SWIFT Certified Applications

Islamic Finance

Technical validation Guide 2018

Version 1.1

February 2018

Legal Notices

Copyright

SWIFT © 2018. 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, SWIFTNet and Accord. Other product, service, or company names in this publication are trade names, trademarks, or registered trademarks of their respective owners.

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 7
2.2 Message Validation and Standards Support 8
2.2.1 Testing scenarios 9
2.2.2 Verification of the Test Results 9

3 Summary of Technical Validation 10

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 provided 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 of the SWIFT Certified Application Islamic Finance 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 Islamic Finance is defined in the SWIFT Certified Application Islamic Finance label criteria 2018

This document focuses on the approach for the technical validation that a vendor application must follow to complete the technical validation against the SWIFT Certified Application Islamic Finance 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 Islamic Finance 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 Islamic Finance Label criteria provide an overview of the criteria that a Islamic Finance application must comply with to be granted the SWIFT Certified Application label

3) SWIFT Commodity Murabaha Message Usage Guidelines

2 Technical Validation Process

SWIFT Certified Application Islamic Finance Label should follow the below matrix for the year 2018. 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	✓	✓	✓	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 requirement for connectivity testing. .

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 of 2018.

Note: The connectivity testing is applicable for new label applicant vendors. New label applicant will demonstrate connectivity using AFT or MQHA or SOAPHA

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 for the vendor application that support the creation, processing and exchange of SWIFT messages for Murabaha and to be accredited with SWIFT Certified Application Label in 2018.

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	RJE or XML v2
	MQHA	RJE or XML v2
	SOAP	XML v2

The vendor application 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 application 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.
- The vendor should demonstrate the capability of the product to integrate with the Alliance Access with the 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)..

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 two messages each for MT 502, MT 509 MT 515, MT 579, MT 599, MT 300, MT 320 and MT620
- The test messages must be compliant to Standards Release 2018 and the message usage guidelines specified in SWIFT Commodity Murabaha Message Usage Guidelines
- 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 application 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 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 two messages each for MT 502, MT 509 MT 515, MT 579, MT 599, MT 300, MT 320, and MT620.These test messages must be compliant to Standards

Release 2018 and the message usage guidelines specified in SWIFT Commodity Murabaha Message Usage Guidelines
- 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 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 build 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 Label 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	
3.		Alliance Access Integration – RJE / XML v2 Format	
4.	3.5	Standards Support for Outgoing Messages	
5.	3.7	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 2018 and the usage guidelines specified in SWIFT Commodity Murabaha Message Usage Guidelines.

The vendor application should generate process and exchange SWIFT messages for Murabaha as described in SWIFT Commodity Murabaha Message Usage Guidelines document.

In particular, for validating the business workflows, the compliance to the following usage guidelines will be verified.

Message Usage Guidelines

Commodity Murabaha message usage guidelines

- **SR 2018 Compliance** – Ability of the application to exchange (send and receive) MT 502, MT 509, MT 515, MT 579 and MT 599 for **Murabaha solution and MT 300,MT320,MT620 for Islamic Finance rulebook solution** as per MFVR for Standards Release 2018
- **Message User Header** – Block 3 of the message header must contain the words MURABAHACA (for Murabaha Customer Acceptance) and MURABAHACP (for Murabaha Customer Placement) in the Message User Reference (MUR) field.
- **Master Transaction Reference** – Master Transaction reference must be repeated in the Linkages block of every message to refer all related messages to the original master agreement.
  - Field 20C must contain the Master Transaction reference with MAST as qualifier
  - First six characters of the BIC + YYMMDD + four digit sequential number is the recommended field structure for the Master Transaction reference
    - where **BIC** refers to BIC of the Islamic bank for the Customer Reference flow and BIC of the Customer for the Customer Placement flow
    - Date refers to the date of Master Agreement signed
    - Sequence number defines the transaction flow that is carried out under the master agreement umbrella
- **Commodity Identification** – Field 35B must be used to identify the commodity. Please refer to section 5.1 of SWIFT Commodity Murabaha Message Usage Guidelines document for the correct usage of commodity identification.
- **Commodity Units** –Financial Instrument Attribute (FIA) block is mandatory for Murabaha transactions. Please refer to section 5.2 of SWIFT Commodity Murabaha Message Usage Guidelines document for the correct usage of commodity units.
  - The commodity units must be specified in the Financial Instrument Attribute Narrative field
  - The foreseen list of commodity units provided in this section must be used
- **Message User Group** – The vendor needs to register to the Islamic Finance Message User Group (MUG) and the following information must be updated in the message header block and in the text block
  - The field 119 in Message User Header Block (Block 3) must be set to ISLFIN
  - A, instance of the A1 Linkages block must be added in all messages; with the common reference to "ISLFIN" (Field 20C – syntax :20C::COMM//ISLFIN)

