SWIFT Certified Application

RTGS Application

Label Criteria 2017

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

Audience

This document is for the following audience:

- Application product Managers
- Developers
- SWIFT customers seeking to understand the SWIFT Certified Application Programme or involved in the selection of 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) on www.swift.com

1 SWIFT for the Real-Time Gross Settlement System (RTGS)

More than 80 High Value Payment Market Infrastructures (HVPMI) worldwide rely on SWIFT. These HVPMI 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 (FIN MT and InterAct MX) to initiate 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
- account-related information exchanged between an account owner and an account servicer

SWIFT WebAccess and FileAct

SWIFT offers a highly secure and reliable channel called SWIFT WebAccess. With SWIFT WebAccess, HVPMI can offer web applications to all SWIFTNet users for monitoring business activities such as the account balances, queued payments, exceptions and errors, and liquidity management.

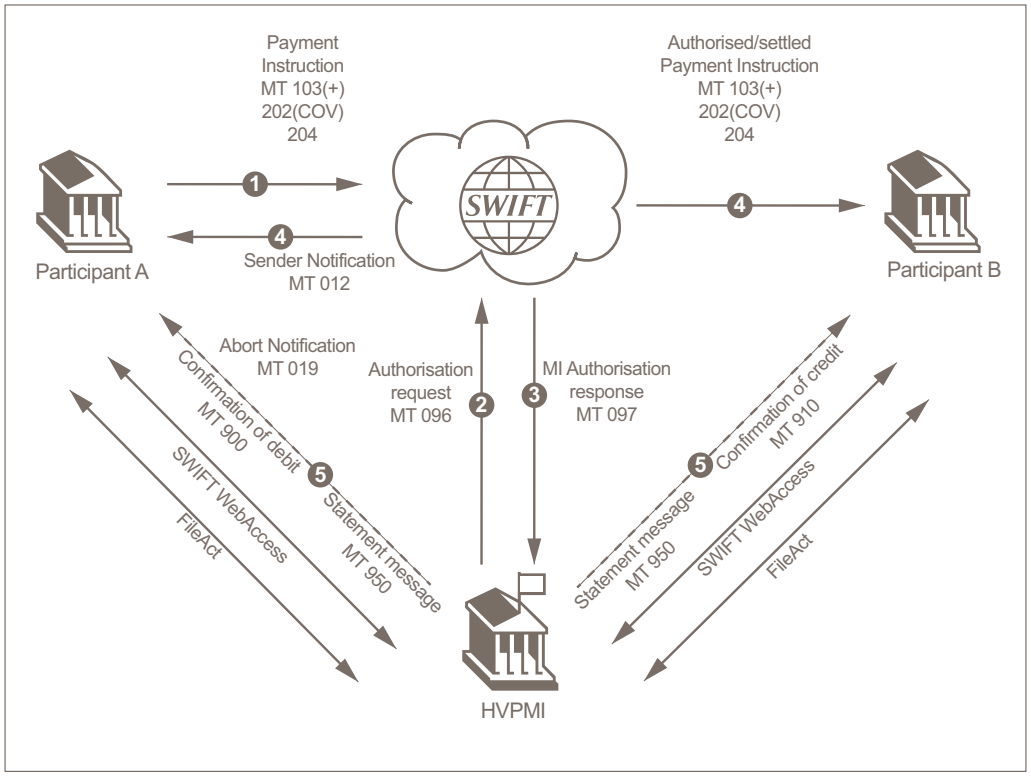
To complement this offering, FileAct allows secure and reliable transfer of files. FileAct is typically used to exchange batches of large reports such as operational and statistical reports, user directories, and reference data.

An HVPMI can choose four options grouped in two main categories: Y-Copy and V-shape.

