReady Exceptions and Investigations Label. The audience must be familiar with SWIFT from a technical and a business perspective.

## 1.3 Related Documents

1. SWIFTRReady Application Programme Overview
2. SWIFTRReady Exceptions and Investigations Label Criteria 2010
3. Message Reference Guide for Standards MX Exceptions and Investigation Release 1.1 and 1.2
4. Exceptions and Investigations Integration Guide
5. AFT test scenario and validation guide
6. MQSA / MQHA test scenario and validation guide

Documents [1] to [4] are downloadable from [www.swift.com/partners](http://www.swift.com/partners). Document [5] and [6] are available in the section Support/Documentation on [www.swift.com](http://www.swift.com).

## 2 Technical Validation Process

In this document, distinction is made between the new label application and label renewal application in terms of number of criteria verified and tests executed by the vendor. The Technical validation focuses on the message validation, standards support, connectivity to Alliance Interfaces and Reference Data Directory integration

The following matrix explain the tests that will be performed by the vendor application

Label Type	Depth of Testing	Message Validation	Standards Support	Integration with Alliance Interfaces	Reference Data
New	Comprehensive	✓	✓	✓	X
Renewal	Automatic (*)	X	X	X	X

(\*) No technical validation is required for the versions of E&I applications that have been certified as SWIFTReady during 2009. Any upgraded versions of applications will, however be subjected to comprehensive testing.

### 2.1 New Label

New Applicants will go through a complete technical validation against the criteria laid down in the SWIFTReady Exceptions and Investigations Criteria [2] document.

The criteria that are verified include:

- Integration with Alliance interfaces
- Support of messaging services
- Support of SWIFT Standards

#### 2.1.1 Integration with Alliance Interfaces

**Requirement:** The Applicant will demonstrate the capability of the product to integrate the SWIFT Alliance Interfaces.

The Applicant needs to demonstrate compliance with at least one of the following options:

- Integration with [Alliance Access](#) or [Alliance Gateway](#) Interface as detailed here below:
- Integration with Alliance Gateway using RAHA and/or MQHA for all messaging services. This compliance is verified through the [SWIFT Interface qualification programme](#).

For Alliance Interface compliance, the support of at least one of the following adaptors will be demonstrated:

- Automated File Transfer mode (AFT) over Alliance Access

## SWIFT Partners

- WebSphere MQ Host Adaptor (MQHA) over Alliance Access
- WebSphere MQ Series Interface for Alliance Access

The vendor needs to successfully connect to and exchange test messages with the Integration Test Bed (ITB).

The vendor must demonstrate the capability of their product to support MX Messaging Standards. To prove their support to MX, the application must be able to connect interactively to Alliance Access or Alliance Gateway using the available connectivity options.

If the application supports more than one adaptor, tests must be performed on each adaptor separately.

### **2.1.1.1 Integration with Alliance Access (AFT, MQSA and MQHA)**

Testing for connectivity to Alliance Access Interface will be verified on the SWIFT Integration Test Bed (ITB) using Alliance Access Release 6.0 or 6.2 or 6.3.

The Applicant will demonstrate the capability of the product to integrate with the Alliance Access. The support for the following adaptors will be demonstrated:

- Automated File Transfer mode (AFT) with Release 6.0 and above
- WebSphere MQ Series Interface for Alliance Access
- WebSphere MQ Host Adaptor (MQHA) over Alliance Access using XMLv2. MQHA is available with Release 6.2 and above

The vendor must connect to SWIFT ITB and receive SWIFT Central Service ACK / NAK notifications.

The Technical Validation documents for the AFT, MQSA and MQHA adaptors are available separately over [www.swift.com](http://www.swift.com) (Partner section). Test scenarios must be followed for every one of the mentioned adaptors.

The vendor must note the following for testing through ITB:

- The vendor will generate and exchange minimum of 2 different scenarios per request type for all the 16 MX messages comprising of bank-to-bank and corporate-to-bank environment as Input Message to SWIFT.
- Currently two releases of SWIFT Standards MX are available
  - SWIFTNet Exceptions and Investigations 1.1.: used in the Bank-to-Bank CUG (in the development, test and training and live environment)
  - SWIFTNet Exceptions and Investigations 1.2.: used in the Corporate-to-Bank CUG (in the development, test and training and live environment)

The MX Standards schema is identical at the business payload level. They are however slightly different at the name space declaration level. The corporate-to-bank flows do not contain the service name in the name space declaration of the Document line. The following table summarises the correct usage of name space declaration in the bank-to-bank and corporate-to-bank flows:

