



SWIFT Certified Applications

Alliance Access Integration – Automated File Transfer

Technical Qualification Test 2018

This document lists the tests for application providers that integrate their middleware or back-office application with Alliance Access using Automated File Transfer (AFT) Adaptor.

Version 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, SWIFT 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	Purpose.....	4
1.2	Audience.....	4
1.3	SWIFT Certified Application Programme.....	4
1.4	Related Documents.....	4
2	Introduction	5
2.1	SWIFT Certified Application Validation.....	5
3	Alliance Access configuration	6
3.1	Alliance Access.....	6
3.2	Message Partner configuration.....	6
3.3	Exchanging messages using Message Partner.....	6
4	Wipro Testing Service	7
5	AFT Test Preparation	8
5.1	Reconciliation of Delivery Notification.....	8
5.2	Transmission Notification.....	8
6	SWIFT Certification AFT testing	9
6.1	Test Evidence.....	9
7	Annexure	10
7.1	Sample Message Partner Configuration.....	10
7.2	Input MT Message sample in RJE format.....	15
7.3	Input MT Message sample in XML v2 format.....	16
7.4	ACK Message with Original Message.....	16
7.5	Delivery Notification Message.....	17
7.6	Output MT Message sample in RJE format.....	17
7.7	NAK Message with Original Message.....	18
7.8	Input message in XML V2 for FileAct.....	19
7.9	Ack message in XML V2 for FileAct.....	20
7.10	OUT message in XML V2 for FileAct.....	21
7.11	Delivery Notification message in XML V2 for FileAct.....	24

1 Preface

1.1 Purpose

This document describes the test scenarios to qualify software integrating with SWIFT Alliance Access using AFT.

The purpose of the AFT qualification is to validate the generation, transmission and reconciliation of files transferred from the partner application to Alliance Access.

1.2 Audience

The target audience for this document is both vendors considering the certification of a product, and SWIFT Users that look after an overview of the SWIFT Certified Application contents. This document guide the application providers that integrate their middleware or back-office application with Alliance Access using AFT. The audience should be familiar with SWIFT world from both a technical and a business perspective.

1.3 SWIFT Certified Application Programme

The SWIFT Certified Application programme covers the entire financial application chain, from Trade, Treasury and Payment, to Corporate and Securities segments.

Each SWIFT Certified Application defines a set of criteria, which are reviewed every year to ensure that the software remains aligned with the financial market evolution and with customer needs.

These criteria are designed to reflect the capability of a financial application to provide message processing automation in a SWIFT context, and to support straight through processing (STP) in order to increase customer value, limit customisation needs and cost, and reduce time to market.

1.4 Related Documents

- [Alliance Access 7.2](#)
- [Alliance Access - System Management Guide](#)
- [sam_aaccess_headers](#)

2 Introduction

Alliance Access provides different integration adapters for back-office applications and middleware products. One of the most common integration adapters to Alliance Access is the Automated File Transfer (AFT).

AFT is using the standard mechanism of Message Partner definition available in Alliance Access, including routing rules and profile definition. Routing rules must also be defined to integrate each Message Partner inside the Alliance Access routing scheme. AFT functionality is aligned with the way all other Message Partner works in Alliance Access.

2.1 SWIFT Certified Application Validation

Support of AFT is one of the qualification criteria for granting the SWIFT Certified Application label to a financial application.

The Partners who deployed the SWIFT Alliance connectivity to SWIFT ITB can perform these tests independently. Test environment configuration is described in [section 3](#).

As an alternative, Wipro Testing Services offers a test service for connecting to SWIFT ITB. Using this service, the Partner can connect to SWIFT ITB. Currently, the testing service allows testing application connectivity with Alliance Access AFT, MQHA and SOAPHA. Please go to [section 4](#), if you wish to use this service.

3 Alliance Access configuration

This set-up is applicable for Partners that deployed an ITB environment and connect to Alliance Access from their premises.

3.1 Alliance Access

To prepare for the tests, the Alliance Access system must be installed and configured at Partner premises.

Alliance Access must be upgraded to release 7.2. It is necessary to get acquainted with the [Alliance Access - System Management Guide](#) and [alliance access 7.2](#) to further configure the interface for test purpose. The Application Interface module of Alliance Access provides all the functions necessary to manage Message Partner profiles. Using Application Interface application, the Partner needs to set up the connection profiles that are used by Alliance Access to connect with external message partners. The Application Interface allows exchanging messages with external back-office systems or "Message Partners".

3.2 Message Partner configuration

The AFT communication session is set up and controlled with a dedicated Message Partner configuration in Alliance Access. Using the procedure described in the Alliance Access System Management Guide – File Transfer Connection Method, create a Message Partner for the file transfer.

- Specify the connection method as File Transfer
- Specify the direction of message transfer (from Message Partner and To Message Partner)
- Configure the other parameters

The partner must ensure that the Alliance Access server must be running and the Message Partner is enabled. The vendor application must have access to the input directory configured in the "From" Message Partner and provide access for Alliance Access to transfer messages in the output directory configured in the "To" Message Partner.

Please refer to System Management Guide – Alliance Access for additional information for configuring and managing Message Partner Profiles. A screenshot of sample Message Partner is provided in [section 7](#).