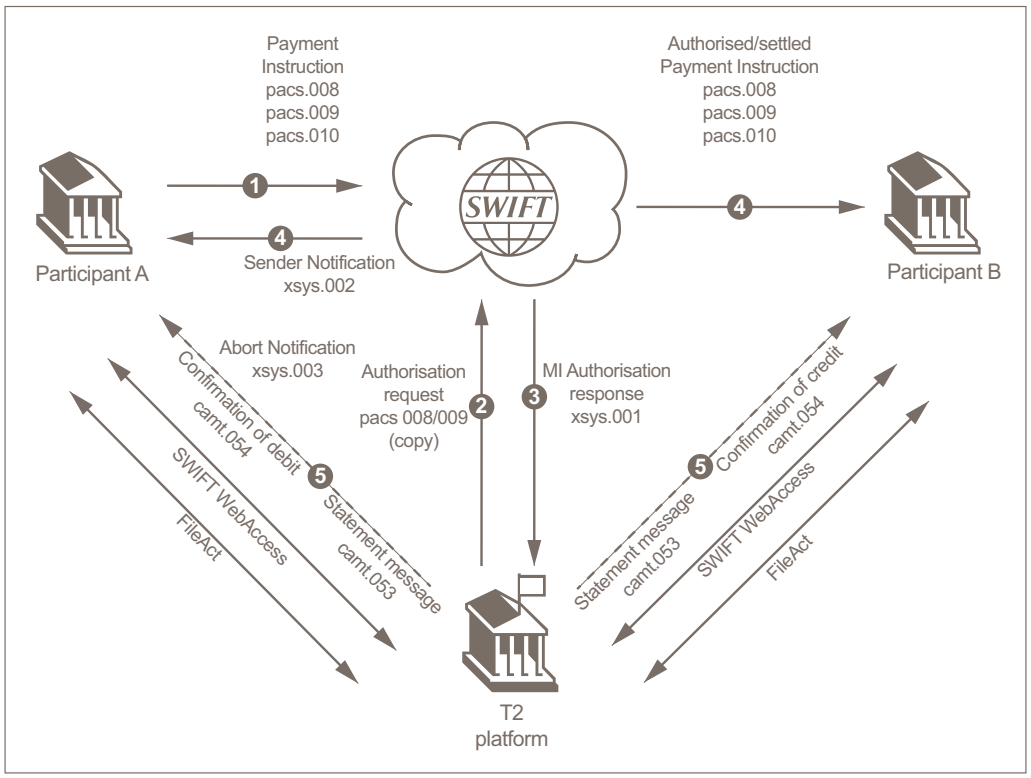
Y-Copy

A normal message is transmitted directly from the sender to the receiver. When a message is sent using FINCopy or SWIFTNet copy, selected fields are copied to the HVPMI. Partial or full copy are available for FIN. SWIFTNet copy currently supports full copy. Y-Copy mode allows a copy destination (the HVPMI) to receive a copy of all (or part) of a message and to authorise or prevent its delivery to the addressee.

Y-Copy RTGS flows with FINCopy and MT



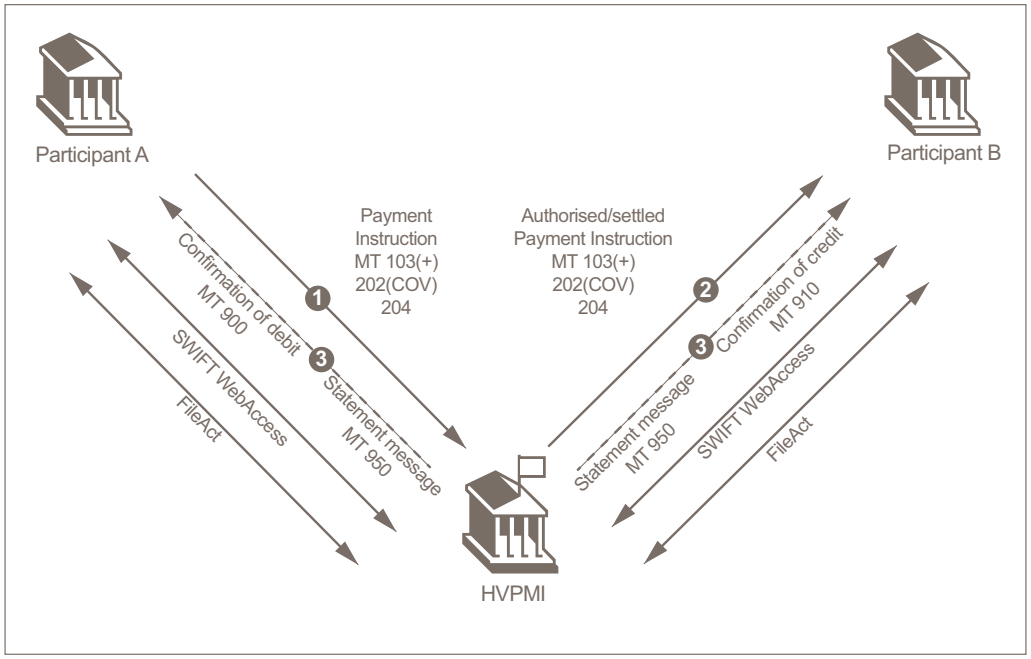
Y-Copy RTGS flows with SWIFTNet Copy and ISO 20022



