SWIFT Certified Applications

RTGS

Technical validation Guide 2019

Version 1

February 2019

Legal notices

Table of Contents

1 Preface

1.1 Introduction

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

SWIFT has engaged with Wipro (referred hereinafter as the “Validation Service Provider”) for performing the Technical Validation of the products applying for a SWIFT Certified Application.

1.2 Purpose and Scope

SWIFT Certified Application RTGS 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 RTGS is defined in the SWIFT Certified Application RTGS label Criteria 2019

This document focuses on the approach that a vendor application must follow to complete the technical validation against the SWIFT Certified Application RTGS criteria.

In this document a distinction is made between a **New Application** (vendors who apply for the label for the first time for a specific product release) and an **Application Renewal** (for product releases that already received the SWIFT Certified Application label in the past).

1.3 Target Audience

The target audience for this document is application vendors considering the certification of their business application for the SWIFT Certified Application RTGS label. The audience must be familiar with the SWIFT portfolio from a technical and a business perspective.

1.4 Related Documents

1. SWIFT Certified Application Programme Overview provides a synopsis of SWIFT Certified Application programme including the benefits to join for application vendors. It also explains the SWIFT Certified Application validation process, including the technical, functional and customer validation.
2. SWIFT Certified Application RTGS label criteria provides an overview of the criteria that a RTGS application must comply with to obtain the SWIFT Certified Application
3. User Handbook: www.swift.com > Support > Resources > Documentation
4. ISO 20022 for High-Value Payments
5. ISO 20022 Harmonisation Charter for Market Infrastructures

2 Technical Validation Process

In this document, a distinction is made between new SWIFT Certified Applications and label renewal applications 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 remaining label criteria are subjected to validation during the functional validation.

The following matrix explains 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 Label	Comprehensive	✓	✓	✓	✓
Renewal Label	Delta	✓	✓	✓	X

New Applicants will go through a complete technical validation against the criteria laid down in the SWIFT Certified Application RTGS criteria document.

For label renewal, any upgraded versions of applications will be subject to comprehensive testing.

The criteria that are verified include:

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

Validation Test Bed

The vendor will need to set up and maintain 'a SWIFT test lab' to develop the required adaptors needed for validation and to perform the qualification tests. The SWIFT lab will include the Alliance Access Interface as the direct connectivity to the Integration Test bed (ITB) (including SWIFTNet Link, VPN Box, RMA security, and HSM box) and the subscription to the InterAct and FileAct messaging services.

The installation and on-going maintenance of this SWIFT lab using a direct ITB connectivity is a pre-requirement for connectivity testing. However, as an alternative for the vendor to connect directly to the SWIFT ITB, the Validation Service provider (VSP) can provide a 'testing as a service' to integrate financial applications with SWIFT Interfaces via a remote Alliance Access over the SWIFT Integrated Test Bed (ITB) at VSP premises. Additional details can be obtained from the Wipro Testing Services – User Guide. (This is a payable optional service, not included in the standard SWIFT Certified Application subscription fee)

2.1 Integration with Alliance Interfaces

Requirement: The vendor will demonstrate the capability of the product to integrate with SWIFT Alliance Interfaces. When integrating with Alliance Access, support for Release 7.2 or higher is mandated for SWIFT Certified Application Label in 2019.

Note: Vendor must exchange test messages using AFT or MQHA or SOAP.

SWIFT will only publish information for which evidences have been provided during the technical validation. In case the vendor application supports several of the above adapters, the vendor is required to provide the appropriate evidences for all of them.

2.1.1 Direct Connectivity

Alliance Access 7.2 or higher is the preferred choice for connectivity.The table below specifies the adaptors and formats that will be tested for the technical validation.

Label Type	Alliance Access 7.2 or higher	
	Adaptor	Format
New and Renewal	AFT	RJE or XML v2
	MQHA	RJE or XML v2
	SOAP	XML v2

The vendor needs to successfully connect to and exchange test messages with the Integration Test Bed (ITB). Vendors can make use of the testing services provided by the Validation Service Provider to connect to the ITB. For more information, refer to Wipro Testing Services – User Guide.

The vendor must demonstrate the capability of their product to support FIN, InterAct and its associated features (example: message validation).

2.1.1.1 Alliance Access Integration

Requirement: The Applicant will demonstrate the capability of the product to integrate with SWIFT Alliance Interfaces.
The vendor should demonstrate the capability of the product to integrate with the Alliance Access with one of the following adaptors:

a. Automated File Transfer mode (AFT)
b. Web Sphere MQ Host Adaptor (MQHA)
c. SOAP Host Adaptor (SOAPHA)

The vendor must connect to the SWIFT ITB and receive SWIFT network ACK / NAK notifications and delivery notifications.