3.3 Exchanging messages using Message Partner

- AFT supports both MT and MX messages. MT test messages can be exchanged using RJE format and XML v2 format, while MX test messages can only be sent in XMLv2 format.
- The application provider will prepare a batch file containing application generated MT or MX messages and copy it in the input directory for Alliance Access to process
- The messages being sent must be the message types supported by the partner application.
- The file name used for automatic input must not contain any space or any other special character.
- The successfully processed test messages will be stored by Alliance Access in the _SI_to_SWIFT Queue [MT test messages) or _SI_to_SWIFTNet (MX test messages) Queue.
- SWIFT Network returns Notification messages for technical reconciliation and response messages, since the test messages were used for "self transfers", meaning, the sender and receiver BIC are the same
- The application must download the Network notifications and messages sent in "Output from SWIFT" direction

4 Wipro Testing Service

- The vendor needs to liaise with Wipro to enrol into Wipro Testing Services and test the exchange of messages through this service
- The vendor will be provided with a PIC (Partner ID Code) This PIC must be used in the sender and receiver block for exchanging messages over ITB
- The service is only available for self transfers, meaning that the sender and receiver of the test messages and test files must bear the same PIC and DN as provided by Wipro
- The connectivity is very similar when you connect from within vendor environment using any standard Secured File Transfer Protocol (SFTP) software, except for the reason that this connectivity is established outside vendor's internal network environment
- Wipro will provide user credential once the vendor agrees on the terms to avail the testing service
- For a SFTP transfer, the vendor will be provided with a root folder with input and output sub-folders at Wipro, with appropriate access rights
- The SFTP uses port 22 to connect and exchange files over internet and hence necessary permission must be obtained upfront from vendor's IT Security team
- The vendor will connect to the Wipro and transfer the application generated MT or MX messages in the input directory for Alliance Access to process
- The messages being sent must be the message types supported by the partner application.
- The file name used for automatic input must not contain any space or any other special character
- Once the connectivity is established, the outgoing messages will be picked automatically by Alliance Access
- SWIFT Network returns Notification messages for technical reconciliation and response messages, since the test messages were used for "self transfers", meaning, the sender and receiver BIC are the same
- The application must download the Network notifications and messages sent in "Output from SWIFT" direction

5 AFT Test Preparation

AFT supports the exchange of messages in the following data formats:

- **RJE Format (MT messages only)**

Currently, RJE (Remote Job Entry) and XML v2 formats are supported for the exchange of test messages. The RJE format is only applicable for MT messages, while XML v2 format is applicable for both MT and MX messages.

In RJE formatted messages, all fields in Block 4 (Message Text Block) have a Carriage Return and Line Feed (CrLf) at the beginning of every field. For fields containing multiple lines, CrLf must be present at the end of every line. RJE format allows multiple messages sent in a batch file. The messages are separated with "\$" as delimiter and there must be no message separator at the end of the last message in the batch file. For more details about the RJE format, please refer to Alliance Access – System Management guide.

- **XML version 2 (MX and MT messages, and files for FileAct service)**

A XML v2 message consists of an Alliance Access Header, an optional Application Header and a Message details block. In case MT messages are exchanged using XML v2 format, then the Message Block must be encrypted using Base 64.

For more information about these formats, see the [Alliance Access System Management Guide – Message Formats Used in AI](#). A sample of the [RJE](#) and [XML v2](#) message format is provided in **Annexure**. Please refer to sam_aaccess_headers.pdf document for messages samples exchanged with Alliance Access, in scope of the SWIFT solution.

For SWIFT Certification, at least one of the following file formats will be tested:

- RJE for MT message
- XML v2 format for MT or MX messages

5.1 Reconciliation of Delivery Notification

When the messages are sent to Alliance Access, the application can optionally request for a delivery notification. This will result in Alliance Access receiving a message about the message delivery, which can be reconciled with the original message.

The Partner must demonstrate the capability of their application to process the Delivery Notification Message and to reconcile it with the original message.

A sample Delivery Notification message is provided in [section 7](#).

5.2 Transmission Notification

A transmission notification is a message representing the result of transmission to SWIFT network. SWIFT performs full syntax and semantic checks before it returns an acknowledgement ([ACK](#)). Other checks, such as validity of the sender and the receiver, are also performed. These checks can cause a message to be rejected and a negative acknowledgement ([NAK](#)) is returned in response.

The vendor must demonstrate their application capability to process the Transmission Notification Message and reconcile with the original message.

A sample Transmission Notification message is provided in [section 7](#).

6 SWIFT Certification AFT testing

To be qualified as AFT compliant, Partners need to send MT and/or MX messages (depending on the label category), and act upon received MT/MX messages including ACK / NAK and delivery notifications.

1. The partner application vendor prepares the number of MT / MX test messages generated by the application as required for the SWIFT Certification at stake. When these messages are placed on the input directory, the "From" session is initiated automatically and the test messages are processed by Alliance Access
2. Partners having their own ITB environment must use their PIC in the sender and receiver fields of the message. The Partner using Wipro Testing Services for connecting to ITB must use the PIC provided by Wipro in the sender and receiver field of the message.
3. If the partner application supports only MT messages, the test messages can be sent in either RJE format or in XML v2 format. If the business application supports SWIFT Solutions, then the only format Alliance can read is XML v2 format
4. For individual label requirements, the vendor application must exchange application supported SWIFT Messages. Vendor should refer to label specific technical validation guide for the in-scope SWIFT MT and/or MX Messages.
5. The partner application must include delivery notification instructions while generating the test messages. The back office application must receive the delivery notification information and reconcile with the original message sent to Alliance Access
6. The acknowledgement of transmission is sent through transmission notification message. The partner application must capture the ACK and NAK received back from SWIFT and reconciled in the application. Evidences of reconciliation mechanism (screen dump, event log, dataset extract,) will be handled back to SWIFT Qualification service provider.

