SWIFT Certified Applications

Collateral Management

Technical validation Guide 2018

Version 1.1

February 2018

Legal notices

Table of Contents

1 Preface

1.1 Introduction

SWIFT initiated the SWIFT Certified Application label programme to help application vendors into offering products that are compliant with the business and technical requirements of the financial industry. SWIFT Certified Application labels 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 Label.

1.2 Purpose and Scope

The certification for the SWIFT Certified Application Collateral Management 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 Collateral Management Label Criteria 2018.

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

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 Collateral Management Label. The audience is expected to 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 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 Collateral Management label criteria provide an overview of the criteria that a Collateral Management application must comply with to be granted with the SWIFT Certified Application label
3) Message Reference Guide for Collateral Management 2.0
4) Collateral Management 2.0 Service Description
5) ISDA Collateral Roadmap-Electronic Messaging, as reference to the market practices and message usage guidelines in the area of OTC derivatives.

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	✓	✓	✓	✓
Label Renewal	Delta Only	✓	✓	✓	X

New applicants will go through a technical validation against the criteria laid down in the SWIFT Certified Application Collateral Management Criteria document.

The criteria that are verified include:

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

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, 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 is mandated for the SWIFT Certified Application Label in 2018.

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 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	
	Adaptor	Format
New and Renewal	AFT or MQHA or SOAPHA	XML v2/RJE

Note: Bilateral: FIN, FileAct and InterAct support are mandatory for SWIFT Certified Application Label accreditation. This compliance will be verified during Functional Validation.

Triparty: FIN and FileAct are mandatory for SWIFT Certified Application Label accreditation. This compliance will be verified during Functional Validation.

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 MT/MX 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.
- The vendor should demonstrate the capability of the product to integrate with the Alliance Access with any 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 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).

In Summary

Messaging service	Standards	Interface	Mandatory adapter
FIN	MT	Alliance Access 7.2	AFT or MQHA or SOAP
FileAct SF (store-and-forward)	Any	Alliance Access 7.2	AFT or MQHA or SOAP
InterAct(store-and-forward)	Any	Alliance Access 7.2	AFT or MQHA or SOAP

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.
- For Bilateral Collateral management vendor should generate and exchange:
    1. Two sets of MX Messages for the following 3 request types as Input Message to SWIFT
        - colr.003.001.03 – MarginCallRequest
        - colr.005.001.03 – CollateralManagementCancellationRequest
        - colr.008.001.03 – CollateralProposalResponse
    2. Three Messages each for MT 540, 542, 202 as Input Message to SWIFT
- For Triparty Collateral management vendor should generate and exchange the following request types as Input Message to SWIFT
    - Three messages each for MT 527,558 and 569
- The test messages must be compliant to Standards Release 2018
- The vendor must request for delivery notification
- The vendor application must exchange the SWIFT messages using Alliance Access in XML v2/RJE 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.
- When the testing is performed on ITB, the service name **swift.colr!x** 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 Collateral Management business message. The vendor must connect to SWIFT ITB, send MT/MX 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.
- For Bilateral Collateral management vendor should generate and exchange:
    1. Two sets of MX Messages for the following 3 request types as Input Message to SWIFT
        - colr.003.001.03 – MarginCallRequest
        - colr.005.001.03 – CollateralManagementCancellationRequest
        - colr.008.001.03 – CollateralProposalResponse
    2. Three Messages each for MT 540, 542, 202 as Input Message to SWIFT
- For Triparty Collateral management vendor should generate and exchange the following request types as Input Message to SWIFT
    - Three messages each for MT 527,558 and 569
- The vendor must request for delivery notification
- The vendor application must exchange the SWIFT messages using Alliance Access in XML v2/RJE format

- When the testing is performed on ITB, the service name **swift.colr!x** 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 Collateral Management business message. The vendor must connect to SWIFT ITB, send MX and 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 & Evidence Documents

