SWIFT Certified Application

# Cash Management for Corporates

## Label Criteria 2018

This document explains the business criteria required to obtain the SWIFT Certified Application for Corporates - Cash Management 2018 label, which is aimed at corporate applications.

26 January 2018

# Table of Contents

# Preface

### Purpose of the document

This document explains the business criteria required to obtain the SWIFT Certified Application for Corporates - Cash Management 2018 label, which is aimed at corporate applications.

### Audience

This document is for the following audience in vendor companies:

- Product Managers
- Development Managers
- Developers

### 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.
- Standards MX - General Information
- 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.
- SWIFT for Corporates > Cash Management > Cash Management - Release 2011
  - Cash Management for Standards MX Reference Guide

    The Cash Management Business area contains messages that support the reporting and advising of the cash side of any financial transaction, including cash movements, transactions and balances, plus any exceptions and investigations related to cash transactions.
  - Payment Initiation for Standards MX Reference Guide

    The Payments Initiation business area contains messages that are used to initiate credit transfers and direct debits. It also contains a set of messages to instruct related operations.
- SWIFT for Corporates > Implement your project
  - FileAct Implementation Guide for SCORE
  - Standards MT - Message Implementation Guide - Volume 1
  - Standards MX Message Reference Guide
  - Standards MX - Message Implementation Guide

    This document describes a set of rules and guidelines that you must follow when you implement, send, or receive ISO 20022 payment initiation and account reporting messages using FileAct in SCORE.

