



SWIFT Partner Management

SWIFTReady Label –
Payments
Technical Validation Guide 2010

Version 1

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

1	Introduction.....	3
1.1	Purpose and Scope.....	3
1.2	Target Audience.....	3
1.3	Related Documents.....	3
2	Technical Validation Process	4
2.1	New Label	4
2.1.1	Integration with Alliance Interfaces	4
2.1.2	Vendor not having ITB Connectivity	7
2.1.3	Message Validation and Standards Support.....	8
2.1.4	Testing Reference Data.....	10
2.2	Label Renewal	12
3	Summary of Technical Validation	13
4	FAQ	14
5	List of MTs support for Outgoing Messages.....	16

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”) to perform the Technical Validation of the products applying for a SWIFTRReady Label.

1.1 Purpose and Scope

The certification for the SWIFTRReady Payments 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 Payments is defined in the SWIFTRReady Payments Label Criteria 2010 ([2]).

This document focuses on the approach for the technical validation that a vendor application must follow to complete the technical validation against SWIFTRReady Payments 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 during the previous year and are applying for renewing 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 Payments Label. The audience must be familiar with the SWIFT portfolio from a technical and a business perspective.

1.3 Related Documents

1. SWIFTRReady Application Programme Overview
2. SWIFTRReady Payments Label Criteria 2010
3. AFT / MQHA test scenario and validation guides

Documents [1] to [3] are downloadable from www.swift.com/partners.

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

Application status	Level of Testing	Message Validation	Standards Support	Connectivity	Reference Data
New	Comprehensive	✓	✓	✓	✓
Renewal	Automatic (*)	X	X	X	X

(*) There is no technical validation for Label renewal during 2010 as there are no changes in the MT Standards Release for Payments.

2.1 New Label

New Applicants will go through a complete technical validation against the criteria laid down in the SWIFTReady Payments 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 with SWIFT Alliance Interfaces. For Alliance Access compliance, the support of at least one of the following adaptors will be demonstrated:

- Automated File Transfer mode over Alliance Access (AFT)
- WebSphere MQ Series Interface for Alliance Access (MQSA)
- WebSphere MQ Host Adaptor over Alliance Access (MQHA)

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 FIN protocol and its associated features (example: message validation). The application must be able to connect to Alliance Access either directly via one of the adaptors listed below or indirectly preferably via one of the SWIFTReady Financial EAI applications.

The application must be able to connect interactively to Alliance Interface using the available connectivity options as listed below:

- The message format supported by the Alliance Interface depends on the connectivity options listed here below and the vendor application must support the message formats as required
- The following matrix explains the test that will be performed by the vendor application:

Protocol / Format	Option 1		Option 2			Option 3
	Alliance Access 6.0		Alliance Access 6.2 / 6.3			Alliance Lite
FIN	AFT	MQSA	AFT	MQSA	MQHA	AutoClient
	RJE, XML v2		RJE, XML v2			RJE

The application vendor must demonstrate, at a minimum, support for Alliance Access (option 1 or option 2). In addition, an application can support an optional connectivity to Alliance Lite.

The choice of connectivity option depends on the business and volume throughput requirement. Alliance Access is the preferred choice for middle and high volume traffic while Alliance Lite is mostly suitable for low volume traffic.

The application interfacing with Alliance Access must interactively connect using

- WebSphere MQ Series Interface for Alliance (MQSA)
OR
- WebSphere MQ Host Adaptor (MQHA) (Available in Alliance Access 6.2)
OR
- Automated File Transfer mode (AFT)

2.1.1.1 Integrating with Alliance Access

- 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 Alliance Access. The support for the following adaptors will be demonstrated:
 1. Automated File Transfer mode (AFT)
 2. WebSphere MQ Series Interface for Alliance (MQSA)
 3. WebSphere MQ Host Adaptor (MQHA)

The Technical Validation documents for the AFT, MQSA and MQHA adaptors are available separately over www.swift.com (Partner section). Test scenarios should be followed for all the above mentioned adaptors.

The vendor must note the following for testing through ITB:

- The vendor must inform SWIFT Partner Management and the Validation Service provider before starting the test execution through ITB and advice which connectivity method is being used.