The Technical Validation documents for the AFT, MQHA and SOAPHA adaptors are available separately on swift.com (Partner section).

Notes for vendors having ITB connectivity:

- The vendor must inform SWIFT and the Validation Service provider before starting the test execution through ITB.
- The testing on ITB can start any time before the validation window allocated 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 the following test messages supported by their application as outgoing from their application
  - Total of 20 outbound test messages comprising a mix of MT1xx, MT2xx, MT9xx and MTn9x .
  - 9 MX Messages in InterAct comprising of pacs.004.001.08, pacs.008.001.07, pacs.009.001.07, pacs.010.001.02,camt.029.001.08,camt.052.001.07,camt.053.001.07,camt.054.001.07, xsys.001
- The test messages must be compliant to Standards Release 2019.
- The vendor must request for delivery notification.
- The vendor application must exchange:
  - FIN messages using Alliance Access RJE or XML v2 format
  - MX messages using InterAct
- 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 Access. The receiver destination of messages must be the same PIC or simply stated messages should be sent to own vendor PIC.
- The vendor must connect to the SWIFT ITB, send messages, receive SWIFT ACK/NAK, Delivery Notification and properly reconcile them by updating the status of sent messages.

- The vendor must inform SWIFT 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 Vendor not having ITB connectivity

The vendor must note the following for testing through Wipro Testing Service:

- The vendor must contact the Validation Service provider and agree on the terms for exchanging test messages using their testing service.
- The Validation Service provider will assign a branch PIC. This PIC must be used for exchanging test messages i.e. the sender and receiver PIC must be the PIC provided the Validation Service provider.
- The Validation Service provider will configure vendor profiles in their environment and inform the vendor about their access credentials. This service will be available for an agreed period for testing the connectivity and exchanging test messages. The entire testing on the ITB must be completed within the time window allotted to the vendor.
- The vendor must generate the following test messages supported by their application as outgoing from their application:
  - Total of 20 outbound test messages comprising a mix of MT1xx, MT2xx, MT9xx and MTn9x.
  - 9 MX Messages in InterAct comprising of pacs.004.001.08, pacs.008.001.07, pacs.009.001.07, pacs.010.001.02,camt.029.001.08,camt.052.001.07,camt.053.001.07,camt.054.001.07, xsys.001.
- These test messages must be compliant to Standards Release 2019.
- The vendor must request for delivery notification.
- The messages must be exchanged in the following formats:
  - FIN messages using Alliance Access RJE or XML v2 format
  - MX messages using InterAct
- The vendor must connect to SWIFT ITB, send messages, receive SWIFT ACK/NAK, Delivery Notification and properly reconcile them by updating the status of sent messages

The vendor must inform SWIFT 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.

2.1.2 Confirmation of Test Execution & Evidence Documents

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

- A copy of the MT test messages in RJE / XML v2 format generated by the business application.
- A copy of the MX test messages in XML v2 format for InterAct.
- Application log / Screenshots evidencing the:
  - processing of SWIFT messages
  - reconciliation of delivery notifications and Acknowledgements
- Event Journal Report and Message File from Alliance Access spanning the test execution window.
- Message Partner Configuration details.

Note: When connected through the Validation Service provider testing services, the Alliance Access logs (Event Journal Report, Message File and Message Partner configuration) will be generated by the Validation Service Provider.

2.1.3 Verification of the Test Results

In order to build 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
- Test messages have been exchanged by the vendor over ITB
- Test messages adhere to the SWIFT format requirement (RJE /XML v2 formats)
- Application is able to reconcile technical messages

2.1.4 Qualification Criteria Verified

Sl. No	SWIFT Certified Application Qualification Criteria Section Ref Number	label Requirement	Pass / Fail Status
1.	3.4	Alliance Access Integration Support-Release 7.2 or higher	
2.		Alliance Access Integration – AFT / MQHA / SOAP Support	
3.		Alliance Access Integration – RJE / XML v2 Format	
4.		Alliance Access Integration– InterAct Support	
5.	3.5	SWIFT MT and MX standard Support	
6.	3.7	Message Validation Standards Release 2019	
7.		Network Validation Rules (MFVR)	

2.2 Message Validation and FIN Standards Support

The vendor must demonstrate the application's capabilities to support SR2019, the Message Format Validation Rules (MFVR), MT Usage Guidelines and STP Guidelines.

