Service

Partner Programme

SWIFT Certified Application - Payments

Label Criteria 2015

This document explains the business criteria required to obtain the SWIFT Certified Application - Payments 2015 label for payments applications.

30 January 2015

Table of Contents

Preface

Purpose of the document

This document explains the business criteria required to obtain the SWIFT Certified Application - Payments 2015 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.

- User Handbook: www.swift.com > Support > Resources > Documentation

1 SWIFT in Payments and Cash Management

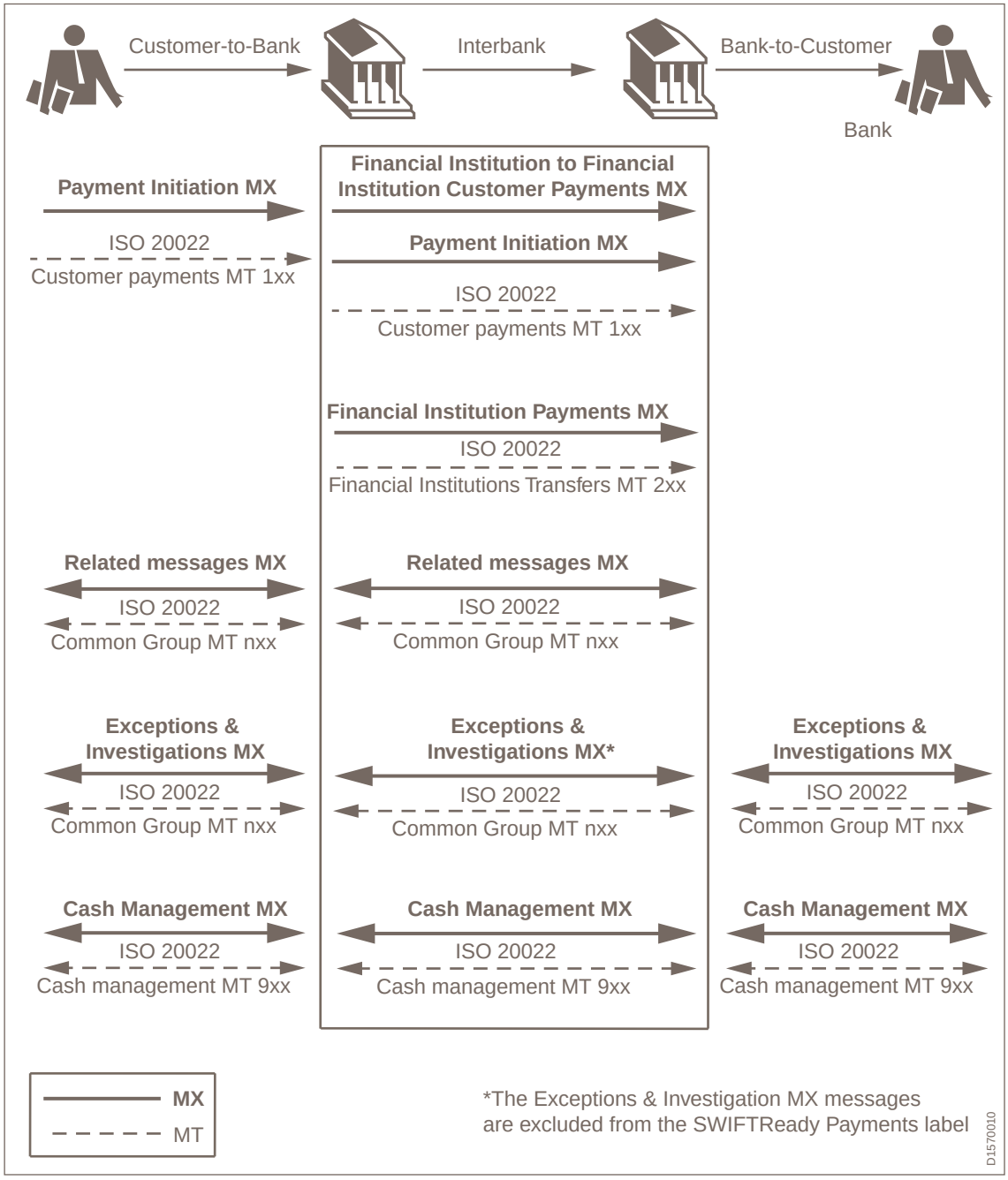
Overview

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.

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 2015

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 2014 are required to prove compliance to the Standards Release (SR) 2015.

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

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 FIN 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

The application must support the FIN protocol.

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. For more information, see the list in "Standards" on page 10.

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

3.4 Connectivity

3.4.1 Direct Connectivity

The vendor must be able to connect its application to SWIFT directly through one of the available Alliance interface adapters.