- The testing on ITB can start at any time before the validation window is allotted to the vendor. However, the entire testing on the ITB must be completed within the time window allotted to the vendor.
- The vendor must generate a total of 20 test messages comprising of MT1xx, MT2xx and MT9xx through their application as outbound message from application
- The test messages must be compliant to Standards Release 2010
- The sender destination used in the messages is the PIC (Partner Identifier Code) that was 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 **RJE** or **XML v2 format**
- The vendor must connect to SWIFT ITB, send MT and MX messages, receive SWIFT ACK/NAK and properly reconcile them by updating the status of sent messages.
- 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.

2.1.1.2 Integrating with Alliance Lite

The Vendor application that support Alliance Lite connectivity, must demonstrate capability to exchange FIN messages using AutoClient facility and reconcile the transaction / original message with the LATS acknowledgements

- SWIFT Partner Management has provided a testing service viz. Alliance Lite AutoClient Testing Service (LATS) to facilitate testing the integration of business application / middleware application with Alliance Lite using AutoClient.
- The vendor must subscribe to LATS by registering their PIC and email address and test integrating their FIN messages in RJE format using LATS
- The vendor must generate a total of 20 test messages comprising of MT1xx, MT2xx and MT9xx through their application as “outbound message from application” and submit to LATS using the email connectivity option.
- LATS responds with ACK / NAK / Pseudo NAK / Delivery Notification 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
- A copy of the MT test messages in RJE / XML v2 format generated by the business application
- In addition, the following evidences are required for evaluating the connectivity testing:

Connectivity through AFT / MQHA / MQSA

- Event Journal Report and Message File from Alliance Access spanning the test execution window

Connectivity through MQHA

- Updated checklist, Message Partner Configuration details as explained in the MQHA Technical Validation Document

Connectivity through MQSA

- Trace Files - SMQSFromMQSeries.TRC and SMQSToMQSeries.TRC

Alliance Lite Connectivity through AutoClient (LATS)

- RJE file with file name <filename>.fin from achieve directory
- RJE file with file name <filename>.fin from reception directory containing:
 - Business message received [Messages sent to own PIC]
 - Status of message sent previously
 - Delivery Notification Message received in response to the request made through the test message
- Error files [if any] with file name <filename>.<timestamp>.fin.err from error directory

Verification of Test Results

In order to issue the scorecard and necessary recommendation, the Validation Service provider will analyse the log files, event journal, the screenshots produced by the vendor to ascertain that:

- all messages are positively acknowledged by the SWIFT Network by reviewing the log files (Log file, Trace file, Alliance Access Event Journal and Message File)
- Test messages have been exchanged by the vendor over ITB / LATS
- Test messages adhere to the SWIFT format requirement (RJE and /or XML v2 formats)

Qualification Criteria Verified

Sl. No	SWIFTReady Label Qualification Criteria			Pass / Fail Status
	Section Ref Number	Label Requirement	Req. No	
1.	3.4.1	Alliance Access Integration Support	1.	
2.	3.4.1	Alliance Access Integration – AFT / MQHA / MQSA Support	2.	
3.	3.4.1	Alliance Access Integration – RJE / XML v2 Format	3.	
4.	3.5	SWIFT MT Support	4.	
5.	3.7.1	Standards Release	5.	
6.	3.7.2	Network Validation Rules (MFVR)	6.	

2.1.2 Vendor not having ITB Connectivity

In case the vendor does not have access to the ITB, they may choose to execute their test messages using a customer test environment or a partner’s SWIFTReady Financial EAI with ITB access. In such cases, the following should be noted:

- 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 SWIFTRReady 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 and SWIFTRReady Financial EAI application.

2.1.3 Message Validation and Standards Support

Requirement: The vendor must demonstrate the application's capabilities to support SR2010, the Message Format Validation Rules (MFVR), MT Usage Guidelines and STP Guidelines.

2.1.3.1 Testing Incoming Messages

- The Validation Service provider will send a set of 20 MT test messages consisting of valid messages which need to be uploaded by the vendor into and processed by his application.
- The test messages will have a mix of MT103, MT 103+ and MT 202 COV
- All test messages will be "inward to the application" direction.
- The application must perform the business validations while parsing the incoming message
- User Header Block (Block 3) will contain a unique reference number in the form of a Message User Reference (MUR) for each test message. The MUR will consist of the MT numerical identification followed by test message sequence number.
- The test messages will have generic test data for Accounts, Dates and BIC. The vendor can change the values / customize to their application needs. For ease of customization, the test messages will be sent in a spreadsheet format with a facility to convert the output into a single RJE formatted file for all the test messages or individual RJE formatted files for every test message.