6.1 Test Evidence

The Partner should extract the following evidences covering the testing period and send them via email to the Validation Service provider for Technical Validation of AFT connectivity test.

Partners with own ITB connectivity

- Alliance Access Event Journal report
- Message File report
- Message Partner Configuration details
- Samples of ASCII (MT) and XMLv2 files (MT and MX)
- Screenshots / Log File / Dataset extract / Reports generated from the Partner application evidencing the test execution through Partner application and the reconciliation mechanism against delivery notification and transmission notification for ACK and NAK

Partners testing through Wipro Testing Service

- Alliance Access Event Journal report, Message File and Message partner configuration details will be generated by Wipro
- The Partner to provide samples of ASCII (MT) and XMLv2 files (MT and MX)
- Screenshots / Log File / Dataset extract / Reports generated from the Partner application evidencing the test execution through Partner application and the reconciliation mechanism against delivery notification and transmission notification for ACK and NAK

7 Annexure

7.1 Sample Message Partner Configuration

Direction: From Message Partner (to Alliance Access) Format: RJE

Message Partner Details - MPA15FTMTIN Help

Configuration **Monitoring**

Name: MPA15FTMTIN
 Description: A15
 Status: Enabled
 Partner Id: 194

Allowed Direction: From Message Partner
 Connection Method: File Transfer

File Transfer

Data Format: RJE
 Session Initiation: Automatic
 Parameter File: Not Required
 Profile Name: R7.0_MsgPartner

Local Authentication

Reception

Input Filename Pattern: D:\BRANCHES\A15\151_5301739162_M
 FileAct Payload Timeout (seconds): 0

Close Refresh Export Print Disable Start Session Previous Next

Message Partner Details - MPA15FTMTIN Help

Configuration **Monitoring**

File Transfer

Data Format: RJE
 Session Initiation: Automatic
 Parameter File: Not Required
 Profile Name: R7.0_MsgPartner

Local Authentication

Reception

Input Filename Pattern: D:\BRANCHES\A15\151_5301739162_M
 FileAct Payload Timeout (seconds): 0
 Validation level: No Validation
 Message modification: Allowed
 Unit to be assigned: None
 Emission expiry: Days
 Batch File Validation: Continue on Rejection
 Build unique file transfer reference:
 Routing: Dispose message in: Ready To Send

Close Refresh Export Print Disable Start Session Previous Next

Direction: To Message Partner (From Alliance Access) Format: RJE

Message Partner Details - MPA15FTMTOUT Help

Configuration | **Monitoring**

Name: MPA15FTMTOUT
 Description: A15
 Status: Enabled
 Partner Id: 195

Allowed Direction: To Message Partner
 Connection Method: File Transfer

File Transfer

Data Format: RJE
 Session Initiation: Automatic
 Parameter File: Not Required
 Profile Name: R7.1_MsgPartner

Local Authentication

Emission

Available	Selected
FileActAcks FileActReceived FileActReject	EPA15FTMTOUT

Close Refresh Export Print Disable Start Session Run Session Previous Next

Message Partner Details - MPA15FTMTOUT Help

Configuration | **Monitoring**

Emission

Exit Points	Available	Selected
	FileActAcks FileActReceived FileActReject MXToBeInvestigated ToBeInvestigated	EPA15FTMTOUT

Output Filename Pattern: D:\BRANCHES\A15\152_5301739162_M
 Output File Extension: out
 Local transfer command:
 Command Parameters:

Always transfer MAC/PAC:
 Transfer PKI Signature:
 Routing Code Transmitted:
 Transfer Original Message with Notification: Always
 Maximum number of messages per session:
 Increment Sequence Number across Sessions:

Run Output Session Triggers

Number of messages: 1
 Or at (hh:mm): Add

Close Refresh Export Print Disable Start Session Run Session Previous Next

Direction: From Message Partner (to Alliance Access) Format: XML v2

Message Partner Details - MPA15FTMXIN Help

Configuration **Monitoring**

Name: MPA15FTMXIN
 Description: A15
 Status: Enabled
 Partner Id: 196

Allowed Direction: From Message Partner
 Connection Method: File Transfer

File Transfer

Data Format: XML Version 2 Original
 Session Initiation: Automatic
 Parameter File: Not Required
 Profile Name: R7.0_MsgPartner

Local Authentication

Reception

Input Filename Pattern: D:\BRANCHES\A15\153_5301739162_M
 Input Attachment Path:

Close Refresh Export Print Disable Start Session Previous Next

Message Partner Details - MPA15FTMXIN Help

Configuration **Monitoring**

Data Format: XML Version 2 Original
 Session Initiation: Automatic
 Parameter File: Not Required
 Profile Name: R7.0_MsgPartner

Local Authentication

Reception

Input Filename Pattern: D:\BRANCHES\A15\153_5301739162_M
 Input Attachment Path:
 FileAct Payload Timeout (seconds): 0
 Generate Report File: No
 Validation level: No Validation
 Message modification: Allowed
 Unit to be assigned: None
 Emission expiry: Days
 Batch File Validation: Continue on Rejection
 Build unique file transfer reference:
 Routing: Dispose message in: Ready To Send