## SWIFT Partners

Message Type	Namespace Declaration	
	corporate-to-bank [EI 1.2]	bank-to-bank & bank-to-corporate [EI 1.1]
camt.007.002.02	urn:swift:xsd:camt.007.002.02	urn:swift:xsd:swift.eni\$camt.007.002.02
camt.008.002.02	urn:swift:xsd:camt.008.002.02	urn:swift:xsd:swift.eni\$camt.008.002.02
camt.026.001.02	urn:swift:xsd:camt.026.001.02	urn:swift:xsd:swift.eni\$camt.026.001.02
camt.027.001.02	urn:swift:xsd:camt.027.001.02	urn:swift:xsd:swift.eni\$camt.027.001.02
camt.028.001.02	urn:swift:xsd:camt.028.001.02	urn:swift:xsd:swift.eni\$camt.028.001.02
camt.029.001.02	urn:swift:xsd:camt.029.001.02	urn:swift:xsd:swift.eni\$camt.029.001.02
camt.030.001.02	urn:swift:xsd:camt.030.001.02	urn:swift:xsd:swift.eni\$camt.030.001.02
camt.031.001.02	urn:swift:xsd:camt.031.001.02	urn:swift:xsd:swift.eni\$camt.031.001.02
camt.032.001.01	urn:iso:std:iso:20022:tech:xsd:camt.032.001.01	urn:swift:xsd:swift.eni\$camt.032.001.01
camt.033.001.02	urn:swift:xsd:camt.033.001.02	urn:swift:xsd:swift.eni\$camt.033.001.02
camt.034.001.02	urn:swift:xsd:camt.034.001.02	urn:swift:xsd:swift.eni\$camt.034.001.02
camt.035.001.01	urn:swift:xsd:camt.035.001.01	urn:swift:xsd:swift.eni\$camt.035.001.01
camt.036.001.01	urn:iso:std:iso:20022:tech:xsd:camt.036.001.01	urn:swift:xsd:swift.eni\$camt.036.001.01
camt.037.001.02	urn:swift:xsd:camt.037.001.02	urn:swift:xsd:swift.eni\$camt.037.001.02
camt.038.001.01	urn:iso:std:iso:20022:tech:xsd:camt.038.001.01	urn:swift:xsd:swift.eni\$camt.038.001.01
camt.039.001.02	urn:swift:xsd:camt.039.001.02	urn:swift:xsd:swift.eni\$camt.039.001.02

- The messages exchanged must adhere to the correct service name specification for the bank-to-bank, bank-to-corporate and corporate-to-bank flows as below:

Message Flow	EI Version	Service Name	Environment
Corporate-to-bank	1.2	swift.corp.eni!p	Test & Training
		swift.corp.eni!x	ITB
Bank-to-bank	1.1	swift.eni!p	Test & Training
		swift.eni!x	ITB
Bank-to-corporate		swift.corp.eni!p	Test & Training
		swift.corp.eni!x	ITB

- When the testing is performed on ITB, the service name specified for ITB environment only must be used
- The application should add the Alliance Access specific messaging interface header to the business payload. The business payload consists of the application header + the Exceptions and Investigations business message. When the application connects with Alliance Access through a Financial EAI, the specific messaging interface header must be added to the business payload.
- The sender destination used in the messages must be the PIC (Partner Identifier Code) used by the application provider to install and license Alliance. The receiver destination of messages must be the same PIC. Or simply stated, messages should be sent to own vendor PIC
- The vendor application must wrap the SWIFT messages using Alliance Access **XML v2 format**
- The vendor must connect to SWIFT ITB, send MX messages, receive SWIFT ACK/NAK and properly reconcile them by updating the status of sent messages

## SWIFT Partners

- Since the sender and receiver BIC [PIC] is the same in the test messages exchanged over ITB, ITB will return the test message back to vendor. The vendor must also process the output messages from SWIFT ITB through the Exceptions and Investigations application.

The vendor must inform SWIFT Partner Management and the Validation Service provider about the completion of the test execution, and provide evidence of testing through application event logs, transmitted messages, and ACK / NAK received messages.