File Naming Convention

- The files will be named SR yy _PymentsMTValidation.xls, where "yy" will represent the Year of the Standards Release. For example, for a file containing MT103 and MT103+ for Standards Release 2010, the file name will be "**SR10_PaymentsMTValidation.xls**"
- The Validation Service provider will also send an MT Test Result Summary file in excel spreadsheet format for the vendor to capture the test results into. The file name will be **xxxx_SRnn_PaymentsMTValidation_Test_Result.xls**, where "xxxx" represents the vendor name and "nn" represents the Standards Release.

Processing the provided SWIFT Message Types

The vendor must input the abovementioned files into the application and perform the business validations. For example, the application can reject a payment message, if the value date is less than current date or greater than 1 month from today's date. Another example could be that the account is not serviced by the application.

- The error listing provided by the application must be easily understandable by business users

Confirmation of Test Execution & Evidence Documents

The vendor must forward through e-mail the following test evidences to the Validation Service provider:

- Sample evidence demonstrating that the application has processed the test messages. This will be done by sending screenshots / log file / application generated reports.
- The MT Test Result Summary file, updated with the test results (**Error Code and Error Line Number**). **A sample of the spreadsheet is provided here below.**

Sl. No.	Message ID (MUR in Block 3)	Business Validation Results	Error Line Number	Error Description	Expected Error Code	Expected Error Line Number	Pass / Fail Status
1	10310000001	Pass	-				
2	10310000002	Error	11				

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 processed by the application
- Analyze the test result to arrive at the scorecard and

2.1.3.2 Testing Outgoing Messages

The application must perform the following validations before forwarding the message to Alliance Access:

- MFVR (Character Set, Syntax, Code word, Semantic, MUG)
- MT Usage Rules listed in SR 2010
- STP Guidelines listed in SR 2010

Generating SWIFT Messages

- The vendor must generate at least one test message for each of the message types required in the criteria document. The list of to be supported messages can be found in section 5 here below.
- The vendor must generate these messages through the business application as outbound (“application to Alliance Access” direction) messages
- Test messages must be compliant to SR 2010
- The vendor application must wrap the SWIFT messages using RJE or XML v2 format

Confirmation of Test Execution & Evidence Documents

The vendor must forward, after the successful exchange of the test Messages, through e-mail the following test evidences to the Validation Service provider:

- Sample evidence demonstrating that the application has processed the test messages. This will be done by sending screenshots / log file / application reports
- A copy of the MT test messages in RJE / XML v2 format generated by the business application

Verification of Test Results

- The Validation Service provider will analyse the log files, event journal, the screenshots produced by the vendor to ascertain that all the messages are processed by the application and analyze the test result to arrive at the scorecard and recommendation.

Qualification Criteria Verified:

Sl. No	SWIFTReady Label Qualification Criteria			Pass / Fail Status
	Section Ref Number	Label Requirement	Req. No	
1.	3.5	Standards (Support for Incoming Message)	9	
2.	3.5	Standards (Support for Outgoing Message)	10	
3.	3.7	Message Validation	11	
4.	3.7.1	Standards Release Guide	12	
5.	3.7.2	Network Validated Rules	13	
6.	3.7.3	MT Usage Rules	14	
7.	3.7.4	STP Guidelines	15	

2.1.4 Testing Reference Data

Requirement: The vendor must demonstrate the application’s capability to validate messages against the BIC and BICPlusIBAN directories. The vendor must use the sample BIC Directory and BICPlusIBAN Directory available on www.swift.com/solutions/messaging/directories.

2.1.4.1 Testing for BIC and BICPlusIBAN Validation

- The test scenario for testing the BIC and BICPlusIBAN are provided in the document attached to this guide
- The test scenarios to be executed in the vendor application will cover:
 - BIC Validation
 - IBAN Structure validation
 - Deriving BIC / Clearing code using BICPlusIBAN Directory
- The test data and sample directory for the testing the BIC / BICPlusIBAN table look-up and validation will be provided to the application vendor before the commencement of the technical validation window
- The application vendor must input these transactions into their application and perform the reference data validation using the sample directories

Generating SWIFT Messages / Error or Warning Notification

Based on the outcome of the validation with the reference data, the output of the test execution must be captured as listed below:

- For the search resulting in positive result, SWIFT messages must be generated in RJE format / XML v2 format
- For the search resulting in negative result, the screenshot displaying the warning / error notification

Confirmation of Test Execution & Evidence Documents

After successful execution of the test scenario for BIC and BICPlusIBAN reference data validation, the vendor must forward, the following test evidences to the Validation Service provider through email:

- Sample evidence demonstrating that the application has processed the BIC and BICPlusIBAN reference data validation. This will be done by sending screenshots or log file.
- A copy of the MT test messages in RJE / XML v2 format generated by the business application.

