SWIFT Certified Application

Payments

Label Criteria 2017

This document explains the business criteria required to obtain the SWIFT Certified Application - Payments 2017 label for payments applications.

27 January 2017

Table of Contents

Preface

Purpose of the document

This document explains the business criteria required to obtain the SWIFT Certified Application - Payments 2017 label for payments applications.

Audience

This document is for the following audience:

- Developers
- Development managers
- Product managers
- SWIFT customers seeking to understand the SWIFT Certified Application Programme or involved in selecting third-party applications

Related documentation

- SWIFT Certified Application Programme Overview

  The document provides an overview of the SWIFT Certified Application Programme. It describes the benefits of the programme for SWIFT registered providers that have a software application they want to certify for compatibility with SWIFT standards, messaging services, and connectivity. This document also describes the application and validation processes that SWIFT uses to check such SWIFT compatibility. SWIFT's certification of an application is not an endorsement, warranty, or guarantee of any application, nor does it guarantee or assure any particular service level or outcome with regard to any certified application.
- SWIFT Certified Application Technical Validation Guides

  The documents explain in a detailed manner how SWIFT validates the application so that this application becomes SWIFT Certified.
- Documentation (User Handbook): www.swift.com

1 SWIFT in Payments and Cash Management

Overview

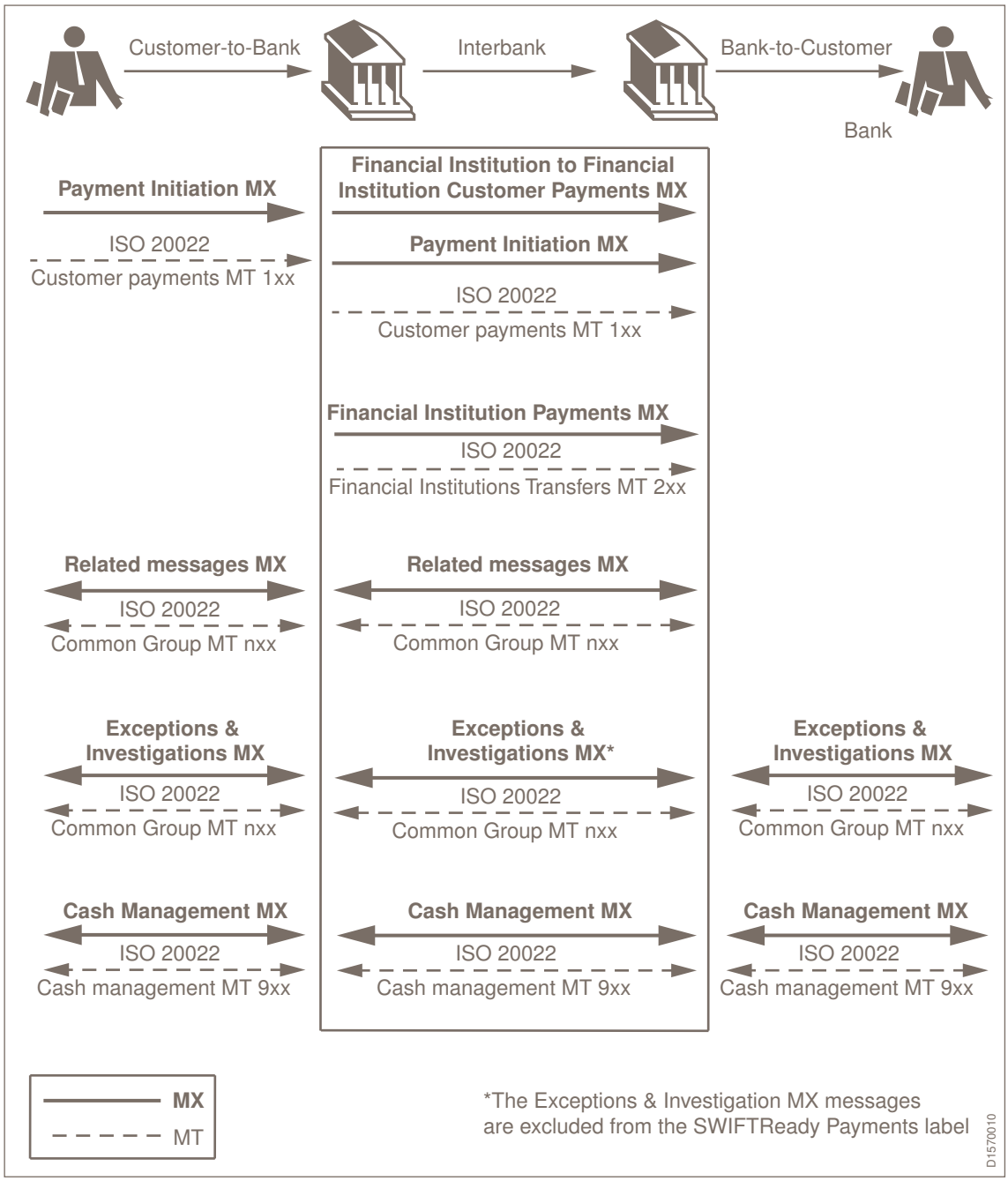
More than 60 clearing systems in the payments market rely on SWIFT. These clearing systems carry from 500 to over 300,000 payments a day. SWIFT offers the secure messaging connectivity and common message standards that are essential to smooth operations.