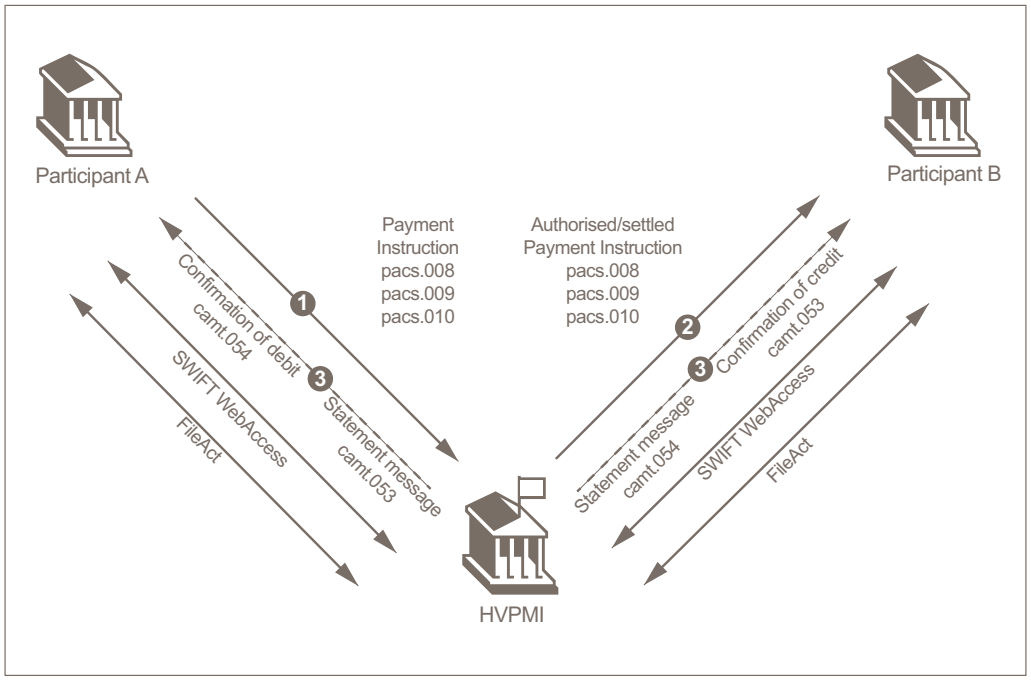
V-shape

The sender bank sends its payment instruction to the HVPMI which clears and settles it before forwarding it to the receiving Bank.

V-shape RTGS flows with FIN MT



V-shape RTGS flows with SWIFTNet and ISO 20022



2 SWIFT Certified Application - RTGS Application Label

The SWIFT Certified Application - RTGS Application label focuses on the certification of the core RTGS application that enables the initiation, generation, processing, and settlement of high value or urgent 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 MX messages, SWIFT connectivity, and SWIFT functionality. The support of FileAct and SWIFT WebAccess is optional.

This label aims to ensure that RTGS Application providers meet well-defined requirements related to SWIFT standards, messaging, and connectivity. This label validates the capability of an application to provide automation in a SWIFT environment for:

- FIN (in Y-Copy and V-shape)
- InterAct in store-and-forward mode (in Y-Copy and V-shape)
- SWIFT WebAccess (optional)
- FileAct (optional)

This label provides transparency to the end users and enables them to make well-informed purchasing decisions. SWIFT certification is frequently listed as a requirement in RFPs for financial applications.