2.2.1 Testing of Incoming Messages

- The Validation Service provider will send a set of valid inbound MT test messages that need to be uploaded and processed.
- The test messages will include the message types flagged as mandatory under section "**3.5 Standards**" of the SWIFT Certified Application RTGS criteria 2019 document.
- The application must perform the business validations while parsing the incoming messages.
- 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 / customise to their application needs. For ease of customisation, the test messages will be sent in a spread sheet 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**_RTGSMTValidation.xls, where "**yy**" will represent the Year of the Standards Release. For example, for a file containing MT103 and MT103+ for Standards Release 2019, the file name will be **"SR19_RTGSMTValidation.xls"**
- The Validation Service provider will provide an MT Test Result Summary file in excel spread sheet format that the vendor should use to capture test results. The file name will be **xxxx**_SR**nn**_RTGSMTValidation_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 above mentioned 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.

2.2.2 Confirmation of Test Execution and Evidence Documents

The vendor must send the following test evidences by email 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 spread sheet 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				

2.2.3 Verification of the Test Results

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

2.2.4 Testing of 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 2019
- STP Guidelines listed in SR 2019

Generating SWIFT Messages

- The New vendor must generate at least one test message for each of the message types flagged as mandatory under section "**3.5 Standards**" of the SWIFT Certified Application RTGS criteria 2019 document. 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 2019.
- The vendor application must wrap the SWIFT messages using RJE or XML v2 format.

2.2.5 Confirmation of Test Execution and Evidence Documents

After successful exchange of the test Messages the vendor must send by email the following test evidence 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.

2.2.6 Verification of the Test Results

The Validation Service provider will review the log files, the screenshots produced by the vendor to ascertain that all the messages are processed by the application and analyse the test result to build the scorecard and recommendation.

2.2.7 Qualification Criteria Verified:

Sl. No	SWIFT Certified Application Qualification Criteria		Pass / Fail Status
	Section Ref Number	Label Requirement	
8.	3.5	Standards (Support for Incoming Message)	
9.	3.5	Standards (Support for Outgoing Message)	
10.	3.7	Message Validation	
11.		Standards Release 2019	
12.		Network Validated Rules	
13.		MT Usage Rules	
14.		STP Guidelines	

2.3 Message Validation and MX Standards Support

Requirement: The purpose of these test messages is to test the application's capabilities to support XML Document Validation (Schema Validation, Extended Validation and Error Codes), MX Rule Books and SWIFTNet InterAct Real-time and store-and-forward mode.

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

- Schema Validation (well-formed XML and valid schema).
- MX Validation (extended validation and generic error code).
- MX Rule Book Validation (Refer to Solutions Service Description document in the UHB section of swift.com).
- Support of the MX pacs, camt, xsys messages.

For additional information on XML Document validation, vendor may please refer to SWIFT Standards MX – General Information and ISO 20022 Harmonisation Charter for Market Infrastructures documents.

2.3.1 Testing of Incoming Messages

The Validation Service provider will send a set of 10 MX test messages consisting of pacs.004.001.08, pacs.008.001.07,pacs.009.001.07,pacs.010.001.02,camt.029.001.08,camt.056.001.07,camt.060.001.03.

File Naming Convention

- The files will bear the name as SR**yy**_RTGS_**nnn**.XML, where "**yy**" will represent the Year of Standards Release and "**nnn**" will mean the test message sequence number. For eg. for a file containing test message for RTGS - Standards Release 2019 with sequence number 001, the file name will be "**SR19_RTGS001.XML**"
- The Validation Service provider will also send a MX Test Result Summary file in excel spread sheet format for capturing the test result from the vendor. The file name will be **xxxx_yy**_MX_RTGS_Test_Result.xls, where "**xxxx**" represents the vendor Name and "**yy**" represents the year of Standards Release.
- One file will contain one test message.

Processing of SWIFT MX Message Categories

The vendor must input the above mentioned 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.

2.3.2 Confirmation of Test Execution & Evidence Documents

The vendor must send the following test evidences by email 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 MX Test Result Summary file, updated with the test results (Error Code and Error Line Number).

A sample of the spread sheet is provided here below:

Sl. No.	Message ID	Business Validation Results	Error Line Number	Error Description	Expected Error Code	Expected Error Line Number	Pass/ Fail Status
1	pacs.004.001.08	Pass	-				
2	pacs.008.001.07	Error	11	Invalid Beneficiary Account			

- The vendor must send the updated MX Test Result Summary file to the Validation Service provider by email.
- In addition the vendor must also send the screenshots / log file by email to the Validation Service provider, as a sample evidence for having processed the test messages through the vendor application.