SWIFT offers a range of message standards to initiate and to clear and settle customer payments between the different parties in the end-to-end payments chain.

The SWIFT Certified Application - Payments label focuses on the certification of core banking or payments applications that enable the initiation, generation, processing, and settlement of interbank payments.

A related set of standards is also available to handle the following:

- Status reporting
- Exceptions and Investigations
- Account-related information exchanged between an account owner and an account servicer



FIN messages

FIN enables the exchange of messages formatted with the traditional SWIFT MT standards. FIN works in store-and-forward mode and offers extensive value-added functionality, such as message copy (FINCopy and FINInform), broadcasts, and online retrieval of previously exchanged messages.

The following ISO 20022 messages complement the traditional FIN messages:

- **pain**

  payment initiation and mandates
- **pacs**

  payment clearing and settlement
- **camt**

  cash management and exceptions and investigations

The MX messages for Exceptions and Investigations are out of scope of this label. The SWIFT Certified Application - Exceptions and Investigations Label covers these messages.

2 SWIFT Certified Application - Payments Label

Overview

The SWIFT Certified Application - Payments label focuses on the certification of core banking or payments applications that enable the initiation, generation, processing, and settlement of interbank payments. This label is awarded to business applications that adhere to a specific set of criteria linked to the support of SWIFT FIN (MT) messages and (optionally) MX messages, SWIFT connectivity, and SWIFT functionality.

Applications out of scope

The following applications are out of scope of the SWIFT Certified Application - Payments label:

- Clearing and settlement applications: Automated Clearing House (ACH) and Real-Time Gross Settlement (RTGS) applications targeted at central institutions
- Software solutions primarily reformatting business data into SWIFT-compliant messages that can be released over SWIFT, (Middleware and Enterprise Application Integrations - EAI)
- Cash management solutions that are targeted to Corporate treasurers. Vendors offering these solutions must apply for the SWIFT Certified Application for Corporates - Cash Management label.
- Exceptions and Investigations case managers. These applications must apply for the Exceptions and Investigations label.

3 SWIFT Certified Application - Payments Criteria 2017

3.1 Certification Requirements

New label

Vendors applying for the SWIFT Certified Application - Payments label for the first time must comply with all criteria as defined in this document.

Label renewal

Vendors that have been granted the SWIFT Certified Application Payments label in 2016 are required to prove compliance to the Standards Release (SR) 2017.

If the vendor has upgraded its application, then SWIFT will request details of the new functionalities that the vendor must demonstrate (for example, new functional validation required).

3.2 Installed Customer Base

Live customer reference

A minimum of five live customers must use the application.

By customer, SWIFT means a distinct financial institution that uses the product to send and receive messages over SWIFTNet.

SWIFT reserves the right to contact the relevant customer to validate the functionality of the application submitted for a SWIFT Certified Application label. A questionnaire is used as the basis for the customer validation. The questionnaire can be in the form of a telephone interview, an e-mail, or a discussion at the customer site. The information provided by the customer is treated as confidential and is not disclosed, unless explicitly agreed with the customer.