Close Refresh Export Print Disable Start Session Previous Next

Direction: From Message Partner (to Alliance Access) Format: XML v2 for FileAct

Message Partner Details - MPA08FTMXIN Help

Configuration **Monitoring**

Name: MPA08FTMXIN
 Description: A08
 Status: Enabled
 Partner Id: 118

Allowed Direction: From Message Partner
 Connection Method: File Transfer

File Transfer

Data Format: XML Version 2 Original
 Session Initiation: Automatic
 Parameter File: Not Required
 Profile Name: R7.0_MsgPartner

Local Authentication

Reception

Input Filename Pattern: D:\BRANCHES\A08\109_3040538744_M
 Input Attachment Path: D:\BRANCHES\A08\109_3040538744_F

Close Refresh Export Print Disable Start Session Previous Next

Message Partner Details - MPA08FTMXIN Help

Configuration **Monitoring**

Data Format: XML Version 2 Original
 Session Initiation: Automatic
 Parameter File: Not Required
 Profile Name: R7.0_MsgPartner

Local Authentication

Reception

Input Filename Pattern: D:\BRANCHES\A08\109_3040538744_M
 Input Attachment Path: D:\BRANCHES\A08\109_3040538744_F

FileAct Payload Timeout (seconds): 0
 Generate Report File: No
 Validation level: No Validation
 Message modification: Allowed
 Unit to be assigned: None
 Emission expiry: Days
 Batch File Validation: Continue on Rejection
 Build unique file transfer reference:

Routing: Dispose message in: Ready To Send

Close Refresh Export Print Disable Start Session Previous Next

Direction: To Message Partner (to Alliance Access) Format: XML v2 for FileAct

Message Partner Details - MPA08FTMXOUT Help

Configuration **Monitoring**

Name:
 Description:
 Status: **Enabled**
 Partner Id: **119**

Allowed Direction:
 Connection Method:

File Transfer

Data Format:
 Use Binary Prefix:
 Session Initiation:
 Parameter File:
 Profile Name:

Local Authentication

Emission

FileActAcks: EPA08FTMXOUT

Close Refresh Export Print Disable Start Session Run Session Previous Next

Message Partner Details - MPA08FTMXOUT Help

Configuration **Monitoring**

Exit Points

Available: FileActAcks, FileActReceived, FileActReject, MXToBelInvestigated, ToBelInvestigated
 Selected: EPA08FTMXOUT

Output Filename Pattern:
 Output File Extension:
 Output Attachment Path:
 Output Attachment Extension:
 Local transfer command:
 Command Parameters:

Always transfer MAC/PAC:
 Message Emission Format:
 Transfer Original Message with Notification:
 Maximum number of messages per session:
 Original Message Format:
 Increment Sequence Number across Sessions:

Run Output Session Triggers

Number of messages:

Close Refresh Export Print Disable Start Session Run Session Previous Next

7.2 Input MT Message sample in RJE format

```
{1:F01SPXAINJJAXXX0001000455}{2:I569SPXAINJJXXXN2}{3:{108:16-569-SR-P001}}{4:
:001/LAST
:20C::SEME//16-569-ACK-P026
:23G:CANC
:98C::PREP//20140202100000
:22F::STBA/EOSP
:22H::REPR//PROV
:16R:COLLPRTY
:95Q::CLPA//PARTY NAME CLT
:97A::SAFE//123456
:16S:COLLPRTY
:16R:LINK
:20C::PREV//569001
:16S:LINK
:16S:GENL
:16R:SUMM
:19A::COVA//USD10000000,
:19A::TEXA//USD9000000,
:19A::MARG//USD270000,
:19A::TCOR//USD11000000,
:92A::MARG//3,0
:25D::GCST//DEFI
:98A::VALN//20140202
:16S:SUMM
:16R:SUME
:22F::COLA//OPTN
:19A::COVA//USD10000000,
:19A::TEXA//USD9000000,
:19A::TCOR//USD11000000,
:92A::MARG//3,0
:25D::GETS//DEFI
:16R:SUMC
:13B::ELIG//1234PROF145
:95P::PTYB//SWHQBEBB
:19A::COVA//USD10000000,
:19A::TEXA//USD9000000,
:19A::TCOR//USD11000000,
:19A::MARG//USD270000,
:92A::MARG//3,0
:25D::GCOS//FLAT
:16R:TRANSDT
:20C::CLTR//CLN00102AB235
:98A::TERM//20140202
:98A::EXRQ//20140202
:19A::COVA//USD10000000,
:19A::TEXA//USD9000000,
:19A::TRAA//USD9000000,
:19A::TCOR//USD11000000,
:22F::MICO//A013
:92A::MARG//5,1
:16R:VALDET
:17B::COLL//Y
:17B::SECU//Y
:98A::SETT//20140202
:19A::MVPF//USD10000000,
:19A::LICO//USD9000000,
:19A::MVPF//USD9000000,
:92B::EXCH//USD/GBP/2,0
:92A::VAFC//2,
:22F::MICO//A013
:16R:SECDT
:35B:ISIN US0000123456
:36B::SECV//UNIT/10000,
:95L::ALTE//LEGALENTIDENTIFIER45
:95P::ACOW//SWHQBEBB
:97B::SAFE//DVPA/234-87-65767
```

```

:25D::SETT//PEND
:11A::DENO//USD
:90A::MRKT//PRCT/2,0
:94B::RATS//VEND
:70C::RATS//AAA+
:16S:SECDDET
:16S:VALDET
:16S:TRANSDDET
:16S:SUMC
:16S:SUME
-}