  Registration to MUG is based on subscription and the vendor can use this link to subscribe
- **Usage of REPO block** – REPO block in FIN message is mandatory. The deferred payment date and price must be provided in this block.

Islamic Finance Rulebook message usage guidelines

- **Message User Group** – The vendor needs to register to the Islamic Finance Message User Group (MUG) and vendors can use this link to check specific rules for MT 300, MT 320 and MT 620 that are described in the SWIFT Messages for Islamic Finance Message Usage Guidelines document.

2.2.1 Testing scenarios

There are four participants in the Murabaha business flows:
- Customer – who approaches the bank to obtain finance or deposit money
- Bank – who executes the customer's orders
- Broker A – who buy and sell commodity from the market
- Broker B – who buy and sell commodity from the market

In these scenarios, customer can be another Bank or a financial institution. Broker A and Broker B could be a third party Bank with whom the commodity is bought or sold. Murabaha guidelines do not prevent buying and selling to the same Broker. I.e. Broker A and B can be one institution.

The vendor must set up its application as the **bank's application** and simulate messages received from other participants in the business flows

The following two main test scenarios have to be executed for the business flow testing:
- Customer Acceptance
- Customer Placement
- When a Murabaha trade consists of a basket of commodities, the details of the basket must be communicated through one separate or a series of separate messages (MT 579 – Certificate of Numbers). The MT 502, MT 509, MT 515 and MT 599 must refer to one basket unit of one basket commodity for the total amount. The details about the composition of commodities must be conveyed through single or multiple MT 579. The master transaction reference in Field 21 must be used to link the MT 579 with other messages in the flow.

For facilitating execution of business workflow testing, test scenarios are provided in a separate spreadsheet file.
- Label applicants must execute all the test scenarios specified therein
- The vendor must create both outgoing and incoming test message scenarios
- The test message must adhere to the MFVR guidelines, SR 2018 and the rules specified in the message usage guidelines
- The vendor application must exchange the SWIFT messages using RJE or XML v2 format

2.2.1.1 Confirmation of Test Execution and Evidence Documents

The vendor should send the following test evidences by email to the Validation Service provider:
- Screenshots, Log Files, Reports from application evidencing generation SWIFT messages
- A copy of the MT 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. The entire test scenario for technical validation provided in the test scenario document must be covered by one or several test messages.

2.2.2 Verification of the Test Results

The Validation Service provider will review the messages, log files; the screenshots produced by the vendor to ascertain that all messages are processed by the application and build the scorecard and recommendation. Qualification Criteria Verified

Sl. No	SWIFT Certified Application Label Qualification Criteria		Pass / Fail Status
	Section Ref Number	Label Requirement	
6.	3.5	Standards Support for Messaging Services	
7.	3.6	Message Reconciliation	
8.	3.7	Message Format Validation Rules (MFVR)	
9.	3.8	Business Workflows	

3 Summary of Technical Validation

Validation Activity		Label NEW
Message Validation [Business Workflow]	Outgoing	Messages required for the Murabaha solution: MT 502, 509, 515, 579 and 599
	Incoming	Messages required for the Islamic Finance rulebook solution: MT 300,320,620
Standards	Standards Release	SR 2018
	Rule Book Ref	Murabaha Message Usage Guidelines Islamic Finance Rulebook message usage guidelines
	Optional Messages	Verified only on specific request by the vendor
Connectivity	Alliance Access 7.2	AFT or MQHA or SOAPHA
	Message Format	RJE and / or XML v2

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