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

- Copy of the MT test messages in RJE / XML v2 format generated by the business application
- Copy of the parameter file and business payload data for FileAct file
- 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

The Validation Service provider will review the log files, event journal, the screenshots produced by the vendor to ascertain that:

- All the messages are positively acknowledged by the SWIFT Network by reviewing the log files
- The Alliance Access messaging interface header is present
- The application header adheres to the schema definition
- The messages are compliant with the standards release requested in the label criteria document
- Application is able to reconcile technical messages

The test results will be analysed to build the scorecard and recommendation

2.1.4 Qualification Criteria Verified

Sl. No	SWIFT Certified Application Label Qualification Criteria		Pass / Fail Status
	Section Ref Number	Label Requirement	
1.	3.4	Alliance Access Integration – AFT / MQHA/SOAPHA	
2.		Alliance Integration – Alliance Access Header Info / XML v2/RJE	
3.	3.5	Messaging Services support – FIN/InterAct/FileAct	
4.	3.3	Standards Support for Outgoing Request Types	

2.2 Message Validation and Standards Support

Requirement: The vendor must demonstrate the application's capability to support MT/MX messaging standards, Collateral Management rulebook compliance. (Please refer to ISDA Collateral Roadmap - Electronic Messaging published by the Collateral Committee (Standards for the Electronic Exchange of OTC Derivative Margin Calls) of ISDA for market practices and message usage guidelines for rulebook compliance)

The vendor must demonstrate the capability of their product to process (generate and respond to) Collateral Management MT/MX messages exchanged between two participants (Collateral Taker and Collateral Giver) for incoming and outgoing workflow.

Technical validation of business workflow will be tested for all the mandatory requirement for Collateral Management events.

The vendor must capture the business payload and transform them into MT/MX message, validate the same against the SWIFT standards and rulebook. The application must add the Alliance Access header information in XML v2 format before transmitting to Alliance Access.

For Bilateral Collateral management, the vendor must create two instances of application one as "collateral giver" and the other as "collateral taker

Collateral Management Event 1: Margin Call Process

Application emulating as Collateral Taker	Application emulating as Collateral Giver
• Correctly generate, batch, and transmit - colr.003 – Margin Call Request transactions - colr.008 – Collateral Proposal Response - colr.005 – Collateral Management Cancellation Request - colr.009 – Collateral Call Dispute Notification	• Receive and process correctly formatted - colr.003 – Margin Call Request transactions - colr.008 – Collateral Proposal Response - colr.005 – Collateral Management Cancellation Request - colr.009 – Collateral Call Dispute Notification
• Receive and process correctly formatted - colr.004 – Margin Call Response messages - colr.007 – Collateral Proposal - colr.005 – Collateral Management Cancellation Request - colr.009 – Collateral Call Dispute Notification	• Correctly generate, batch, and transmit - colr.004 – Margin Call Response messages - colr.007 – Collateral Proposal - colr.005 – Collateral Management Cancellation Request - colr.009 – Collateral Call Dispute Notification
• Reject or accept collateral proposals, acknowledge dispute notifications and send appropriate messages	• Accept, reject or dispute margin call requests initiate collateral proposals, acknowledge dispute notifications and send appropriate messages

Collateral Management Event 2: Substitution Processing

Application emulating as Collateral Taker	Application emulating as Collateral Giver
• Receive and process correctly formatted - colr.010 – Collateral Substitution Request - colr.012 – Collateral Substitution Confirmation - colr.005 – Collateral Management Cancellation Request - colr.006 – Collateral Management Cancellation Status	• Correctly generate, batch, and transmit - colr.010 – Collateral Substitution Request - colr.012 – Collateral Substitution Confirmation - colr.005 – Collateral Management Cancellation Request - colr.006 – Collateral Management Cancellation Status
• Correctly generate, batch, and transmit	• Receive and process correctly formatted