3.3 Messaging

FIN protocol

The application must support the FIN protocol (for example, message validation).

In particular, the application must be able to generate the correct FIN header, body, and trailer blocks. It must also be able to parse and act upon any incoming messages as appropriate.

FileAct and InterAct for MX messages (optional)

The support of FileAct and InterAct to transport MX payments and cash management messages is optional.

Related information

Standards on page 10

3.4 Direct Connectivity

Requirements

For direct connectivity, the vendor application must integrate with Alliance Access. A business application that does not connect directly to Alliance cannot be considered for a SWIFT Certified Application label.

The direct connection from the business application to Alliance Access can be achieved using one or more of the Alliance Access adapters:

- MQ Host Adapter (MQHA)
- Automated File Transfer (AFT)
- SOAP Host Adapter

The vendor must develop and test SWIFT application integration using Alliance Access 7.0 or 7.2. Proper support of either Alliance Access Release 7.0 or 7.2 is mandatory for the 2017 label.

Mandatory adapters

Messaging service	Standards
FIN	MT

Note *If the application supports several of the previously mentioned adapters, then the vendor may provide the appropriate evidence for some or all of them during the technical validation. SWIFT only publishes information for which evidence has been provided.*

SWIFTNet Release 7.2

A mandatory upgrade to the underlying technology behind SWIFT's interface products is planned for 2017. The aim of the release is to continue to provide a highly secure and efficient SWIFT service for our customers in the years ahead.

Note *Release 7.2 support will become a mandatory requirement in 2018. SWIFT recommends that you test, plan, and prepare for this change accordingly during the course of 2017. Customers will expect statements about your readiness soon after general availability.*

More details on the SWIFTNet Release 7.2 can be found on www.swift.com:

- Release 7.2
- User Handbook

Local Authentication (LAU)

Local Authentication provides integrity and authentication of files exchanged between Alliance Access and any application that connects through the application interface. Local Authentication requires that the sending entity and Alliance Access use the same key to compute a Local Authentication file signature. With the increased number of cyber-attacks on the financial industry, customers will expect message signing with LAU from their application providers.

Note *Although Local Authentication support is not mandatory to receive the 2017 SWIFT Certified Application label, SWIFT strongly encourages SWIFT Certified providers to plan for LAU support.*

3.5 Standards

The application must support the messages that belong to categories 1, 2 and 9, incoming or outgoing (or both), as described in FIN Messages Required for SWIFT Certified Application - Payments 2017 Label on page 18, and according to Standards Release 2017. The application must be able to support all fields and all code words, both mandatory and optional.

The application must be able to:

- generate all outgoing messages types in categories 1, 2 and 9, validate them against the related syntax and semantic rules, then route them to the SWIFT interface
- receive and parse any incoming message in these categories, and properly act upon them, according to the business transaction rules.

ISO 20022-compliant messages

Although ISO 20022 implementation is not mandatory to receive the 2017 SWIFT Certified Application - Payments label, SWIFT strongly encourages Certified Application providers to plan for ISO 20022 adoption.

Applications that support ISO 20022 must comply with the following:

- ISO 20022 Harmonisation Charter
- ISO 20022 Version and Release Management - Best Practices
- Recommendations for Implementation of ISO 20022 Messages – Best Practices

Amongst other requirements, this implies that applications must:

- support the latest or previous version of ISO 20022 messages as available
- align its maintenance cycle with the MX release cycle
- rely on the message specifications as published on MyStandards

Mandatory support of ISO 20022 for RTGS

Support of ISO I20022 standards is mandatory to support banks that are a member of an RTGS system. For more information, see the ISO 20022 Harmonisation Charter and the SWIFT Certified Application - RTGS Application Label Criteria.

The ISO 20022 messages are listed ISO 20022 Messages Optional for SWIFT Certified Application - Payments 2016 Label on page 20.

3.6 Message Reconciliation

SWIFT validates messages at different levels and provides notifications related to the validation and transmission results of the messages sent. The application must capture these notifications and ensure technical reconciliation, error handling, repair, and retransmission where appropriate.

