SWIFT Certified Application

CSDs and Securities Market Infrastructures

Label Criteria 2018

This document explains the criteria required to obtain the SWIFT Certified Application - CSDs and Securities Market Infrastructures 2018 label for your business application.

26 January 2018

Table of Contents

Preface

Purpose of the document

This document explains the business criteria required to obtain the SWIFT Certified Application - CSDs and Securities Market Infrastructures 2018 label.

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 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 CSDs, ICSDs, and Securities Market Infrastructures

More than 80 Central Securities Depositories (CSDs) and International Securities Depositories (ICSDs) use SWIFT to support securities processing, using settlement and reconciliation, asset servicing, collateral management or funds messages.

Overall, messaging to and from CSDs and ICSDs represented close to 1 billion messages in 2017. This amounts to almost 30 percent of all securities messages over SWIFT FIN.

SWIFT offers the range of message standards (FIN, MT, and InterAct MX) to support CSDs and Securities Market Infrastructures (SMIs) activities with their different counterparties (such as participants, other market infrastructures, and agents) to manage their securities operations end-to-end along the securities chain.

Moreover, SWIFT offers a highly secure and reliable channel called SWIFT WebAccess, which allows CSDs to offer web applications to all SWIFTNet users. SWIFT WebAccess allows users to monitor business activities such as the account balances, to enter urgent instructions manually, and to manage exceptions and errors.

During the last few years, CSDs and securities market infrastructures such as T2S (TARGET2-Securities), JASDEC, and DTCC also started to lead the trend towards the adoption of ISO 20022 messages in their respective markets. This trend is now confirmed and close to 100 ISO 20022 projects are in the pipeline within CSDs and Securities Markets Infrastructures (SMIs) communities for the next 5 years.

This led to the creation of the ISO 20022 Harmonisation Charter, which is supported by all major securities infrastructures. The charter defines the principles for a harmonised, coordinated, and efficient roll out of ISO 20022 throughout the industry.

Although ISO 20022 implementation is not mandatory to receive the 2018 SWIFT Certified Application - CSDs and Securities Market Infrastructures label, SWIFT strongly encourages Certified Application providers to plan for ISO 20022 adoption.

2 SWIFT Certified Application - CSDs and Securities Market Infrastructures Application Label

The SWIFT Certified Application – CSDs and Securities Market Infrastructures (SMIs) application label focusses on the certification of the application that enables the initiation, generation, processing, and reporting of securities transactions related messaging by market infrastructures. This label is awarded to business applications that adhere to a specific set of criteria linked to the support of SWIFT FIN (MT) messages or SWIFT MX messages, or both MT and MX, SWIFT connectivity, and SWIFT functionality. In addition, support of FileAct and SWIFT WebAccess is recommended.

This label aims to ensure that CSDs and Securities Market Infrastructures application providers meet well-defined requirements around SWIFT standards, messaging, and connectivity.

This label validates the capability of an application to provide automation in a SWIFT environment for the following types of messaging.

- FIN and/or InterAct store-and-forward

  InterAct is optional in 2018 but will become mandatory in the near future.
- SWIFT WebAccess (optional)
- FileAct (optional)

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

3 SWIFT Certified Application - CSDs and Securities Market Infrastructures Application Criteria 2018

3.1 Certification Requirements

New label

Vendors applying for the SWIFT Certified Application - CSDs and Securities Market Infrastructures label for the first time must comply with all criteria as defined in this document.

3.2 Installed Customer Base

Live customer reference

A minimum of one live customer must use the application.

By customer, SWIFT means a distinct CSD or Securities Market Infrastructure (SMI) 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

The CSDs and Securities Market Infrastructures application must support the FIN protocol or the InterAct store-and-forward protocol (or both) as described in this section. The application must support the required message sets in ISO 15022 or in ISO 20022 (or both). For more information, see MT Messages on page 9.

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.

For more information, see MT Messages on page 9.

InterAct Store-and-Forward protocol (optional)

The application must support the InterAct Store-and-Forward 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.

FileAct (optional)

FileAct can be used by the CSDs and securities market infrastructures' applications for a variety of flows to securely send files, including the following:

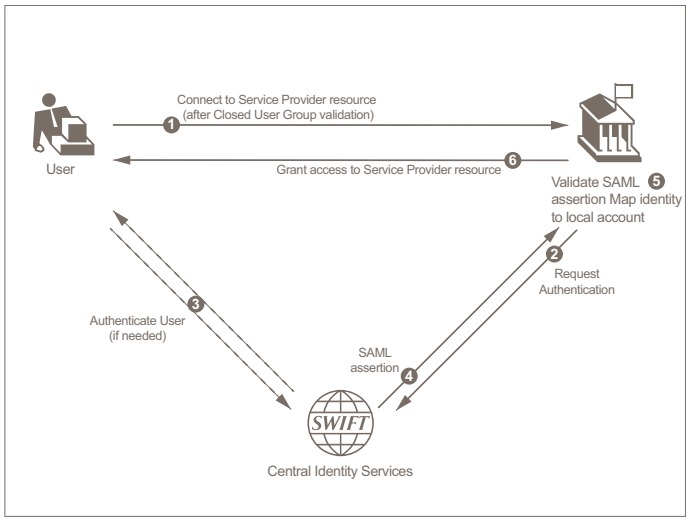
- Ad-hoc or scheduled (such as end of day) automated reports to participants (for example: transaction overviews, audit logs, transaction copies)
- Information exchange with ancillary systems
- Regulatory reporting

SWIFT WebAccess (optional)

SWIFT WebAccess provides a highly secure and reliable screen-based channel over SWIFT. It can be used by users of the CSDs and securities markets infrastructures application to securely monitor their business activities such as securities balances/positions, pending settlement instructions, settled settlement instructions, 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 7.2. Proper support of Alliance Access Release 7.2 is mandatory for the 2018 label.