```

7.3 Input MT Message sample in XML v2 format

```

_001000_____<?xml version="1.0" encoding="UTF-8"?>
<DataPDU xmlns="urn:swift:saa:xsd:saa.2.0">
  <Header>
    <Message>
      <SenderReference>MT101-b64-test2-feb10</SenderReference>
      <MessageIdentifier>fin.101</MessageIdentifier>
      <Format>MT</Format>
      <Sender>
        <BIC12>SPXAINJJAA05</BIC12>
      </Sender>
      <Receiver>
        <BIC12>SPXAINJJXXX</BIC12>
      </Receiver>
      <InterfaceInfo>
        <UserReference>101-ACK-N-XXX-01</UserReference>
      </InterfaceInfo>
      <NetworkInfo>
        <Service>swift.fin!p</Service>
      </NetworkInfo>
      <SecurityInfo>
        <SWIFTNetSecurityInfo/>
      </SecurityInfo>
    </Message>
  </Header>

  <Body>DQo6MjA6MTAzLUFDSy1OLVhYWC0wMw0KOjIzQjpDUkVEDQo6MzJBOjExMDIxMIVTRDE
wMDAsMDANCjozM0I6VVNEMTAwMCwwMA0KOjUwQTovMTIzNDU2DQpTV0hRQkVCQg0KOjU3Q
TpTV0hRQkVCQg0KOjU5QTpTV0hRQkVCQg0KOjcxQTpTSEENCi19</Body>
</DataPDU>

```

7.4 ACK Message with Original Message

```

{1:F21SPXAINJJAXXX0062122997}{4:{177:1107130720}{451:0}{108:16-540-SR-
P001}}{1:F01SPXAINJJAXXX0062122997}{2:I540SPXAINJJXXXN2}{3:{108:16-540-SR-P001}}{4:
:16R:GENL
:20C::SEME//16-540-SR-2016
:23G:NEWM
:16R:LINK
:20C::POOL//REFERENCE
:36B::TURN//FAMT/1000000,
:16S:LINK
:16S:GENL
:16R:TRADDET
:98A::SETT//20101120
:35B:ISIN US0000123456
ABCD
:16R:FIA

```


:94B::PLIS/XNYS/EXCH/NEWYORK STOCC EXCHANGE
:22F::MICO//A012
:98A::MATU//20181120
:16S:FIA
:22F::RPOR//DEFR
:16S:TRADDET
:16R:FIAC
:36B::SETT//FAMT/100000,
:97A::SAFE//123456
:16S:FIAC
:16R:SETDET
:22F::STCO//NPAR
:22F::SETR//TURN
:16R:SETPRTY
:95P::BUYR//SWHQBEBB
:16S:SETPRTY
:16R:SETPRTY
:95P::SELL//SWHQBEBB
:97A::SAFE//123456
:16S:SETPRTY
:16R:SETPRTY
:95P::DEAG//SWHQBEBB
:16S:SETPRTY
:16R:SETPRTY
:95C::PSET//US
:16S:SETPRTY
:16S:SETDET
-}{5:{MAC:00000000}{CHK:D37613267275}}

7.5 Delivery Notification Message

{1:F21SPXAINJJAXXX0062040262}{4:{177:1107131151}{451:0}}{1:F01SPXAINJJAXXX0062040262}
{2:O0110621110713DYLRLXXXXHXXX00004188011107130721S}{4:{175:0720}{106:110713SPXAINJ
JAXXX0062122997}{108:16-540-SR-
P001}{175:0720}{107:110713SPXAINJJAXXX0062040261}}{5:{CHK:70D184C5EACD}{SYS:}}{S:{CO
P:P}}

7.6 Output MT Message sample in RJE format

{1:F21SPXAINJJAXXX0062040261}{4:{177:1107131150}{451:0}}{1:F01SPXAINJJAXXX0062040261}
{2:O5400720110713SPXAINJJAXXX00621229971107130720N}{3:{108:16-540-SR-P001}}{4:
:16R:GENL
:20C::SEME//16-540-SR-2010
:23G:NEWM
:16R:LINK
:20C::POOL//REFERENCE
:36B::TURN//FAMT/1000000,
:16S:LINK
:16S:GENL
:16R:TRADDET
:98A::SETT//20101120
:35B:ISIN US0000123456
ABCD
:16R:FIA
:94B::PLIS/XNYS/EXCH/NEWYORK STOCC EXCHANGE
:22F::MICO//A012
:98A::MATU//20181120
:16S:FIA

:22F::RPOR//DEFR
:16S:TRADDET
:16R:FIAC
:36B::SETT//FAMT/100000,
:97A::SAFE//123456
:16S:FIAC
:16R:SETDET
:22F::STCO//NPAR
:22F::SETR//TURN
:16R:SETPRTY
:95P::BUYR//SWHQBEBB
:16S:SETPRTY
:16R:SETPRTY
:95P::SELL//SWHQBEBB
:97A::SAFE//123456
:16S:SETPRTY
:16R:SETPRTY
:95P::DEAG//SWHQBEBB
:16S:SETPRTY
:16R:SETPRTY
:95C::PSET//US
:16S:SETPRTY
:16S:SETDET
-}{5:{MAC:00000000}{CHK:D37613267275}}{S:{SAC:}{COP:P}}