Verification of Test Results

The Validation Service provider will validate the vendor output against the expected results and analyze the test result to arrive at the scorecard recommendation

Qualification Criteria Verified

Sl. No	SWIFTReady Label Qualification Criteria			Pass / Fail Status
	Section Ref Number	Label Requirement	Req. No	
8.	3.10.1	BIC Directory	16	
9.	3.10.4	BICPlusIBAN	17	

2.2 Label Renewal

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

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

3 Summary of Technical Validation

Test Activity		Label NEW	Label RENEWAL
Message Validation	Outgoing	20 messages of MT1xx, 2xx, 9xx	Automatic Renewal (There is no technical validation for Label renewal during 2010 as there are no changes in the Standards Release for Payments category. Optionally, the vendor can perform connectivity tests as detailed in section 2.1.1 for the support of MQHA and / or AutoClient)
	Incoming	20 messages of MT103 and 202 COV. Only valid scenarios will be tested	
Standards	SRG	2010	
	Market Practice	NA	
	Optional Messages	Not Verified	
Connectivity	Alliance Access	FIN → AFT and MQHA	
	Alliance Lite Release 2.0	FIN → AutoClient	
	Message Format	AFT → RJE	
		MQSA → RJA / XML v2	
MQHA → RJE / XML v2			
	AutoClient FIN → RJE		
	Indirect Connectivity	Test Evidence / Log File from EAI Application	
Reference Data Directory	BIC & BICPlusIBAN	Scenario Based Testing	
	Integration	Screenshot Verification	

4 FAQ

1. Is it mandatory to provide error code and line number however our application gives only textual description of the error encountered?

It is good if you can populate the appropriate error code [which is a standardised way of reporting an error]. However, taking into account the limitation of the business applications, SWIFT can still accept the textual description of the encountered error coupled with the erroneous field impacted during the message validation.

2. In the test messages supplied to us for test execution, can we change the sender and receiver BICs (in header) so that we won't need to change this setup in our system?

The test messages are provided in an excel file. You can change / customize the values according to your requirement, before processing through the application.

3. How the application should perform validation on the "Copy of fields" in n9x messages?

SWIFT does not validate the relationship between the copied field(s) and the original message. Even if not defined for the referenced message, any valid field except 77F, 77G or 77T (error code(s): T13) is accepted as the "Copy of fields".

SWIFT only validates the syntax of a BIC used in the text of the appended message. A Test and Training destination may not be referenced by a LIVE user (error code(s): T27 T46).

The values furnished in the Copy of field[s] must be a "valid" field. Since the relationship with the original message [furnished in Filed 11S] and the copied fields[s] are not checked, the validation is performed individually for the "copy of field[s].

4. What is the need for Test data directory containing BIC and Currency directories?

All BIC and Currency data's provided in the test data directory should be considered as good values and to be updated in your system. While performing validation of the input messages, the data's related to BIC and Currency should be validated against the list of data's provided in the test data directory. If the value is not present in the directory then the message should be reported as FAIL.

5. What if my application only supports a subset of messages mentioned in technical validation guide?

Evaluation report will be formed based on the number of messages provided to us as test evidence. The list of Message Types for which the evidences are not provided will be reported in the evaluation report enabling SWIFT will to take a final decision.

6. Is it mandatory to provide the MT messages in RJE files?

Yes, all MT Messages should be supplied in RJE file format only.

7. For generating the outgoing messages, is there any restriction that we must use only the BICs that are supplied to us for the incoming messages or can we use our own data?

There is no restriction that you must use only these BIC for generating outgoing messages. Instead, you must use your PIC as sender and receiver of the Message, which would facilitate.

5 List of MTs support for Outgoing Messages

MT	Usage
101	Request For Transfer
102 and 102+	Multiple Customer Credit Transfer
103 and 103+	Single Customer Credit Transfer
200	Financial Institution Transfer for its own account
201	Multiple Financial Institution Transfer for its own account
202 and 202 COV	General Financial Institution Transfer
203	Multiple Financial Institution Transfer
205 and 205 COV	Financial Institution Transfer Execution
210	Notice to Receive
900	Confirmation of Debit
910	Confirmation of Credit
920	Request message
941	Balance Report
942	Interim Transaction Report

*** End of Document ***