A business application that does not connect directly to Alliance cannot be considered for a SWIFT Certified Application label.

Requirements

For direct connectivity, the vendor application must integrate with Alliance Access.

The direct connection from the business application to Alliance Access can be achieved using one 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. Proper support of Alliance Access 7.0 is mandatory for the 2015 label.

The SWIFT Certified Application - Payments label requires support for either Automated File Transfer (AFT) or an interactive link with MQ Host Adapter (MQHA) or SOAP.

Mandatory adapters

Messaging service	Standards	Interface	Mandatory adapter
FIN	MT	Alliance Access 7.0	AFT or MQHA or SOAP

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.

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.

Note Local Authentication support will become a mandatory requirement in 2016. SWIFT recommends that you prepare for this change accordingly.

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 2015 Label" on page 18, and according to Standards Release 2015. 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.

Although ISO 20022 implementation is not mandatory to receive the 2015 SWIFT Certified Application label, SWIFT strongly encourages SWIFT Certified Application providers to plan for ISO 20022 adoption when relevant for their customer base. The ISO 20022 messages are listed "ISO 20022 Messages Optional for SWIFT Certified Application - Payments 2015 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 2015 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.

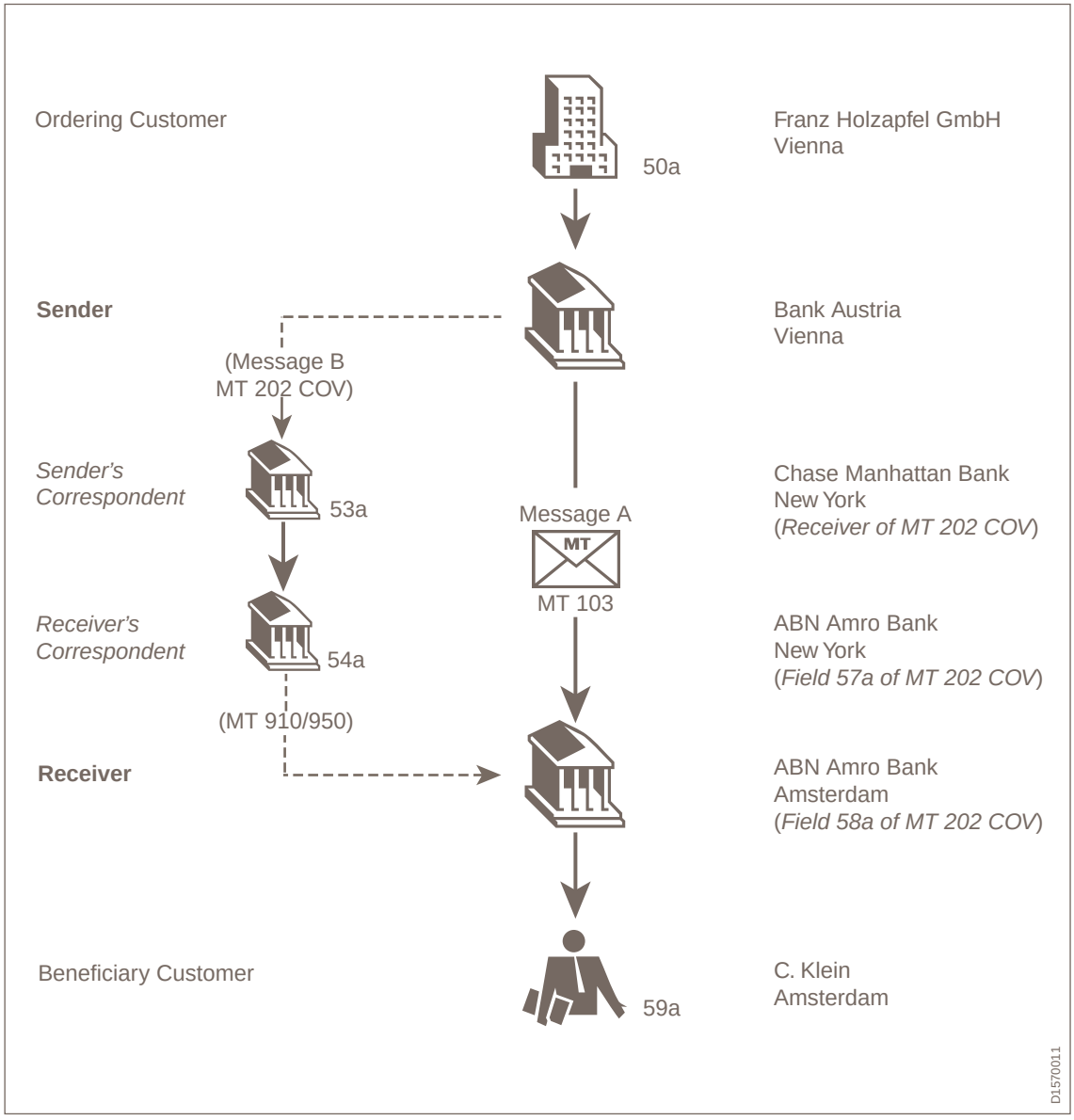
- Field 77T Extended Remittance Information: can only be used if both the Sender and the Receiver of the message have subscribed to the Extended Remittance Information Message User Group (MUG). If the field is used, then the Sender must set the validation flag to REMIT in field 119 of the user header of the message. If field 77T is not present, then the code of the validation flag must not be REMIT.