7.7 NAK Message with Original Message

{1:F21SPXAINJJAA050011096785}{4:{177:1102101209}{451:1}{405:E46005}{108:16-101-NAK-01}}{1:F01SPXAINJJAA050011096785}{2:I101SPXAINJJAA05N}{3:{108:16-101-NAK-01}}{4:
:20:10-101-NAK-01
:13C:/RNCTIME/1240+0100
:23B:CRTS
:23E:TELI/Additional Information
:23E:TELI
:32A:091120USD15000,00
:33B:USD15100,00
:50K:/12345678
ORDERING CUSTOMER NAME
:52A:SWHQBEBB
:53D:/C/23456789
SENDER'S CORRESPONDENT
HONG KONG BRANCH
HONG KONG
:54B:/C/987654321
HONG KONG BRANCH
:56A:/C/654321
SWHQBEBB
:57D:/654321
ACCOUNT WITH INSTITUTION
:59:BENEFICIARY CUSTOMER NAME
HONG KONG
HONG KONG
:70:/INV/070717, 12345, INVOICE
NUMBERS 24578, 54789,
354789, 545884, 578822
987664, 3211458, 56412636
:71A:BEN
:71F:USD100,00
:72:/ACC/INSTRUCTIONS ARE FOR
//ACCOUNT WITH INSTITUTION
//TO EXECUTE
:77B:/ORDERRES/US//ADDITIONAL INFO

```
//CONTINUATION OF ADDITIONAL INFO  
-}{5:{MAC:00000000}{CHK:F815F08BA4D7}}
```

7.8 Input message in XML V2 for FileAct

```
_001154_____<?xml version="1.0" encoding="UTF-8" standalone="no" ?>  
<Saa:DataPDU xmlns:Saa="urn:swift:saa:xsd:saa.2.0" xmlns:Sw="urn:swift:snl:ns:Sw"  
xmlns:SwGbl="urn:swift:snl:ns:SwGbl" xmlns:SwInt="urn:swift:snl:ns:SwInt"  
xmlns:SwSec="urn:swift:snl:ns:SwSec">  
  <Saa:Revision>2.0.7</Saa:Revision>  
  <Saa:Header>  
    <Saa:Message>  
      <Saa:SenderReference>AFT_FA_test1</Saa:SenderReference>  
      <Saa:MessageIdentifier>camt.007.002.02</Saa:MessageIdentifier>  
      <Saa:Format>File</Saa:Format>  
      <Saa:Sender>  
        <Saa:DN>o=spxainjj,o=swift</Saa:DN>  
        <Saa:FullName>  
          <Saa:X1>SPXAINJJXXX</Saa:X1>  
        </Saa:FullName>  
      </Saa:Sender>  
      <Saa:Receiver>  
        <Saa:DN>o=spxainjj,o=swift</Saa:DN>  
        <Saa:FullName>  
          <Saa:X1>SPXAINJJXXX</Saa:X1>  
        </Saa:FullName>  
      </Saa:Receiver>  
      <Saa:InterfaceInfo>  
        <Saa:UserReference>AFT_FA_test1</Saa:UserReference>  
      </Saa:InterfaceInfo>  
      <Saa:NetworkInfo>  
        <Saa:Service>swift.generic.fast!x</Saa:Service>  
      </Saa:NetworkInfo>  
    </Saa:Message>  
  </Saa:Header>  
  <Saa:Body>AFT_FA.JPG</Saa:Body>  
</Saa:DataPDU>
```

7.9 Ack message in XML V2 for FileAct

```
_002098_____<?xml version="1.0" encoding="UTF-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:saa:xsd:saa.2.0" xmlns:Sw="urn:swift:snl:ns.Sw"
xmlns:SwInt="urn:swift:snl:ns.SwInt" xmlns:SwGbl="urn:swift:snl:ns.SwGbl"
xmlns:SwSec="urn:swift:snl:ns.SwSec">
<Saa:Revision>2.0.7</Saa:Revision>
<Saa:Header>
<Saa:TransmissionReport>
<Saa:SenderReference>AFT_FA_test1</Saa:SenderReference>
<Saa:ReconciliationInfo>SNL02013D11330601714009891C</Saa:ReconciliationInfo>
<Saa:NetworkDeliveryStatus>NetworkAcked</Saa:NetworkDeliveryStatus>
<Saa:OriginalInstanceAddressee>
<Saa:X1>SPXAINJJXXX</Saa:X1>
</Saa:OriginalInstanceAddressee>
<Saa:ReportingApplication>SWIFTNetInterface</Saa:ReportingApplication>
<Saa:NetworkInfo>
<Saa:Priority>Normal</Saa:Priority>
<Saa:IsPossibleDuplicate>>false</Saa:IsPossibleDuplicate>
<Saa:Service>swift.generic.fast!x</Saa:Service>
<Saa:Network>SWIFTNet</Saa:Network>
<Saa:SessionNr>000083</Saa:SessionNr>
<Saa:SeqNr>000000004</Saa:SeqNr>
<Saa:SWIFTNetNetworkInfo>
<Saa:RequestType>camt.007.002.02</Saa:RequestType>
<Saa:SNLRef>SNL02016-2018-01-01T12:08:36.8976.000007Z</Saa:SNLRef>
<Saa:Reference>5d8c33e0-5ae4-4509-b6dc-813a2eafa1ef</Saa:Reference>
<Saa:SnFInputTime>0140:2018-01-01T12:10:10</Saa:SnFInputTime>
<Saa:TransferRef>SNL02013D11330601714009891C</Saa:TransferRef>
<Saa:FileStartTime>20180101173833</Saa:FileStartTime>
<Saa:FileEndTime>20180101173858</Saa:FileEndTime>
</Saa:SWIFTNetNetworkInfo>
</Saa:NetworkInfo>
<Saa:Interventions>
<Saa:Intervention>
<Saa:IntvCategory>TransmissionReport</Saa:IntvCategory>
<Saa:CreationTime>20180101173833</Saa:CreationTime>
<Saa:OperatorOrigin>SYSTEM</Saa:OperatorOrigin>
<Saa:Contents>
<AckNack>
```

```
<PseudoAckNack>{1:F21SPXAINJJAXXX000083000000004}{4:{177:1201011738}{451:0}{311:ACK}{108:AFT_FA_test1}}</PseudoAckNack>
</AckNack>
</Saa:Contents>
</Saa:Intervention>
</Saa:Interventions>
<Saa:IsRelatedInstanceOriginal>true</Saa:IsRelatedInstanceOriginal>
<Saa:MessageCreator>ApplicationInterface</Saa:MessageCreator>
<Saa:IsMessageModified>false</Saa:IsMessageModified>
<Saa:MessageFields>NoOriginal</Saa:MessageFields>
</Saa:TransmissionReport>
</Saa:Header>
</Saa:DataPDU>
```