Applications out of scope

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

- Clearing applications: Automated Clearing House (ACH)
- Core banking application
- Software solutions primarily reformatting business data into SWIFT-compliant messages that can be released over SWIFT
- 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. For more information, see www.swift.com.
- Exceptions and Investigations case managers. These applications must apply for the Exceptions and Investigations label. For more information, see www.swift.com.

3 SWIFT Certified Application RTGS Application Criteria 2017

3.1 Certification Requirements

New label

Vendors applying for the SWIFT Certified Application - RTGS Application 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 RTGS Application label in 2016 are required to prove compliance with 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 one live customer must use the application.

By customer, SWIFT means a distinct High Value Payments Market Infrastructure that uses the product to send and receive messages over SWIFT.

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. 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 Standards on page 11.

InterAct store-and-forward protocol

The application must support the InterAct in store-and-forward mode protocol. In particular, the application must be able to generate the correct InterAct header and payload (business application header and document). It must also be able to parse and act upon any incoming messages as appropriate. For more information, see Standards on page 11.

FileAct (optional)

FileAct can be used by the RTGS application for a variety of flows to securely send files, including the following:

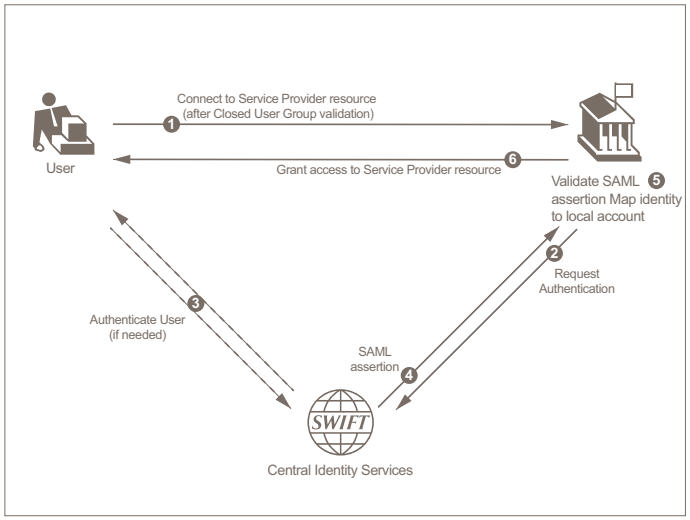
- ad-hoc or scheduled (for example, end of day) automated reports to participants (for example: transaction overviews, audit logs, and transaction copies)
- information exchange with ancillary systems
- regulatory reporting

SWIFT WebAccess (optional)

SWIFT WebAccess provides a highly secure and reliable screen-based channel over SWIFT. Users of the RTGS application can use SWIFT WebAccess to securely monitor their business activities such as account balances, queued payments and liquidity management, and to handle manually exceptions and errors.

The application must support SWIFT WebAccess by being able to integrate with SWIFT WebAccess. It must be able to generate requests to and process responses from the central identity services using the SAML protocol for the purpose of authenticating users and optionally processing non-repudiable transactions.

Connecting to Web server over WebAccess



1. Web server connection requested
2. Authentication requested
3. User authenticated
4. Authentication confirmed
5. Authentication response validated
6. Web server access granted

For more information, see the User Handbook.

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.

The SWIFT Certified Application - RTGS Application 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
InterAct in store-and-forward mode	MX	Alliance Access 7.0 or 7.2	AFT or MQHA or SOAP
FIN	MT	Alliance Access 7.0 or 7.2	AFT or MQHA or SOAP
FileAct in store-and-forward mode	Any	Alliance Access 7.0 or 7.2	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.*

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

MT

The application must support the messages in the following table that belong to categories 0, 1, 2, and 9 (incoming and outgoing), and according to Standards Release 2017. The application must support all fields and all code words, both mandatory and optional.