- colr.011 – Collateral Substitution Response - colr.005 – Collateral Management Cancellation Request - colr.006 –Collateral Management Cancellation Status •Accept, reject Collateral Substitution Request initiate Collateral Substitution Response, acknowledge cancellation requests, cancellation status and send appropriate messages	- colr.011 – Collateral Substitution Response - colr.005 – Collateral Management Cancellation Request - colr.006 –Collateral Management Cancellation Status •Reject or accept Collateral Substitution Response, acknowledge cancellation requests, cancellation status and send appropriate messages

Collateral Management Event 3: Interest Payment Process

Application emulating as Collateral Taker	Application emulating as Collateral Giver
•Receive and process correctly formatted - colr.013 – Interest Payment Request - colr.015 – Interest Payment Statement •Correctly generate, batch, and transmit - colr.014 – Interest Payment Response •Reject or accept Interest Payment Request , acknowledge Interest Payment Statement and send appropriate messages	•Correctly generate, batch, and transmit - colr.013 – Interest Payment Request - colr.015 – Interest Payment Statement •Receive and process correctly formatted - colr.014 – Interest Payment Response •Accept, reject Interest Payment Response and send appropriate messages

The application/middleware should be able to generate the following messages.

Securities collateral	Receive free of payment	MT540
	Delivery free of payment	MT542
	Settlement Confirmation of receive free	MT544
	Settlement confirmation of delivery free	MT546
Cash collateral	Cash delivery instruction	MT202

For Triparty collateral management vendor must create two instances of the application for sending and receiving of test messages

Process	Message name	Message identifier
Instruction	Triparty Collateral Instruction	MT527
Processing	Triparty Collateral Status and Processing Advice	MT558
Reporting	Triparty Collateral and Exposure Statement	MT569

2.2.1 Test Scenarios Planning and Execution

The test message files must cover the end-to-end processing of margin call – issuance, response, notification of collateral to be moved and notification of dispute between two participants - collateral taker and collateral giver. For facilitating execution of business work flow testing, test scenarios are provided in a separate spreadsheet file.

- The vendor must create both outgoing and incoming test message scenarios
- The test message must adhere to the rules specified in the Rulebook and will be verified during technical validation

- The application should add the Alliance Access specific messaging interface header to the business payload. The business payload consists of the application header + the collateral management business message.

2.2.1 Confirmation of Test Execution and Evidence Documents

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

- Screenshots, Log Files, Reports from application evidencing processing and reconciliation of the SWIFT Messages exchanged
- A copy of the MT/MX test messages in RJE/XML v2 format generated by the business application

The vendor must update the spreadsheet detailing each executed test scenario with a brief description of the test case. All the minimum mandatory test type requirements for technical validation should be at least covered by one or several test messages.

2.2.2 Verification of the Test Results

The Validation Service provider will verify the following while performing the technical validation:

- The Alliance Access messaging interface header is present
- The application header adheres to the schema definition
- Coverage of Scenarios
- Adherence to collateral management message reference guide and adherence to collateral management rulebook

The test results will be analysed to build the scorecard and recommendation

2.2.3 Qualification Criteria Verified

Sl. No	SWIFT Certified Application Label Qualification Criteria		Pass / Fail Status
	Section Ref Number	Label Requirement	
5.	3.6	Message Validation	
6.	3.7	Collateral Management Rulebook	
7.	3.8	Message Work Flow –Bilateral/Triparty collateral management	

3 Summary of Technical Validation

Validation Activity			Label NEW	Label RENEWAL
Message Validation	Bilateral	Collateral Giver/Collateral Taker	FIN MT-540,542,544,546,202	FIN MT-540,542,544,546,202
	Triparty	Collateral Giver/Collateral Taker	FIN MT-527,558,569	NA
Standards	Standards Release	SR 2018		
	Rule Book Ref	ISDA Collateral Roadmap - Electronic Messaging		
	Optional Messages	Verified only on specific request by the vendor		
Connectivity	Alliance Access 7.2	AFT or MQHA or SOAPHA		
	Message Format	XML v2/RJE		

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