The 2015 Standards Release becomes effective in November 2015, 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) requires a second person to validate it before execution

4 Reference Data Integration

Introduction

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 both for message validation and as a look-up function in the message creation and message repair stations.

It is the responsibility of 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 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 location, to perform a search, and to get a list of results. From this result window, the user must be able to select the correspondent BIC and copy it into 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 a non-existent BIC, then the application must send an alert notifying the user that this BIC is not valid.

Available format and delivery

The BIC Directory is downloadable on www.swift.com in full or delta versions. It 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 BIC-11 codes from the ISO registry (more than 200 countries), from connected and non-connected financial institutions and corporates.
- Name and address details for each BIC
- FIN service codes
- National clearing codes, including CHIPS, TARGET, and EBA data

- Bank hierarchy information
- Payment system routing data
- Country, currency, and holiday information

Available formats

Flat file in XML or TXT format

Delivery

A version of the Bank Directory Plus tailored to SAP systems is available. **Bank Directory for SAP™** combines in one file the complete set of bank codes and BICs for SEPA and non-SEPA countries. It is optimised for easy and fast set-up and maintenance of a bank master data table on the SAP/ERP system.

The file is also downloadable from the SWIFTRef download portal, which is available from the SWIFTRef access point.

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

Available formats

Flat file in XML or TXT format

Delivery

The file is downloadable from the SWIFTRef download portal, which can be accessed from the SWIFTRef access point.

4.4 SWIFTRef Suite

Introduction

SWIFTRef offers a suite of global payments reference data services. These services are housed and maintained in a flexible relational database and accessible in a choice of formats and delivery channels matched to the business needs.

Purpose

Vendors are able to access all the Standard Settlement Instructions, BICs, national bank codes, IBAN information, routing directories (SEPA and other payment systems) and more through SWIFTRef. Vendors can be sure that the data is up-to-date, comprehensive, and consistent with all related payments reference data sets on the platform.

Related information

Additional information about SWIFTRef is available on swiftref.swift.com.

5 Marketing and Sales

Requirements

In order to maximise the business value of the SWIFT Certified Application for Corporates - 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 2015 and 2016 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.

Appendix A

FIN Messages Required for SWIFT Certified Application - Payments 2015 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	✓	✓
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	✓	✓

Mandatory/ Optional	MT	MT Name	Incoming	Outgoing
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	✓	✓

Appendix B

ISO 20022 Messages Optional for SWIFT Certified Application - Payments 2015 Label

B.1 Payments Clearing and Settlement (pacs)

Message Name	Message ID (XML Schema)
FIToFIPaymentStatusReportV06	pacs.002.001.06
FIToFICustomerDirectDebitV05	pacs.003.001.05
PaymentReturnV05	pacs.004.001.05
FIToFIPaymentReversalV05	pacs.007.001.05
FIToFICustomerCreditTransferV05	pacs.008.001.05
FinancialInstitutionCreditTransferV05	pacs.009.001.05

B.2 Cash Management (camt)

Message Name	Message ID (XML Schema)
BankToCustomerAccountReportV05	camt.052.001.05
BankToCustomerStatementV05	camt.053.001.05
BankToCustomerDebitCreditNotificationV05	camt.054.001.05
AccountReportingRequestV03	camt.060.001.03
NotificationToReceiveV04	camt.057.001.04
NotificationToReceiveCancellationAdviceV04	camt.058.001.04
NotificationToReceiveStatusReportV04	camt.059.001.04
RequestToModifyPaymentV02	camt.087.001.02
CustomerPaymentCancellationRequestV04	camt.055.001.04
FIToFIPaymentCancellationRequestV04	camt.056.001.04
ResolutionOfInvestigationV05	camt.029.001.05

B.3 Payment Initiation (pain)

Message Name	Message ID (XML Schema)
CustomerCreditTransferInitiationV06	pain.001.001.06
CustomerPaymentStatusReportV06	pain.002.001.06
CustomerPaymentReversalV05	pain.007.001.05

Message Name	Message ID (XML Schema)
CustomerDirectDebitInitiationV05	pain.008.001.05

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