SWIFT Partners

SWIFT Certified Application Exceptions and Investigations

Technical validation Guide 2016

Version 1

February 2016

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 mandated 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 Exceptions and Investigations 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 Exceptions and Investigations label criteria 2016

This document focuses on the approach that a vendor application must follow to complete the technical validation certified against the SWIFT Certified Application Exceptions and Investigations 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 for 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 SWIFT Certified Application Exceptions and Investigations 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 Exceptions and Investigations label criteria provide an overview of the criteria that a Exceptions and Investigations application must comply with to be granted the SWIFT Certified Application label
3. Bank-to-Bank - Standards MX Message Reference Guide (26 June 2009)
4. Corporate-to-Bank - Standards MX Message Reference Guide (26 June 2009)-
5. Exceptions and Investigations Integration Guide

2 Technical Validation Process

In this document a distinction is made between new label 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 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
Label Renewal	Delta	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.

New Applicants will go through a complete technical validation against the criteria laid down in the SWIFT Certified Application Exceptions and Investigations Criteria document.

The criteria that are verified include:

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

Note: Renewal label vendor will be tested only for Alliance Access connectivity testing. For message validation and standards support, there will be no technical validation as there is no change in the mandatory qualification criteria. Any upgraded versions of applications will, however be subjected to comprehensive testing.

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 InterAct messaging service.

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 7.0 is mandated for SWIFT Certified Application Label in 2016.

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 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 7.0	
	Adaptor	Format
New and Renewal	AFT	XML v2
	MQHA	
	SOAPHA	

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 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 7.0.
- The vendor will demonstrate the capability of the product to integrate with the Alliance Access with one of the following adaptors:
  - Automated File Transfer mode (AFT)
  - WebSphere 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 application should generate and send six outbound request types among the 16 MX messages in both the bank-to-bank and the corporate-to-bank CUGs
- The vendor must request for delivery notification
- The vendor application must exchange the SWIFT messages using Alliance Access 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.
- When the testing is performed on ITB, the service name specified for ITB environment only must be used. The details of Namespace Declaration and Service Name specification are provided in the end of this section.
- The application should add the Alliance Access specific messaging interface header to the business payload. The business payload consists of the application header + the Exceptions and Investigations business message
- The vendor must connect to SWIFT ITB, send MX 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.

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 and send six outbound request types among the 16 MX messages in both the bank-to-bank and the corporate-to-bank CUGs.
- Vendor must request for delivery notification
- The vendor application must exchange the SWIFT messages using Alliance Access XML v2 format
- When the testing is performed on ITB, the service name specified for ITB environment only must be used. The details of Namespace Declaration and Service Name specification are provided in the end of this section.
- The application should add the Alliance Access specific messaging interface header to the business payload. The business payload consists of the application header + the Exceptions and Investigations business message. The vendor must connect to SWIFT ITB, send MX 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 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:

- A copy of the MX test messages in XML v2 format generated by the business application
- Alliance Access Event Journal Report and Message File spanning the test execution window
- Application log / Screenshots evidencing the
    - processing of SWIFT messages
    - reconciliation of delivery notifications and Acknowledgements
- 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 if;

- All the messages are positively acknowledged by the SWIFT Network by reviewing the log files
- The application header adheres to the schema definition
- The MX Messages adhere to the Exceptions and Investigations Rulebook and MX Message Reference Guide, by sample verification of the MX Messages
- The messages are compliant with the standards release requested in the label criteria document, i.e. Exceptions and Investigations 1.2
- Application is able to reconcile technical messages

The test results will be analysed for building the scorecard and recommendation.

2.1.4 Qualification Criteria Verified

Sl. #	SWIFT Certified Application Label Qualification Criteria		Pass / Fail Status
	Section Ref #	Label Requirement Requirement Criteria	
1.	3.3.1	Alliance Access Integration Support	
2.		Alliance Access Integration Connectivity (AFT/MQHA/SOAPHA)	
3.		Alliance Access Integration – XML v2 Format	
4.		Alliance Access Integration – Application Header	
5.	3.5	Correct Payload Structure	
6.	3.5	Bank-to-bank and corporate-to-bank – SWIFTNet Service Name	

2.2 Message Validation and Standards Support

Requirement: The vendor must demonstrate the application's capability to support MX messaging standards, and Exceptions and Investigations (EI) rulebook compliance.

Note: The message validation and standards support testing is applicable to new label applicants only.

For each of the 16 EI messages, the vendor must generate and send on ITB two instances of the messages, one in the bank-to-bank CUG – swift.eni!x (with correct service name in message header), the other one on the corporate-to-bank CUG – swift.corp.eni!x (without service name in message header)

Namespace Declaration and Service Name

- In both CUGs, the MX Standards schemas are identical at the business payload level. They are however slightly different at the name space declaration level. The corporate-to-bank standards do not contain the service name in the name space declaration of the Document line and three of them have different names due to ISO certification.

- The following table summarises the correct usage of name space declarations in the bank-to-bank and corporate-to-bank spaces.