7.10 OUT message in XML V2 for FileAct

```
_004279_____<?xml version="1.0" encoding="UTF-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:saa:xsd:saa.2.0" xmlns:Sw="urn:swift:snl:ns:Sw"
xmlns:SwInt="urn:swift:snl:ns:SwInt" xmlns:SwGbl="urn:swift:snl:ns:SwGbl"
xmlns:SwSec="urn:swift:snl:ns:SwSec">
<Saa:Revision>2.0.7</Saa:Revision>
<Saa:Header>
<Saa:Message>
<Saa:SenderReference>OSPXAINJJXXX007AFT_FA_test1$120101</Saa:SenderReference>
<Saa:MessageIdentifier>camt.007.002.02</Saa:MessageIdentifier>
<Saa:Format>File</Saa:Format>
<Saa:SubFormat>Output</Saa:SubFormat>
<Saa:Sender>
<Saa:DN>o=spxainjj,o=swift</Saa:DN>
<Saa:FullName>
<Saa:X1>SPXAINJJXXX</Saa:X1>
</Saa:FullName>
</Saa:Sender>
<Saa:Receiver>
<Saa:DN>o=spxainjj,o=swift</Saa:DN>
<Saa:FullName>
<Saa:X1>SPXAINJJXXX</Saa:X1>
</Saa:FullName>
</Saa:Receiver>
```

```
<Saa:InterfaceInfo>
<Saa:UserReference>AFT_FA_test1</Saa:UserReference>
<Saa:MessageCreator>SWIFTNetInterface</Saa:MessageCreator>
<Saa:MessageContext>Original</Saa:MessageContext>
<Saa:MessageNature>Financial</Saa:MessageNature>
</Saa:InterfaceInfo>
<Saa:NetworkInfo>
<Saa:Priority>Normal</Saa:Priority>
<Saa:IsPossibleDuplicate>>false</Saa:IsPossibleDuplicate>
<Saa:Service>swift.generic.fast!x</Saa:Service>
<Saa:Network>SWIFTNet</Saa:Network>
<Saa:SessionNr>006100</Saa:SessionNr>
<Saa:SeqNr>000000116</Saa:SeqNr>
<Saa:SWIFTNetNetworkInfo>
<Saa:RequestType>camt.007.002.02</Saa:RequestType>
<Saa:SNLRef>SNL02018-2018-01-01T12:08:36.8976.000007Z</Saa:SNLRef>
<Saa:Reference>5d8c33e0-5ae4-4509-b6dc-813a2eafa1ef</Saa:Reference>
<Saa:SnFQueueName>spxainjj_file!x</Saa:SnFQueueName>
<Saa:SnFInputTime>0140:2018-01-01T12:10:10</Saa:SnFInputTime>
<Saa:SnFDeliveryTime>2018-01-01T12:10:10Z</Saa:SnFDeliveryTime>
<Saa:TransferRef>SNL02013D11330601738010042C</Saa:TransferRef>
<Saa:StoredTransferRef>SNL02013D11330601714009891S</Saa:StoredTransferRef>
<Saa:FileStartTime>20180101173858</Saa:FileStartTime>
<Saa:FileEndTime>20180101173926</Saa:FileEndTime>
</Saa:SWIFTNetNetworkInfo>
</Saa:NetworkInfo>
<Saa:SecurityInfo>
<Saa:SWIFTNetSecurityInfo>
<Saa:SignerDN>cn=fin1spxainjj,o=spxainjj,o=swift</Saa:SignerDN>
<Saa:NRTType>SvcOpt</Saa:NRTType>
<Saa:SignatureResult>Success</Saa:SignatureResult>
<Saa:SignatureValue>
  <SwInt:RequestPayload type="swift.fileact.secsecureddata">
<Sw:FileRequestHeader>
<SwInt:Requestor>o=spxainjj,o=swift</SwInt:Requestor>
<SwInt:Responder>o=spxainjj,o=swift</SwInt:Responder>
<SwInt:Service>swift.generic.fast!x</SwInt:Service>
<SwInt:RequestType>camt.007.002.02</SwInt:RequestType>
```

```
<SwInt:Priority>Normal</SwInt:Priority>
<SwInt:RequestRef>AFT_FA_test1</SwInt:RequestRef>
</Sw:FileRequestHeader>
<Sw:TransferRef>SNL02013D11330601714009891</Sw:TransferRef>
<Sw:Digest>
<Sw:DigestAlgorithm>SHA-1</Sw:DigestAlgorithm>
<Sw:DigestValue>5iSXh3GDOdNT4cUGaOFeMhO6/og=</Sw:DigestValue>
</Sw:Digest>
</SwInt:RequestPayload>
  <SwSec:Crypto>
    <SwSec:CryptoInternal>
      <SwSec:CipherKey>UEVNRkBQcm9jLVR5cGU6IDQsTUIDLU9OTFkNCkNvbnRlbnQtRG9tYWluOiBS
      RkM4MjJINckVudHJ1c3RGaWxlLVZlcnNpb246IDluMA0KT3JpZ2luYXRvci1ETjogY249ZmluMXNweG
      FpbmpqLG89c3B4YWluamosbz1zd2lmdA0KT3JpZy1TTjogMTMwNzEzNjk2Mw0KTUIDLUlUzm86IFNI
      QTI1NiwgUINBLA0KIFpqbMZHMMWJLR3RIS25YcnI6RHBaQ0dyScTnc0pXbDNvWjNjVHRxVWdZUUIj
      WXEwMVp5YmY2ZGhPSW8xSE1SSkcNCiBON3JicW10ckdYU01idFBGajJjZytLU2FrUFNxBjYjUjYjV
      2J0SW00WjBrTGx5UVkwM2FNMVVPbHBWNEdJd3hUDQogamF4RmtTNWZvT0R4KzJjczNjcGE3Q
      VBkL2tsTy9pcTNDsgYzeFNfdEp4REZLNjG4WHNuRXFNT0tiVG12VzJOZw0KIDd5bnlyN3R2Wk0w
      azBsTzQ5aUZrUVILUk1wTGvYs3FaYzZtYktoMdbBRENiMDU5TDVYV0I4VUFwREhlazJOaFkNCiB
      WaDNTeXF1NFR4UFU5bVNjckpaRGdhYS9BaTVMS2F6QzM0aEpjRmplYjlpVm9leE9BM25EWEkxQ
      yt5OGIvWHpYDQogalZVZFP3a2tpc2NhWWcrYnhaaHV2dz09DQo=</SwSec:CipherKey>
      <SwSec:CryptoProtocol>4.0:3.0</SwSec:CryptoProtocol>
    </SwSec:CryptoInternal>
    <SwSec:CryptoInfo>
      <SwSec:MemberRef>RequestPayload</SwSec:MemberRef>
      <SwSec:SignDN>cn=fin1spxainjj,o=spxainjj,o=swift</SwSec:SignDN>
    </SwSec:CryptoInfo>
  </SwSec:Crypto>
</Saa:SignatureValue>
<Saa:FileDigestAlgorithm>SHA-1</Saa:FileDigestAlgorithm>
<Saa:FileDigestValue>5iSXh3GDOdNT4cUGaOFeMhO6/og=</Saa:FileDigestValue>
</Saa:SWIFTNetSecurityInfo>
</Saa:SecurityInfo>
<Saa:FileLogicalName>AFT_FA.JPG</Saa:FileLogicalName>
</Saa:Message>
</Saa:Header>
<Saa:Body>AFT_FA.JPG.SNL02013D11330601738010042C.ath</Saa:Body>
</Saa:DataPDU>
```