3.7 Message Validation

FIN central services validate every FIN message against syntax and semantic rules. The central system rejects messages that do not pass validation, which incurs substantial cost for SWIFT users. To avoid this, vendor applications must provide the same level of validation on the generated messages as the FIN central services do.

The vendor application must build and validate all messages according to the message format and field specifications described in the Standards Release 2017 for Category 1, 2 and 9 messages. In addition, the application must ensure that outgoing messages comply with the following rules and the guidelines described in the *Standards MT Message Reference Guides*:

- Network validated rules
- Usage Rules
- Straight-through processing (STP) guidelines
- Standards Usage Guidelines

Typical rules that are checked during certification for the MT 103 include:

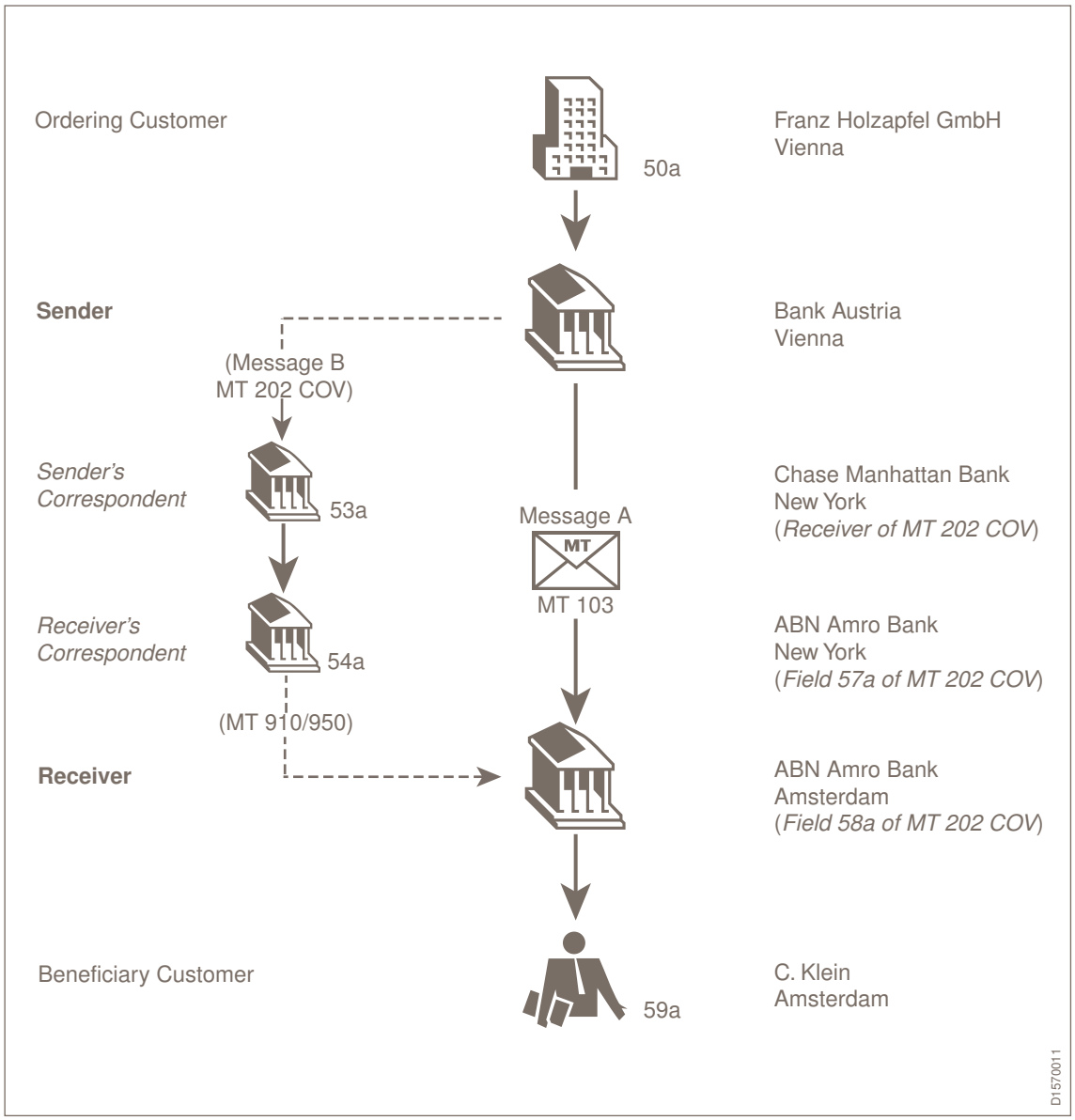
- Field 33B Instructed Currency and Amount: used when the currency and amount are different from those specified in field 32B.
- Field 36 Exchange Rate: must be present when a currency conversion or an exchange has been performed on the Sender's side.
- Field 77T Extended Remittance Information: can only be used if both the Sender and the Receiver of the message have subscribed to the Extended Remittance Information Message User Group (MUG). If the field is used, then the Sender must set the validation flag to REMIT in field 119 of the user header of the message. If field 77T is not present, then the code of the validation flag must not be REMIT.