Message Type	Namespace Declaration	
	corporate-to-bank	bank-to-bank
camt.007.002.02	urn:swift:xsd:camt.007.002.02	urn:swift:xsd:swift.eni$camt.007.002.02
camt.008.002.02	urn:swift:xsd:camt.008.002.02	urn:swift:xsd:swift.eni$camt.008.002.02
camt.026.001.02	urn:swift:xsd:camt.026.001.02	urn:swift:xsd:swift.eni$camt.026.001.02
camt.027.001.02	urn:swift:xsd:camt.027.001.02	urn:swift:xsd:swift.eni$camt.027.001.02
camt.028.001.02	urn:swift:xsd:camt.028.001.02	urn:swift:xsd:swift.eni$camt.028.001.02
camt.029.001.02	urn:swift:xsd:camt.029.001.02	urn:swift:xsd:swift.eni$camt.029.001.02
camt.030.001.02	urn:swift:xsd:camt.030.001.02	urn:swift:xsd:swift.eni$camt.030.001.02
camt.031.001.02	urn:swift:xsd:camt.031.001.02	urn:swift:xsd:swift.eni$camt.031.001.02
camt.032.001.01	urn:iso:std:iso:20022:tech:xsd:camt.032.001.01	urn:swift:xsd:swift.eni$camt.032.001.01
camt.033.001.02	urn:swift:xsd:camt.033.001.02	urn:swift:xsd:swift.eni$camt.033.001.02
camt.034.001.02	urn:swift:xsd:camt.034.001.02	urn:swift:xsd:swift.eni$camt.034.001.02
camt.035.001.01	urn:swift:xsd:camt.035.001.01	urn:swift:xsd:swift.eni$camt.035.001.01
camt.036.001.01	urn:iso:std:iso:20022:tech:xsd:camt.036.001.01	urn:swift:xsd:swift.eni$camt.036.001.01
camt.037.001.02	urn:swift:xsd:camt.037.001.02	urn:swift:xsd:swift.eni$camt.037.001.02
camt.038.001.01	urn:iso:std:iso:20022:tech:xsd:camt.038.001.01	urn:swift:xsd:swift.eni$camt.038.001.01
camt.039.001.02	urn:swift:xsd:camt.039.001.02	urn:swift:xsd:swift.eni$camt.039.001.02

- The messages exchanged must adhere to the correct service name specification for the bank-to-bank, bank-to-corporate and corporate-to-bank flows as below:

Message Flow	Service Name	Environment
Corporate-to-bank and bank-to-corporate	swift.corp.eni!p	Test & Training
	swift.corp.eni	ITB
Bank-to-bank	swift.eni!p	Test & Training
	swift.eni	ITB

- The application should add the Alliance Access specific messaging interface header to the business payload. The business payload consists of the application header + the Exceptions and Investigations business message. When the application connects with Alliance Access through a Financial EAI, the specific messaging interface header must be added to the business payload.

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 MX test messages in XML v2 format generated by the business application

2.2.2 Verification of the Test Results

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

- The Alliance Access messaging interface header is present

- The application header adheres to the schema definition
- The MX Messages adhere to the Exceptions and Investigations Rulebook and MX Message Reference Guide, by sample verification of the MX Messages
- The messages are compliant with the standards release requested in the label criteria document, i.e. Exceptions and Investigations 1.2

The test results will be analysed for building the scorecard and recommendation

2.2.3 Qualification Criteria Verified

Sl. #	SWIFT Certified Application Label Qualification Criteria		Pass / Fail Status
	Section Ref #	Label Requirement Requirement Criteria	
7.	3.3.1	Alliance Access Integration – XML v2 Format	
8.		Alliance Access Integration – Application Header	
9.	3.5	Messaging Support – EI 1.2 – bank-to-bank and corporate-to-bank	
10.	3.5	Standards Support – EI 1.2 – bank-to-bank and corporate-to-bank	
11.	3.5	Correct Payload Structure	
12.	3.7	Message Validation	

3 Summary of Technical Validation

Validation Activity		Label NEW	Label RENEWAL
Message Validation	Outgoing	16 EI messages	No Validation
Standards	SRG	EI Release 1.2	
	Rule Book Ref	EI Rulebook	
	Optional Messages	Verified only on specific request by the vendor	
Connectivity	Alliance Access	AFT or MQHA or SOAPHA	NA
	Message Format	RJE and / or XML v2	NA

4 FAQ

1. Currently we do not have ITB connectivity, and we are NOT sure whether our customers allow us to use their environment. However, we have Alliance Access installed at our end. Could you please clarify whether it is sufficient, for the technical validation, to connect our application to Alliance Access using AFT or MQHA or SOAPHA and provide you the evidences?

   Connecting to ITB and exchanging test messages over ITB is mandatory as per the Qualification Criteria for SWIFT Certified Application Exceptions & Investigations Label. 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

2. What is the correct setting for the Validation Level in the Alliance Access HeaderInfo field?

   The validation level in the Alliance Access HeaderInfo must be at least “Intermediate”. Otherwise Alliance Access will not validate against the installed ENI schema.

3. What are the implications of the Validation Level in the HeaderInfo, as we find that all have the same level of validation?

   Indeed for MX, unlike MT, the “minimum” and “intermediate” settings have the same behaviour. However, these emission profile settings can be overridden in the XML v2 (Validation Level). So if “none” is specified in XML v2, then it overrides “minimum” and “intermediate” of the emission profile. If “maximum” is present in the emission profile then it is enforced even if “none” is in XML v2.

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