SWIFT Certified Applications

Corporates Cash Management

Technical validation Guide 2017

Version 1.1

February 2017

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 Applications 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

The certification of the SWIFT Certified Application for Corporates Cash 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 for Corporates Cash Management label Criteria 2017

This document focuses on the approach that a vendor application must follow to complete the technical validation against the SWIFT Certified Application for Corporates Cash Management criteria

In this document, a distinction is made between a **New Application** (vendors who apply the first time for a specific product release) and an **Application Renewal** (for product releases that already received the SWIFTReady 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 Cash Management label. The audience must be familiar with SWIFT from a technical and a business perspective.

1.4 Related Documents

- 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.
- The SWIFT Certified Application for Corporates Cash Management label criteria provide an overview of the criteria that a corporate application must comply with to be granted the SWIFT Certified Application.
- SWIFT for Corporates – SWIFT Standards MT Implementation Guide
- SWIFT Standards MX Message Reference Guide
- SWIFT for Corporates – SWIFTNet FileAct Implementation Guide
- SWIFT Standards MX – General Information
- SWIFT for Corporates - Standards MX Implementation Guide
- SWIFT for Corporates – Resource Centre

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 subject to validation during the functional validation.

The following matrix explains the tests that have to be performed by the vendor application in 2017.

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

(*)Connectivity testing is applicable only if the renewal vendor wish to qualify for the adapters other than the one, which they had shown in the past.

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 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 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 7.0 or 7.2 is mandated for the SWIFT Certified Application in 2017.

Note: New label applicant vendors, and vendors renewing their label application must exchange MT messages and MX 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 7.0 or 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 7.0 or 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, FileAct 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:
  - 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 Partner Management 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
  - 20 MT test messages in FIN comprising of Payment Messages (MT 101, 199 ,999)
  - 5 MX Messages in FileAct files comprising of pain.001.001.03
- These test messages must be compliant to Standards Release 2017
- 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 FileAct
- 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 Partner Management 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.

2.1.1.2 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
  - 20 MT test messages comprising of Payment (MT 101, 199 ,999)
  - 5 MX Messages in FileAct files comprising of pain.001.001.03.
- These test messages must be compliant to Standards Release 2017
- 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 FileAct
- 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 Partner Management 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:

- A 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
- 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 and FileAct)
- 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	
2.		Alliance Access Integration – AFT / MQHA / SOAP Support	
3.		Alliance Access Integration – RJE / XML v2 Format	
4.		Alliance Access Integration– FileAct Support	
5.	3.5	SWIFT MT and MX Support	
6.		Standards Release	
7.		Network Validation Rules (MFVR)	

2.2 Message Validation and FIN Standards Support

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

2.2.1 Testing of Incoming Messages

- The Validation Service provider will send a set of 20 MT test messages consisting of valid messages, which need to be uploaded by the vendor into and processed by vendor application.
- Test messages will consist of MT 940 and 942 and will be "inward to the application" direction.
- 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 spreadsheet 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 SRyy_CashMgtMTValidation.xls, where "yy" will represent the Year of the Standards Release. For example, for a file containing test messages for Standards Release 2017, the file name will be "SR17_CashMgtMTValidation.xls"
- The Validation Service provider will provide an MT Test Result Summary file in excel spreadsheet format that the vendor should use to capture the test results. The file name will be xxxx_SRnn_CashMgtMT_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 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 spreadsheet 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	Invalid Beneficiary Account			

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)
- SWIFT Standards MT Implementation Guide

Generating SWIFT Messages

- The vendor must generate 5 test messages for MT101 through their business application and as outbound ("application to Alliance Access") messages
- Test messages must be compliant to SR 2017
- The vendor application must wrap the SWIFT messages using RJE or XML v2 format

2.2.5 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
- 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, 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.