The 2017 Standards Release becomes effective in November 2017, but SWIFT expects the vendor to provide adequate testing time to its customers before these messages go live.

3.8 Business Workflow

The application must be able to automatically generate correct MTs when an event occurs or when a user manually enters an event.

Whenever possible, subsequent messages must be generated automatically. For example, if an outgoing MT 103 contains field 53A (Sender's Correspondent), then an MT 202/MT 205 COV must be generated automatically mapping the necessary information, references, and fields into the cover payment message. This is illustrated in the following information flow.



The application must be able to do the following:

- Receive incoming messages and to process them according to predefined rules

  The messages must be passed on to the accounting system or to the next processing module or application in the chain if additional processing is needed.
- Automatically populate (whenever possible) and generate Common Group Messages. For example, if an incoming message requires a query message to be sent, then the user must have the possibility to ask the system to generate an MT n95 (Query).
- Populate the query with the respective references of the original transaction and provide a mechanism to copy the original message, if required

3.9 User Interface

The application must have a manual entry, display, and repair capability for the MTs (and, optionally the MXs) listed previously. For more information, see Standards on page 10.

Message entry

The application must make it possible for a user to manually input or modify the MT messages, by offering normalised fields for input (independent of the underlying syntax and business meaning).

Message repair

The application must validate the user data input at field level and must flag any invalid entry, prompting the user to correct the input. This includes, but is not limited to, flagging mandatory fields.

User profile management

The application must provide a user profile management functionality to ensure that only authorised users can perform specific tasks.

The vendor must demonstrate the following:

- how its application handles user profile creation, update, and deletion
- that access is denied or an operation is refused if a user is not entitled to perform this operation
- that the application supports the "four eyes principle" by showing that a specific operation (for example, payment initiation or validation of certain fields) requires a second person to validate it before execution

4 Reference Data Integration

The application must support the directories that are documented in this section.

Optional directories are clearly identified as such.

4.1 BIC Directory

Overview

The application must provide access to the BIC Directory (or the eventual replacements of the BIC Directory: BIC Plus or BIC Directory 2018) both for message validation and as a look-up function in the message creation and message repair stations.

It is the responsibility of directory subscribers at all times to make sure that they use the latest version of the BIC Directory. As such, SWIFT expects the application to support the BIC Directory monthly update in an efficient manner without disrupting customer operations.

Retrieval functionality during message composition

The BICs contained in the BIC Directory, BIC Plus, and BIC Directory 2018 can be used in various fields of the SWIFT messages. The absence of BICs in these fields is one of the major obstacles to straight-through processing (STP) and causes manual intervention on the recipient side. SWIFT expects vendors to provide an integrated interface within their application to make it possible for users to retrieve and input correctly formatted BICs into the proper fields.

Search functionality

The user must be able to enter a number of search criteria, such as bank name or address, to perform a search, and to get a list of results. From this result window, the user must be able to select the required BICs and copy these into the different bank identifier fields of the message (that is, the transaction).

If the search criteria return no results, then the user must be alerted that no BIC is available. If the user manually enters an invalid BIC, then the application must send an alert notifying the user that this BIC is not valid.

Available format and delivery

Flat file in XML or TXT format.