### **Confirmation of Test Execution & Evidence Documents**

After successful exchange of the test messages, the vendor will forward by email to the Validation Service provider the following test evidences:

- Screenshots, Log Files, Reports from application evidencing processing and reconciliation of the SWIFT Messages exchanged
- **For Alliance Access Integration**
  - Connectivity through AFT, MQSA and MQHA**
    - A copy of the XML v2 format files generated by the business application
    - Alliance Access Event Journal Report and Message File spanning the test execution window
  - Connectivity through MQHA**
    - Updated checklist, Message Partner Configuration details as explained in the MQHA Technical Validation Document [MQHA Connectivity]
  - Connectivity through MQSA**
    - Trace Files - SMQSFromMQSeries.TRC and SMQSToMQSeries.TRC

### **Verification of Test Results**

The Validation Service provider will analyse the log files, event journal, the screenshots produced by the vendor to ascertain if;

- all the messages are positively acknowledged by the SWIFT Network by reviewing the log files (MQSA trace files, Alliance Access Event Journal and Message File)
- the Alliance Access messaging interface header is present
- the application header adheres to the schema definition
- the MX Messages adhere to the Exceptions and Investigations Rulebook and MX Message Reference Guide, by sample verification of the MX Messages
- the messages are compliant with the standards release requested in the label criteria document, i.e. EI 1.1 and 1.2

The test results will be analyzed for arriving at the scorecard and recommendation

## Qualification Criteria Verified

Sl. #	SWIFTReady Label Qualification Criteria			Pass / Fail Status
	Section Ref #	Label Requirement		
		Requirement Criteria	Ref #	
1.	3.3.1	Alliance Access Integration Support	1	
2.		Alliance Access Integration Connectivity [AFT /MQSA /MQHA]	2	
3.		Alliance Access Integration – XML v2 Format	3	
4.		Alliance Access Integration – Application Header	4	
5.	3.4	Messaging Support – EI Release 1.1 and 1.2	5	
6.	3.5	Standards Support – MX Message Reference Guide 1.1 and 1.2	6	
7.	3.5.2	Correct Payload Structure	7	
8.	3.5.4	Bank-to-bank and corporate-to-bank – SWIFTNet Service Name	8	
9.	3.7	Message Validation	9	

### 2.1.2 Vendors not having ITB Connectivity

In case the vendor does not have access to the ITB, he may choose to execute their test messages using a customer test environment or a partner's SWIFTReady Financial EAI.

- When testing occurs through a customer, the customer reference must be provided (Name, telephone, function to cater for customer interview).
- When testing occurs through certified SWIFTReady Financial EAI, the EAI name and testing configuration details must be provided.

Please note that the actual test execution and test evidence collection as described in 2.1.1 also apply when testing through a customer or SWIFTReady Financial EAI

## 2.2 Label Renewal

**Mandatory Requirement:** For SWIFTRReady Reconciliation Label 2010, there are no changes to qualification criteria for technical validation and hence no technical validation will be performed for granting SWIFTRReady Label.

**Optional Requirement:** If the vendor application supports the optional requirement of MQHA connectivity, the vendor must perform the Testing for MQHA Connectivity as explained above in section 2.1.1.

### 3 Summary of Technical Validation

Validation Activity		Label NEW	Label RENEWAL
<b>Message Validation</b>	Outgoing	16 EI messages	Automatic Renewal No technical validation is required for the versions of E&I applications that have been certified as SWIFTReady during 2009. Any upgraded versions of applications will, however be subjected to comprehensive testing.
<b>Standards</b>	SRG	EI Release 1.1 & 1.2	
	Rule Book Ref	EI Rulebook	
	Optional Messages	Not Applicable	
<b>Connectivity</b>	Alliance Access	AFT or MQSA or MQHA	
	Message Format	XML v2	
	Indirect Connectivity	Test Evidence / Log File from EAI Application	

## 4 FAQ

1. **Currently we do not have ITB connectivity, and we are NOT sure whether our customers allow us to use their environment. However, we have Alliance Access installed at our end. Could you please clarify, for the technical validation, is it sufficient, if we connect our application to Alliance Access using AFT or MQSA and provide you the evidences?**

Connecting to ITB and exchanging test messages over ITB is mandatory as per the Qualification Criteria for SWIFTReady Exceptions & Investigations Label. If you do not have ITB connectivity, you have to contact SWIFT Partner Management to discuss possible options.

2. **What is the correct setting for the Validation Level in the Alliance Access HeaderInfo field?**

The validation Level in the Alliance Access HeaderInfo must be at least "Intermediate". Otherwise Alliance Access will not validate against the installed ENI schema.

3. **What are the implications of the Validation Level in the HeaderInfo, as we find that all the there have the same level of validation?**

Indeed for MX, unlike MT, the "minimum" and "intermediate" settings have the same behaviour. However, these emission profile settings can be overridden in the XML v2 (Validation Level). So if "none" is specified in XML v2, then it overrides "minimum" and "intermediate" of the emission profile. If "maximum" is present in the emission profile then it is enforced even if "none" is in XML v2.

**\*\*\* End of document \*\*\***