2.2.7 Qualification Criteria Verified

Sl. No	SWIFT Certified Application Qualification Criteria		Pass / Fail Status
	Section Ref Number	label Requirement	
8.	3.5	Standards	
9.	3.7	Message Validation (MFVR for FIN)	

2.3 Message Validation and MX Standards Support

Note: Testing for message validation and standards support is only for new label applicant vendors

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 FileAct 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 pain SCORE version 3 messages as well as MX camt.052.001.02, camt.053.001.02 & camt.054.001.02.

For additional information on XML Document validation, vendor may please refer to SWIFT Standards MX – General Information and SWIFT for Corporates - Standards MX Implementation Guide documents.

2.3.1 Testing of Incoming Messages

- The Validation Service provider will send a set of 10 MX test messages consisting of pain.002.001.03, camt.052.001.02,camt.053.001.02 and camt.054.001.02

File Naming Convention

- The files will bear the name as SRyy_CashMgt_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 Corporate Cash Management - Standards Release 2017 with sequence number 001, the file name will be "SR17_CashMgt001.XML"
- The Validation Service provider will also send a MX Test Result Summary file in excel spreadsheet format for capturing the test result from the vendor. The file name will be xxxx_yy_MX_Corporates Cash Management_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 spreadsheet 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	Pain.002-001.03	Pass	-				
2	Pain.002-002.03	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 5 test messages for pain.001.001.03 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	
10.	3.5	Standards	
11.	3.7	Message Validation (Rule Book Compliance for MX)	

3 Summary of Technical Validation

<table>
<tr><th colspan="2">Validation Activity</th><th>label NEW</th><th>label RENEWAL</th></tr>
<tr><td rowspan="2">Message Validation</td><td>Outgoing</td><td>FIN → MT 101, 199, 999

FileAct → pain 001 version 03</td><td rowspan="2">NA</td></tr>
<tr><td>Incoming</td><td>FIN → MT 199, 940, 942, 999

FileAct → pain 002 version 03

• camt 052.001.02
• camt 053.001.02
• camt 054.001.02</td></tr>
<tr><td rowspan="3">Standards</td><td>Standards Release</td><td colspan="2">Standards Release 2017 compliance</td></tr>
<tr><td>Rule Book Ref</td><td colspan="2">SCORE Rule book</td></tr>
<tr><td>Optional Messages</td><td colspan="2">Verified only on specific request by the vendor</td></tr>
<tr><td rowspan="4">Connectivity</td><td rowspan="4">Alliance Access 7.0 or 7.2</td><td colspan="2">FIN → AFT or MQHA or SOAPHA</td></tr>
<tr><td colspan="2">FileAct (RT) and (SF)</td></tr>
<tr><td colspan="2">RJE, XML v2</td></tr>
<tr><td colspan="2">FileAct → Parameter in XML v2</td></tr>
</table>

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 / MX Validations 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 where your application is installed. For example, MT 940, 942 and pain.002.001.03, camt.052.001.02,camt.053.001.02 and camt.054.001.02

Messages are normally received as incoming messages to a corporate. 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 pain.001 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 the incoming messages be composed? For FIN, will it have all the blocks (Block 1 to 4) and for MX messages will the messages contain the Alliance specific Header Info, Business Payload?

MT Messages provided will have header blocks and message text i.e. Block 1 to 4). For MX messages, the Validation Service provider will send only the Business Payload.

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 In MX messages, what do you mean by Extended Validation?

The extended validation will include the following:

- Cross Element Validation
- Intra-element Validation
- Calculations or derived elements
- External tables

9 For testing outgoing messages, it is mentioned that vendor application should generate 5 MT and 5 MX messages. Is number 5 fixed? Can we generate and provide you additional test messages?

Vendor application should generate and provide a minimum of 5 MT and 5 MX Message over ITB. Additional test messages are acceptable but not recommended.

10 Can MT messages be provided in multiple RJE files?

Though acceptable, it is preferable to send the entire MT Messages in a single RJE file.

11 Can MX messages be provided in single file?

No. one file must contain only one MX message. i.e. 5 files should be supplied each having single MX message.

12 How will the validation service provider verify “End to End Messaging support”?

End to End Messaging Support will be verified during Functional Validation. It will not be covered during technical validation process.

*****End of Document*****