Delivery

The BIC Directory, BIC Plus, and BIC Directory 2018 are downloadable in a manual or automated manner from the SWIFTRef Access Point in full and delta versions. Upon request, they can also be delivered through FileAct.

The BIC Directory, BIC Plus, and BIC Directory 2018 must either be copied into the application repository system or stored in the back office for access by the vendor application through a defined interface.

4.2 Bank Directory Plus

Content

Bank Directory Plus contains the following information:

- All BIC11s from the ISO registry (more than 200 countries), from connected and non-connected financial institutions and corporates active on FIN, FileAct, and/or InterAct.
- All LEI (Legal Entity Identifier) from the endorsed LOUs (Local Operating Units).
- Name and address details for each BIC
- FIN service codes
- National clearing codes (160+ countries), including CHIPS, TARGET, and EBA data. For a limited number of countries (10+), national codes are also provided with name and address in local language (for example, China, Japan, Russia).
- Bank hierarchy information
- Country, currency, and holiday information
- Timezone information

Available formats

Flat file in XML or TXT format

Delivery

The Bank Directory Plus is downloadable in a manual or automated manner from the SWIFTRef Access Point in full and delta versions. Upon request it can also be delivered through FileAct.

4.3 IBAN Plus

Content

The IBAN Plus directory contains the following information:

- IBAN country formats
  - IBAN country prefix
  - IBAN length
  - Bank code length, composition, and position within the IBAN
- Institution name and country
- Institution bank and branch codes in the formats as embedded in IBANs
- Institution BICs as issued together with the IBANs to the account holders
- Data for the SEPA countries and the non-SEPA countries that adopted the IBAN
- Updates to the file when new IBAN country formats are registered with SWIFT in its capacity as the ISO IBAN registry

The directory is ideal for accurate derivation of BIC from IBAN, covering 68 IBAN countries (including all SEPA countries).

Available formats

Flat file in XML or TXT format

Delivery

The IBAN Plus is downloadable in a manual or automated manner from the SWIFTRef Access Point in full and delta versions. Upon request it can also be delivered through FileAct.

4.4 SWIFTRef Business Applications

Introduction

SWIFTRef offers a portfolio of reference data products and services. Data is maintained in a flexible relational database and accessible in a choice of formats and delivery channels matched to business needs.

Purpose

Application vendors are able to access BICs, National bank/Sort codes, IBAN data, payment routing data (including SEPA and other payment systems), Standard Settlement Instructions (SSIs), LEIs, MICs (Market Identification Codes), BRNs (Business Registration Numbers), GIINs (Global Intermediary Identification Numbers), and more. Through SWIFTRef, vendors can ensure that their applications support the most accurate and up-to-date reference and entity data for smooth payments initiation and processing.

Related information

Additional information about SWIFTRef for application vendors is available on swiftref.swift.com/swiftref-business-applications.

5 Marketing and Sales

Requirements

In order to maximise the business value of the SWIFT Certified Application - Payments label, collaboration between SWIFT and the vendor is expected. More specifically, the vendor must provide SWIFT, under a non-disclosure agreement, with the following information:

- A list of customers actively using the application in a SWIFT context

  The list must contain the institution name, location, and an overview of the integration scope (domain, features, and sites) for the current and previous year.
- A list of all customers active in the financial sector
- A product roadmap for 2017 and 2018 containing the plans for further developments, SWIFT support, and new releases
- A complete set of documentation, including feature overview, SWIFT adapters, workflow engine capability, and user manuals

In addition, the vendor must dedicate a page of their web site to describe the SWIFT Certified Application used in a SWIFT context.