Mandatory adapters

The SWIFT Certified Application - CSDs and Securities Market Infrastructures label requires support for either Automated File Transfer (AFT) or an interactive link with MQ Host Adapter (MQHA) or SOAP for Alliance Access 7.2. The adapters must support the following messaging service and Standards:

Messaging service	Standards
FIN	MT
InterAct in store-and-forward mode	MX

The CSDs and Securities Market Infrastructures application must support the FIN protocol or the InterAct store-and-forward protocol (or both). See also Messaging on page 6.

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 messages and 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 message/file signature. With the increased number of cyber-attacks on the financial industry, customers will expect message signing with LAU from their application providers.

For more information about LAU, see the Alliance Access Developer Guide.

Note *Although Local Authentication support is not mandatory to receive the 2018 SWIFT Certified Application label, SWIFT strongly encourages SWIFT Certified providers to plan for LAU support.*

3.5 Standards

The CSDs and Securities Market Infrastructures application must support the securities settlement and reconciliation messages. It must also support at least one of the two following messages sets:

- corporate actions management
- collateral management

The application must support these message sets in ISO 15022 or in ISO 20022 (or both) and be in line with global market practices where they exist.

The application must be able to support all fields and all code words, both mandatory and optional.

For more information, see MT Messages on page 9 and MX Messages on page 9.

3.5.1 MT Messages

The CSDs and Securities Market Infrastructures application must support the securities settlement and reconciliation messages. It must also support at least one of the two following messages sets:

- corporate actions management
- collateral management

The application must be able to do the following:

- Generate all outgoing messages types in categories 5 (see below), 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.

Securities settlement and reconciliation messages

For more information, see the SWIFT Certified Application - Securities Settlement Label Criteria.

Corporate actions messages

For more information, see the SWIFT Certified Application - Corporate Actions Label Criteria.

Collateral management messages

For more information, see "Securities and cash collateral" and "Triparty collateral management" messages as described in the SWIFT Certified Application - Collateral Management Label Criteria.

3.5.2 MX Messages

The CSDs and Securities Market Infrastructures application must support the securities settlement and reconciliation messages. It must also support at least one of the two following messages sets:

- corporate actions management
- collateral management

ISO 20022-compliant messages

Although ISO 20022 implementation is not mandatory to receive the 2018 SWIFT Certified Application - CSDs and Securities Market Infrastructures label, SWIFT strongly encourages Certified Application providers to plan for ISO 20022 adoption.

The CSDs and Securities Market Infrastructures application must support the messages that belong to the categories semt and sese, and one of the two following categories: seev or colr. This includes incoming and outgoing messages for equivalent MT categories and scenarios.

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
- be in line with global market practice established by the Securities Market Practice Group (SMPG)
- take into account the ISO 20022/ISO 15022 coexistence rules
- ensure CSDs supported by the application provider publish on the CSD homepage (in MyStandards) the list of messages as well as versions used with their communities

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

The application must be able to do the following:

- generate all outgoing messages types from these listed categories, 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

Settlement and Reconciliation messages

For more information, see "ISO 20022 Messages Optional for Securities Settlement" in the SWIFT Certified Application - Securities Settlement Label Criteria.

Corporate Action messages

For more information, see "ISO 20022 for Corporate Actions" in the SWIFT Certified Application - Corporate Actions Label Criteria.

Collateral Management messages

For more information, see "Bilateral Collateral Management" messages as described in the SWIFT Certified Application - Collateral Management Label Criteria. See also the SWIFT MX Collateral Management Message Name and Description.

3.6 Message Reconciliation

The application must be able to manage message flows received in a non-FIFO order, such as cancellations received before its related instruction.

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 2018 for Category 5 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 2018 Standards Release becomes effective in November 2018, 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 on MyStandards.

3.8 User Interface

The application must have a manual entry, display, and repair capability for the MTs or the MXs (or both) listed in Standards on page 9.

Message entry

The application must make it possible for a user to manually input or modify the MT or MX (or both) 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, or Bank Directory Plus) 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 a part of the BIC, 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 Portal 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 BIC Directory (more than 200 countries), from connected and non-connected financial institutions and corporates active on FIN, FileAct, and/or InterAct.
- LEIs (Legal Entity Identifier) from the endorsed LOUs (Local Operating Units).

  Only LEIs that have a corresponding BIC are included.
- Name and address details for most BICs
- 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

Although some of the information listed previously is less relevant for CSDs and Securities Market Infrastructures, we need to stress the growing importance of LEI in the securities area.

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 Portal in full and delta versions. Upon request it can also be delivered through FileAct on a daily or monthly basis.

4.3 IBAN Plus (NA)

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
- Institution bank and branch codes for which no IBANs have been issued and hence that should not be found in IBANs.

The directory is ideal for accurate derivation of BIC from IBAN, covering 72 IBAN countries (including all SEPA countries). It is also ideal for validating IBANs. The capability to validate IBANs is important as many corporations generate IBANs for their vendors, suppliers, and clients, which in many cases are not the correct IBANs issued by the banks.

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 on a daily and monthly basis. Upon request it can also be delivered through FileAct.

4.4 SWIFTRef Business Applications (NA)

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 - CSDs and Securities Market Infrastructures 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 2018 and 2019 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