SWIFT Certified Applications

Securities Settlement

Technical validation Guide 2019

Version 1

February- 2019

Legal notices

Table of Contents

1 Preface 4
1.1 Introduction 4
1.2 Purpose and Scope 4
1.3 Target Audience 4
1.4 Related Documents 4

2 Technical Validation Process 5
2.1 Integration with Alliance Interfaces 5
2.1.1 Direct Connectivity 5
2.1.2 Confirmation of Test Execution and Evidence Documents 7
2.1.3 Verification of the Test Results 7
2.1.4 Qualification Criteria Verified 8
2.2 Message Validation and Standards Support 8
2.2.1 Testing of Incoming Messages 8
2.2.2 Confirmation of Test Execution and Evidence Documents 9
2.2.3 Verification of the Test Results 9
2.2.4 Testing Outgoing Messages 9
2.2.5 Confirmation of Test Execution and Evidence Documents 10
2.2.6 Verification of the Test Results 10
2.2.7 Qualification Criteria Verified 10

3 Summary of Technical Validation 10

4. FAQ 11

1 Preface

1.1 Introduction

SWIFT initiated the SWIFT Certified Application programme to persuade application vendors to offer 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 here after as the “Validation Service Provider”) for performing the technical validation of the products applying for a SWIFT Certified Application.

1.2 Purpose and Scope

The certification for the SWIFT Certified Application Securities Settlement 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 SWIFT Certified Application Securities Settlement 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 Securities Settlement criteria.

In this document a distinction is made between a **New Application** (vendors who apply for the certification 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 SWIFT Certified Application Securities Settlement Label. The audience must be familiar with SWIFT from a technical and a business perspective.

1.4 Related Documents

1) The SWIFT Certified Application Programme Overview provides a synopsis of the 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) The SWIFT Certified Application for Securities Settlement label criteria provides an overview of the criteria that a Securities Settlement application must comply with to be granted the SWIFT Certified Application.

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 2019:

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

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 FIN 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 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, Release 7.2 or higher support is mandated for the SWIFT Certified Application in 2019.

Note: New label applicant vendors and vendors renewing their label application 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. The vendor is required to perform the connectivity testing with any one of the adaptors mentioned below.

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 the FIN protocol and its associated features (example: message validation).

2.1.1.1 Alliance Access Integration

- Testing for connectivity to Alliance Access Interface will be verified on the SWIFT Integration Test Bed (ITB) using Alliance Access Release 7.2 or higher.
- The vendor should demonstrate the capability of the product to integrate with the Alliance Access with one of the following adaptors:
  - Automated File Transfer mode (AFT)
  - Web Sphere MQ Host Adaptor (MQHA)
  - 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 application should generate the following outbound test messages
  - Applications targeting intermediaries (Account Servicers), must generate 24 test messages (two test messages each for MT 535, 536, 540, 541, 542, 543, 544, 545, 546, 547, 548 and MT 578 - 586)
  - Applications targeting non-intermediaries (Account owners) must generate 20 test messages (five test messages each for MT 540, 541, 542, 543, 548 and MT 578 - 586)
- The test messages must be compliant to Standards Release 2019
- The vendor must request for delivery notification
- The vendor application must exchange the SWIFT messages using Alliance Access RJE or XML v2 format
- 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 SWIFT ITB, send MT 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 though application event logs, transmitted messages and ACK / NAK received messages.

Notes for vendors 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 application should generate the following outbound test messages
  - Applications targeting intermediaries (Account Servicers), must generate 24 test messages (two test messages each for MT 535, 536, 540, 541, 542, 543, 544, 545, 546, 547, 548 and MT 578 - 586)
  - Applications targeting non-intermediaries (Account owners) must generate 20 test messages (five test messages each for MT 540, 541, 542, 543, 548 and MT 578 - 586)
- The test messages must be compliant to Standards Release 2019
- The vendor must request for delivery notification
- The vendor application must exchange the SWIFT messages using Alliance Access RJE or XML v2 format
- The vendor must connect to SWIFT ITB, send MT 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 though application event logs, transmitted messages and ACK / NAK received messages.

2.1.2 Confirmation of Test Execution and 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
- Application log / Screenshots evidencing the
  - processing of SWIFT messages
  - reconciliation of delivery notifications and Acknowledgements
- Alliance Access Event Journal Report and Message File 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 issue the scorecard and necessary recommendation, the Validation Service provider will review 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 (RJE and /or XML v2 formats).
- Application is able to reconcile technical messages

2.1.4 Qualification Criteria Verified

Sl. No	SWIFT Certified Application Qualification Criteria		Pass / Fail Status
	Section Ref Number	Label Requirement	
1.	3.4	Alliance Access Integration – AFT / MQHA /SOAPHA	
2.		Alliance Access Integration Support – Release 7.2 or higher	
3.		Alliance Access Integration – RJE / XML v2 Format	
4.	3.5	Standards Support	
5.	3.6	Standards Release	
6.	3.6	Message Format Validation Rules (MFVR)	

2.2 Message Validation and Standards Support

Requirement: The vendor must demonstrate the application's capability to support FIN messages, the rules and guidelines set out in MFVR for SR 2019.