2.3.3 Verification of the Test Results

The Validation Service provider will review the log files, the screenshots produced by the vendor to ascertain that all the messages are processed by the application and analyse the test result to build the scorecard and recommendation.

2.3.4 Testing of Outgoing Messages

- The vendor must generate test messages for pacs.004.001.08, pacs.008.001.07, pacs.009.001.07, pacs.010.001.02,camt.029.001.08, camt.052.001.07, camt.053.001.07, camt.054.001.07, xsys.001 through their business application and as outbound ("application to Alliance Access") messages.
- The test messages must be compliant to MX validation (Schema and Extended Validation) and Rulebook compliance.
- The vendor application must exchange the SWIFT messages using XML v2 format.

2.3.5 Confirmation of Test Execution and Evidence Documents

The vendor must send the following test evidences by email 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.
- A copy of the MX test messages in XML v2 format generated by the business application.
- One file should contain a single MX message only.

2.3.6 Verification of the Test Results

The Validation Service provider will review the log files, messages generated and the screenshots produced by the vendor to ascertain that all the messages are processed by the application and analyse the test result to build the scorecard and recommendation.

2.3.7 Qualification Criteria Verified

Sl. No	SWIFT Certified Application Qualification Criteria		Pass / Fail Status
	Section Ref Number	label Requirement	
15.	3.5	Standards	
16.	3.7	Message Validation (Rule Book Compliance for MX)	

2.4 Testing of Reference Data

Requirement: The vendor must demonstrate the application's capability to validate messages against the BIC, Bank Directory Plus and IBAN Plus directories. The vendor must use the sample BIC Directory, Bank Directory Plus and IBAN Plus available on http://swiftref.swift.com/resource-category/products

Testing for BIC, Bank Directory Plus and IBAN Plus Validation

The test scenario for testing the BIC, Bank Directory Plus and IBAN Plus are provided in the swiftref Test scenario document.

- The test scenarios to be executed in the vendor application will cover:
  - BIC Validation
  - IBAN Structure validation
  - Deriving BIC / Clearing code

The test data and sample directory for testing the BIC, Bank Directory Plus and IBAN Plus table look-up and validation will be provided to the application vendor before the start 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.

Reference Data Validation

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.

2.4.1 Confirmation of Test Execution and Evidence Documents

After successful execution of the test scenario for BIC, Bank Directory Plus and IBAN Plus reference data validation, the vendor must send the following test evidences to the Validation Service provider by email:

- Sample evidence demonstrating that the application has processed the BIC, Bank Directory Plus and IBAN Plus 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.

2.4.2 Verification of the Test Results

The Validation Service provider will validate the vendor output against the expected results and analyse the test result to build the scorecard recommendation.

2.4.3 Qualification Criteria Verified

Sl. No	SWIFT Certified Application Qualification Criteria		Pass / Fail Status
	Section Ref Number	Label Requirement	
17	4.1	BIC Directory	
18	4.2	Bank Directory Plus	
19	4.3	IBAN Plus	

3 Summary of Technical Validation

Validation Activity		Label NEW	Label RENEWAL
Message Validation	Outgoing	**MT Messages**: All mandatory MTs as per table in label Criteria document MT103 103+, 200,202, 202 COV, 204, 900, 910, 940, 941, 942, 950, n91, n96, n98, n99, 97 **MX Messages:**pacs.004.001.08, pacs.008.001.07, pacs.009.001.07, pacs.010.001.02, Camt.029.001.08, camt.052.001.07, camt.053.001.07, camt.054.001.07, xsys.001	n99
	Incoming	**MT Messages**: All mandatory MTs as per table in Label Criteria document MT103 103+, 200,202, 202 COV, 204, 940, n91, n92, n95, n98, n99, 96 only valid scenarios will be tested **MX Messages**: pacs.004.001.08, pacs.008.001.07, pacs.009.001.07, pacs.010.001.02, camt.056.001.07, camt.029.001.08, camt.060.001.03	n92,n99
Standards	Standards Release	SR2019	
	Market Practice	HVPS Global Market Practice, ISO 20022 Harmonisation Charter for Market Infrastructures	
	Optional Messages	Verified only on specific request by the vendor	
Connectivity	Alliance Access 7.2 or higher	FIN → AFT or MQHA or SOAPHA	
	Message Format	RJE or XML v2	
Reference Data Directory	BIC, Bank Directory Plus and IBAN Plus	Scenario Based Testing	
	Integration	Screenshot Verification	

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