The application must be able to do the following:

- generate all outgoing messages types in categories 0, 1, 2, and 9 (listed in the following table), 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

FIN Messages Required for SWIFT Certified Application – RTGS Application 2017 Label

Mandatory/ Optional	MT	MT Name	Incoming	Outgoing
M	103 103+	Single Customer Credit Transfer	✓	✓
M	200	Financial Institution Transfer for its Own Account	✓	✓
M	202	General Financial Institution Transfer	✓	✓
M	202 COV	General Financial Institution Transfer	✓	✓
M	204	Financial Markets Direct Debit Message	✓	✓
M	900	Confirmation of Debit		✓
M	910	Confirmation of Credit		✓
M	940	Customer Statement Message	✓	✓
M	941	Balance Report		✓
M	942	Interim Transaction Report		✓
M	950	Statement Message		✓

Mandatory/ Optional	MT	MT Name	Incoming	Outgoing
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	✓	✓
M	96	Authorization request	✓	
M	97	Authorization response		✓

MX

The application must support the messages that belong to the categories pacs, camt, and xsys (incoming and outgoing), as listed in ISO 20022 Messages for SWIFT Certified Application – RTGS Application 2017 Label on page 12 and according to the HVPS Global Market Practice.

In addition, the application must comply with the best practice principles for ISO 20022 implementations, as outlined in the ISO 20022 Harmonisation Charter for Market Infrastructures.

This implies that the applications must do the following:

- be in line with global market practice for the HVP market as mentioned previously
- support the latest or previous version of pacs and camt messages as available
- align its maintenance cycle with the MX release cycle, which will be same as FIN cycle as from 2016
- rely on the message specifications as published by the MI on MyStandards

The application must be able to do the following:

- generate all outgoing messages types described in the following tables, 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 Messages for SWIFT Certified Application – RTGS Application 2017 Label

Payments Clearing and Settlement (pacs)

Mandatory/ Optional	Message Name	Message ID (XML Schema)	Incoming	Outgoing
M	Payment Return	pacs.004.001.05	✓	✓
M	FIToFICustomerCreditTransferV05	pacs.008.001.05	✓	✓

Mandatory/ Optional	Message Name	Message ID (XML Schema)	Incoming	Outgoing
M	FinancialInstitutionCreditTransferV05	pacs.009.001.05	✓	✓
M	Financial Institution Direct Debit V01	pacs.010.001.01	✓	✓

Cash Management (camt)

Mandatory/ Optional	Message Name	Message ID (XML Schema)	Incoming	Outgoing
M	ResolutionOfInvestigation	camt.029.001.05		✓
M	BankToCustomerAccountReport	camt.052.001.05		✓
M	BankToCustomerStatementV05	camt.053.001.05		✓
M	BankToCustomerDebitCreditNotificationV05	camt.054.001.05		✓
M	FIToFIPaymentCancellationRequest	camt.056.001.04	✓	

System messages (xsys)

Mandatory/ Optional	Message Name	Message ID (XML Schema)	Incoming	Outgoing
M	Y-Copy Authorisation or refusal	xsys.001		✓

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

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.

The vendor application must build all messages according to the message format and field specifications described in the Standards Release 2017 for Category 0,1, 2, and 9 messages (that is, in line with network validation and usage rules).

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:

- Straight-through processing (STP) guidelines
- Standards Usage Guidelines

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.

InterAct in Store-and-forward Mode

InterAct in store-and-forward mode central services validate every message against syntax and semantic rules. The central system rejects messages that do not pass validation, which incurs substantial cost for SWIFT users.

The vendor application must build and validate all messages according to the message format and field specifications described in the ISO20222 for High-Value Payments Usage Guidelines for pacs and camt messages, available on MyStandards.

3.8 User Interface

The application must have a manual entry, display, and repair capability for the MTs and the MXs listed in Standards on page 11.

Message entry

The application must make it possible for a user to manually input or modify the MT and MX 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.

A version of the Bank Directory Plus tailored to SAP systems is available. **Bank Directory for SAP™** includes 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

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 - RTGS Application 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.

Legal Notices

Copyright

Restricted Distribution

Do not distribute this publication outside your organisation unless your subscription or order expressly grants you that right, in which case ensure you comply with any other applicable conditions.

Disclaimer

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 and binding version.

Trademarks

SWIFT is the trade name of S.W.I.F.T. SCRL. The following are registered trademarks of SWIFT: the SWIFT logo, SWIFT, SWIFTNet, Accord, Sibos, 3SKey, Innotribe, the Standards Forum logo, MyStandards, and SWIFT Institute. Other product, service, or company names in this publication are trade names, trademarks, or registered trademarks of their respective owners.