Note: The Message Validation and Standards Support are applicable for both New and Renewal label applicants.

2.2.1 Testing of Incoming Messages

The Validation Service provider will send a set of 10 valid MT test messages that should be uploaded and processed in the application. These test messages will cover MT 535-536, MT 540-548 and MT 578-586. Since the message types supported depends on the target customer implementation, the Validation Service provider will send the test messages as defined below:

Target Customer Implementation	Message Types	Test Message Direction
Account Servicers	MT 535 – 536, 540 – 548, 578 – 586	Inward to the application
Account Owners	MT 535, 544 – 548, 578 - 586	

- The vendor must inform SWIFT and the Validation Service provider about the choice of customer implementation beforehand.
- All test messages will be "inward to the application" direction
- The test messages will cover the key fields that undergone changes in SR 2019
- The application must process SR 2019 impacted incoming messages
- 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 / 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 as SRyy_SecsSettMTValidation.xls, where "**yy**" will represent the Year of the Standards Release. For example, for a file containing test messages for Standards Release 2019, the file name will be "**SR19_SecsSettMTValidation.xls**"
- The Validation Service provider will also send an MT Test Result Summary file in excel spread sheet format for the vendor to capture the test results. The file name will be **xxxx**_SR**nn**_SecsSettMT_Validation_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.

2.2.2 Confirmation of Test Execution and Evidence Documents

The vendor should 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. 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	54010000001	Pass	-				
2	54110000002	Error	11				

2.2.3 Verification of the Test Results

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

2.2.4 Testing Outgoing Messages

The vendor application should generate 50 outbound test messages as defined below. The test messages must be the one that is supported by their application with reference to their target client implementation.

Target Customer Implementation	Message Types	Test Message Direction
Account Servicers	MT 535 – 536, 540 – 548, 578 - 586	Outward from the application
Account Owners	MT 540 – 543, 548, 578 - 586	

- The test messages must contain the key fields that undergone changes in SR 2019. The Validation Service provider will provide the list of key fields before the technical validation window.
- The vendor application must wrap the SWIFT messages using RJE or XML v2 format

2.2.5 Confirmation of Test Execution and Evidence Documents

The vendor should send the following test evidences by email to the Validation Service provider:

- Screenshots and Log Files from application evidencing generation SWIFT messages
- A copy of the MT test messages in RJE / XML v2 format generated by the business application
- List of fields that have undergone changes which are covered in the messages generated

2.2.6 Verification of the Test Results

The Validation Service provider will review the messages generated, log files, the screenshots produced by the vendor to ascertain that all 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	
1.	3.5	Standards Support for Messaging Services	
2.	3.6	Standards Release	
3.	3.6	Message Format Validation Rules (MFVR)	

3 Summary of Technical Validation

Validation Activity		Label NEW	Label RENEWAL
Message Validation	Outgoing	Account Servicers: MT 535,536, 540,541,542,543,544,545, 546,547,548, 578,586 Account Owners: MT 540,541,542,543,548, 578,586	AccountServicers:MT535,536, 540,541,542,543,544,545,546,547, 548, 578,586 Account Owners: MT 540,541,542,543,548, 578,586
	Incoming	Account Servicers: MT 535,536,540,541,542,543, 544,545,546,547,548,578, 586 Account Owners: MT 535, 544,545,546,547,548, 578,586	Account Servicers: MT 535,536, 540,541,542,543,544,545,546,547, 548,578,586 Account Owners: MT 535, 544,545,546,547,548, 578,586
Standards	Standards Release	SR 2019	
		Incoming Messages are tested only for positive instances	
	Rule Book Ref	Not Applicable	
	Optional Messages	Verified only on specific request by the vendor	
Connectivity	Alliance Access 7.2 or higher	AFT or MQHA or SOAPHA	

	Message Format	RJE and / or XML v2

4. FAQ

1 Will the MT test messages provided for technical validation contains the header blocks as well or only text block [Block 4] of the message?

MT test messages will contain the Blocks from 1 to 4.

2 What exactly should we populate Error Code in MT Test Result Summary file?

The business application must perform business validation only, since the test messages sent by the Validation Service provider will be a correct message that complies with MFVR.

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