SWIFT Certified Applications

Corporate Treasury

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 6
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 of Outgoing Messages 9
2.2.5 Confirmation of Test Execution and Evidence Documents 9
2.2.6 Verification of the Test Results 9
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 help application vendors into offering products that are compliant with the business and technical requirements of the financial industry. SWIFT Certified Applications 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 of the SWIFT Certified Application for Corporates Treasury 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 for Corporates Treasury label criteria 2018.

This document focuses on the approach that a vendor application must follow to complete the technical validation certified against SWIFT Certified Application for Corporates Treasury 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 middleware suite / business application for the SWIFT Certified Application for Corporates Treasury 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 Corporates Treasury label criteria provide an overview of the criteria that corporates application must comply with to be granted with the SWIFT Certified Application label.
3) SWIFT for Corporates – Resource Centre
4) SWIFT for Corporates – SWIFT Standards MT Implementation Guide

2 Technical Validation Process

In this document, a distinction is made between new label 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 and connectivity to Alliance Interfaces. The remaining label criteria are subject to validation during the functional validation.

The following matrix explains the tests that have to be performed by the vendor application in 2018.

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

Both New Applicants and label renewal applicants will go through a technical validation against the criteria laid down in the SWIFT Certified Application Corporates Treasury Criteria document.

The criteria that are verified include:

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

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 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 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	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 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 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 vendor 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 fifteen test messages as outgoing from their application in the corporate-to-bank message flow
  - three each in MT 300
  - one each in MT 199, 999 and 399
- 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 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 vendor 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 fifteen test messages as outgoing from their application in the corporate-to-bank message flow
  - three each in MT 300
  - one each in MT 199, 999 and 399
- 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 RJE or XML v2 format
- The vendor must connect to the 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 verify 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 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 Support-Release 7.2	
2.		Alliance Access Integration – AFT / MQHA/SOAP Support	
3.		Alliance Access Integration – RJE / XML v2 Format	
4.	3.6	SWIFT MT Support	
5.		Standards Release	
6.		Network Validation Rules (MFVR)	

2.2 Message Validation and Standards Support

Requirement: The vendor must demonstrate the application's capability to support FIN messages and the rules and guidelines set out for SCORE.

Note: Testing for message validation and standards support is applicable for both New and Renewal label applicant vendors.

2.2.1 Testing of Incoming Messages

- The Validation Service provider will send a set of 20 MT test messages for new label applicant and 10 Test messages for renewal label applicant 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 MT 199, 940, 942, 999, 300, 320, 399
- All test messages will be "inward to the application" direction complying to Standards Release 2018
- 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 SR**yy**_TreasuryMTValidation.xls, where "**yy**" will represent the Year of the Standards Release. For example, for a file containing test messages for Standards Release 2018, the file name will be **"SR18_TreasuryMTValidation.xlsx"**
- The Validation Service provider will provide an MT Test Result Summary file in excel spread sheet format that the vendor should use to capture the test results. The file name will be **xxxx**_SR**nn**_MT_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 as inbound SWIFT messages and perform the business validations. For example, the application can reject a Foreign Exchange Confirmation message, if the value date is less than current date or trade date is a future 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	94010000001	Pass	-				
2	94210000002	Error	11				

2.2.3 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.

2.2.4 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 2018
- STP Guidelines listed in SR 2018

Generating SWIFT Messages

- The vendor must generate 5 test messages each for MT101, 210, 300, 320,399,199,999.
- 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 2018
- 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 the successful exchange of the test messages, 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 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	
7.	3.5	Standards (Support for Incoming Message)	
8.		Standards (Support for Outgoing Message)	
9.	3.6	Rule book Compliance	
10.		Standards Release Guide	
11.		Network Validated Rules	
12.		MT Usage Rules	
13.		STP Guidelines	

3 Summary of Technical Validation

Validation Activity		Label NEW	Label RENEWAL
Message Validation	Outgoing	FIN → MT 101, 199, 999, 210, 300, 320, 399	FIN → MT101,MT 210, MT 300,MT 320
	Incoming	FIN → MT 199, 940, 942, 999, 300, 320, 399	FIN → MT 300,320
Standards	SRG	SR2018	
	Rule Book Ref	SCORE Rule book	
	Optional Messages	Verified only on specific request by the vendor	
Connectivity	Alliance Access 7.2	FIN → AFT or MQHA or SOAPHA	
	Message Format	RJE or XML v2	

4 FAQ

1. What is the process for the validation of incoming messages?

   For incoming messages validation, you have to process the test messages supplied by the Validation Service provider and parse the message respecting the MFVR and SCORE Implementation Guidelines / Rule Book as the case may be.

2. Our application is on the corporate side and hence could you please inform us about the list of messages that we will receive, and what are the message types that we need to generate for label accreditation?

   The Validation Service provider will send you test messages that are received by the Corporates (bank-to-corporate flows) where your application is installed. Please refer to the label Criteria document for the list of messages in the bank-to-corporate flows. In addition, the Validation Service provider will provide you the static data (Account Number, BIC and BEI) for you to upload and validate.

   For the outgoing message validation, you have to generate 5 messages each of MT 101 and MT 210 from your application and attach the sample screenshot or application log file as evidence. These messages must be complaint to current SR MFVR and SCORE Rule book guidelines.

3. How will be incoming messages be composed?

   MT Messages provided will have header blocks and message text. I.e. Block 1 to 4).

4. For the MT validation, is it just the fact that the messages were entered in the application system and routed to a Valid or Invalid queue? Or do we need to specify each and every error that was found in the messages (in which case this might take several screen prints per message!)?

   In respect of valid / invalid messages, you can report the parsing errors or VALID as the case may be, in a spread sheet as per the format provide to you. Additionally, you can provide the screenshots for a sample set of messages that have failed / parsed through the application.

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

   The parsing result must be populated using the SWIFT defined Error Code. E.g. T13, T28 etc.

6. What if we report error description instead of error code?

   Not recommended. Error code reporting is the preferred and unambiguous method of reporting a discrepancy. However, in exceptional cases, Error Description is acceptable, provided, it is accompanied by the error line.

7. We are familiar with the SMART Test messages. Will you be using the same test messages for the technical validation of our application?

   The test messages that will be used for the technical validation will be similar to the SCORE messages used in SMART test messages

8. For testing outgoing messages, it is mentioned that vendor application should generate 10 MT messages. Can we generate and provide you additional test messages?

   Vendor application should generate and provide at least 10 MT Message over ITB. Additional test messages provided are acceptable but not recommended.

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