7.11 Delivery Notification message in XML V2 for FileAct

```
_004279_<?xml version="1.0" encoding="UTF-8" ?>
<Saa:DataPDU xmlns:Saa="urn:swift:saa:xsd:saa.2.0" xmlns:Sw="urn:swift:snl:ns.Sw"
xmlns:SwInt="urn:swift:snl:ns.SwInt" xmlns:SwGbl="urn:swift:snl:ns.SwGbl"
xmlns:SwSec="urn:swift:snl:ns.SwSec">
<Saa:Revision>2.0.7</Saa:Revision>
<Saa:Header>
<Saa:DeliveryNotification>
<Saa:ReconciliationInfo>SNL02013D11330601714009891C</Saa:ReconciliationInfo>
<Saa:ReceiverDeliveryStatus>RcvDelivered</Saa:ReceiverDeliveryStatus>
<Saa:MessageIdentifier>Delivery Notification</Saa:MessageIdentifier>
<Saa:InterfaceInfo>
<Saa:MessageCreator>SWIFTNetInterface</Saa:MessageCreator>
<Saa:MessageContext>Original</Saa:MessageContext>
<Saa:MessageNature>Network</Saa:MessageNature>
</Saa:InterfaceInfo>
<Saa:NetworkInfo>
<Saa:Priority>Normal</Saa:Priority>
<Saa:IsPossibleDuplicate>>false</Saa:IsPossibleDuplicate>
<Saa:Network>SWIFTNet</Saa:Network>
<Saa:SessionNr>006079</Saa:SessionNr>
<Saa:SeqNr>000000557</Saa:SeqNr>
</Saa:NetworkInfo>
</Saa:DeliveryNotification>
</Saa:Header>
<Saa:Body>
<Sw:NotifySnFRequestHandle>
<Sw:SnFRef>SNL02013D11330601714009891C</Sw:SnFRef>
<Sw:SnFRefType>FileAct</Sw:SnFRefType>
<Sw:AcceptStatus>Accepted</Sw:AcceptStatus>
<Sw:AckSwiftTime>2018-01-01T12:10:44Z</Sw:AckSwiftTime>
</Sw:NotifySnFRequestHandle>
</Saa:Body>
</Saa:DataPDU>
```

*** End of Document ***