A FIN Messages Required for SWIFT Certified Application - Payments 2017 Label

A.1 Incoming and Outgoing MT Messages

Mandatory/ Optional	MT	MT Name	Incoming	Outgoing
O	101	Request For Transfer	✓	✓
M	102 102+	Multiple Customer Credit Transfer	✓	✓
M	103 103+	Single Customer Credit Transfer	✓	✓
O	103 REMIT	Single Customer Credit Transfer	✓	✓
O	104	Direct Debit and Request for Debit Transfer Message	✓	✓
O	105	EDIFACT Envelope	✓	✓
O	107	General Direct Debit Message	✓	✓
O	110	Advice of Cheque(s)	✓	✓
O	111	Request for Stop Payment of a Cheque	✓	✓
O	112	Status of a Request for Stop Payment of a Cheque	✓	✓
M	200	Financial Institution Transfer for its Own Account	✓	✓
M	201	Multiple Financial Institution Transfer for its Own Account	✓	✓
M	202	General Financial Institution Transfer	✓	✓
M	202 COV	General Financial Institution Transfer	✓	✓
M	203	Multiple General Financial Institution Transfer	✓	✓
O	204	Financial Markets Direct Debit Message	✓	✓
M	205	Financial Institution Transfer Execution	✓	✓
M	205 COV	Financial Institution Transfer Execution	✓	✓
O	207	Request for Financial Institution Transfer	✓	✓
M	210	Notice to Receive	✓	✓

Mandatory/ Optional	MT	MT Name	Incoming	Outgoing
O	256	Advice of Non-Payment of Cheques	✓	✓
M	900	Confirmation of Debit	✓	✓
M	910	Confirmation of Credit	✓	✓
O	920	Request Message	✓	✓
O	935	Rate Change Advice	✓	✓
O	940	Customer Statement Message	✓	✓
O	941	Balance Report	✓	✓
O	942	Interim Transaction Report	✓	✓
O	950	Statement Message	✓	✓
O	970	Netting Statement	✓	✓
O	971	Netting Balance Report	✓	✓
O	972	Netting Interim Statement	✓	✓
O	973	Netting Request Message	✓	✓
O	985	Status Enquiry	✓	✓
O	986	Status Report	✓	✓
M	n90	Advice of Charges, Interest and Other Adjustments	✓	✓
M	n91	Request for Payment of Charges, Interest and Other Expenses	✓	✓
M	n92	Request for Cancellation	✓	✓
M	n95	Queries	✓	✓
M	n96	Answers	✓	✓
M	n98	Proprietary Message	✓	✓
M	n99	Free Format Message	✓	✓

B ISO 20022 Messages Optional for SWIFT Certified Application - Payments 2016 Label

B.1 Payments Clearing and Settlement (pacs)

Message Name	Message ID (XML Schema)
FIToFIPaymentStatusReportV07	pacs.002.001.07
FIToFICustomerDirectDebitV06	pacs.003.001.06
PaymentReturnV06	pacs.004.001.06
FIToFIPaymentReversalV06	pacs.007.001.06
FIToFICustomerCreditTransferV06	pacs.008.001.06
FinancialInstitutionCreditTransferV06	pacs.009.001.06
FinancialInstitutionDirectDebitV02	pacs.010.001.02

B.2 Cash Management (camt)

Message Name	Message ID (XML Schema)
BankToCustomerAccountReportV06	camt.052.001.06
BankToCustomerStatementV06	camt.053.001.06
BankToCustomerDebitCreditNotificationV06	camt.054.001.06
AccountReportingRequestV03	camt.060.001.03
NotificationToReceiveV05	camt.057.001.05
NotificationToReceiveCancellationAdviceV05	camt.058.001.05
NotificationToReceiveStatusReportV05	camt.059.001.05
RequestToModifyPaymentV03	camt.087.001.03
CustomerPaymentCancellationRequestV05	camt.055.001.05
FIToFIPaymentCancellationRequestV05	camt.056.001.05
ResolutionOfInvestigationV06	camt.029.001.06

Message Name	Message ID (XML Schema)
AdditionalPaymentInformationV06	camt.028.001.06

B.3 Payment Initiation (pain)

Message Name	Message ID (XML Schema)
CustomerCreditTransferInitiationV07	pain.001.001.07
CustomerPaymentStatusReportV07	pain.002.001.07
CustomerPaymentReversalV06	pain.007.001.06
CustomerDirectDebitInitiationV06	pain.008.001.06

B.4 Mandates

Message Name	Message ID (XML Schema)
MandateInitiationRequestV04	pain.009.001.04
MandateAmendmentRequestV04	pain.010.001.04
MandateCancellationRequestV04	pain.011.001.04
MandateAcceptanceReportV04	pain.012.001.04

Legal Notices