# 1 SWIFT for Corporates - Cash Management Solution

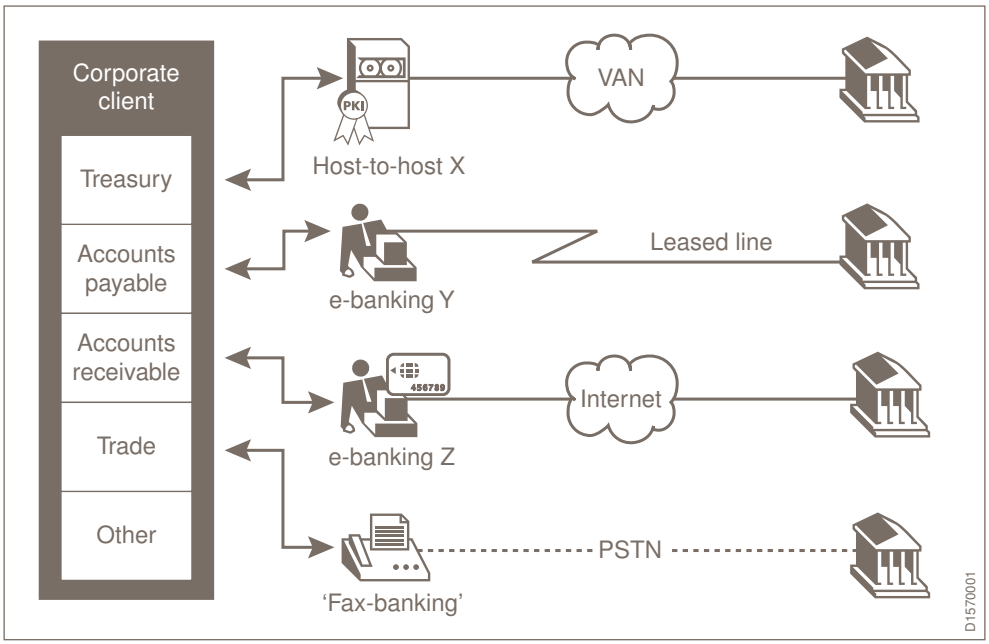
## Background

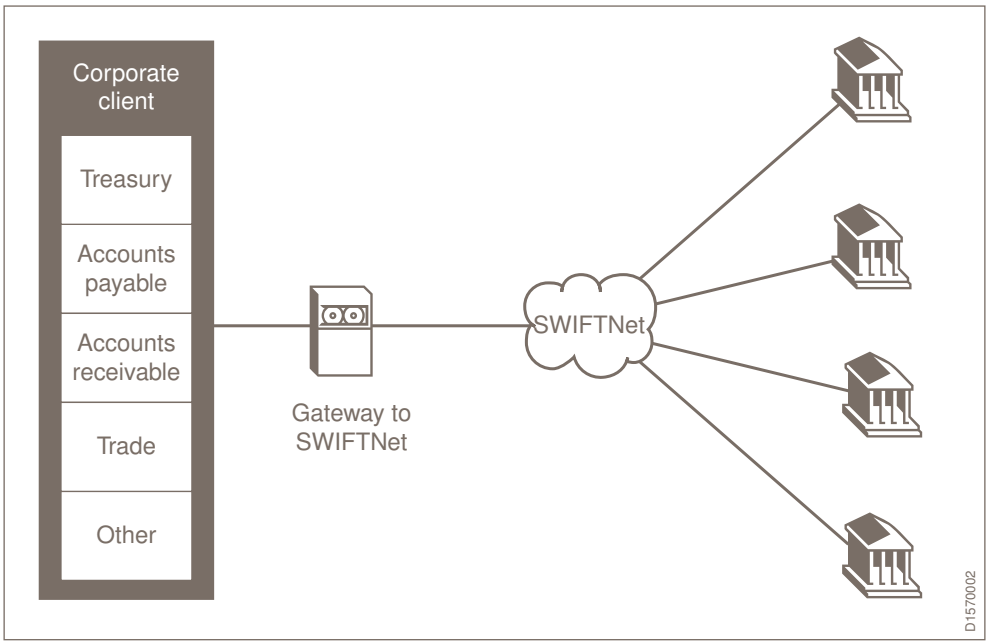
The corporate world has undergone significant changes in recent years. An ever more competitive, global, and regulated market is forcing treasurers to rethink the way they operate.

Treasurers must respond to several challenges, such as reducing operational risk and complying with an ever stricter regulatory framework.

To address these challenges, improved efficiency and overall control are needed. For this reason, treasurers increasingly try to centralise and automate their operations.

They then face the challenge of different platforms and communication standards when trying to establish electronic connections with their banks. Clearly, this situation is not ideal because these environments are costly to maintain and operate. In addition, such environments are a source of risk because their heterogeneity is more difficult to control (for example, weak business continuity plans due to complexity, and lack of security discipline due to a high number of passwords).






### The SWIFT for corporates offering

In response to these issues, and with the support of its community, SWIFT has created its SWIFT for Corporates offering, which enables corporates to use SWIFT's single, secure, and reliable messaging platform to access the services that their financial institutions can provide (for example, cash management services). This enables corporates to reduce cost and risk, optimise their liquidity management, and strengthen security.

The SWIFT for Corporates - Cash Management offering encompasses the following components:

- **SWIFT standards**

  Standards MT (ISO 15022) and Standards MX (ISO 20022) messages are supported. Non-SWIFT standards in the context of Cash Management are also allowed.

- **SWIFT messaging services**

  FIN and FileAct (real-time mode and store-and-forward mode)

- **Rulebook**

  Sets out rules and best practices for the use of the standards and messaging services

- **Access models**

  SCORE, MA-CUG, Treasury Counterparty

# 2 SWIFT Certified Application for Corporates - Cash Management Label

## Overview

The SWIFT Certified Application for Corporates - Cash Management label aims at business applications that are capable of processing and exchanging cash management flows (for example, supplier payments).

To qualify for this programme, applications must offer a set of business functions that involve the processing of the data exchanged over SWIFTNet. Such applications include, for example, treasury management systems, accounts payable/receivable modules within Enterprise Resource Planning (ERP) systems, and payment factory applications.

Applications that primarily aim to facilitate connectivity (that is, reformatting and technical integration with third-party applications) and stand-alone enterprise application integration (EAI) products without further business functionality do not qualify.

The label is awarded after successful technical and functional validations by SWIFT experts.

# 3 SWIFT Certified Application for Corporates - Cash Management Criteria 2018

## 3.1 Certification Requirements

**New label**

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

**Existing label (renewal from previous year)**

- **Mandatory**

  Vendors that have been granted the SWIFT Certified Application - Cash Management label in 2017 are required to prove compliance with the Standards Release (SR) 2018 and connectivity through Alliance Access 7.2.

- **Optional**

  - New messages supported in SCORE

  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 corporate 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

**Overview**

The messaging services and related tools form the core offering of SWIFT and include information directories and business intelligence.

**Mandatory**

- **FIN**

FIN is SWIFT's core store-and-forward messaging service. It enables the exchange of individual structured financial messages in a secure and reliable way.

- **FIleAct**

  FileAct enables the secure and reliable transfer of files and is typically used to exchange batches of structured financial messages and large reports. FileAct supports tailored solutions for market infrastructure communities, closed user groups, and financial institutions. FileAct is particularly suitable for bulk payments, securities value-added information and reporting, and for other purposes, such as central bank reporting and intra-institution reporting.

**Optional**

- **Reference Data**

  BIC Directory

  Bank Directory Plus

  IBAN Plus

  See more information about reference data in section Reference Data Integration (Optional) on page 11.

# 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 for Corporates - Cash Management 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 |
| FileAct in real-time mode | Any |
| FileAct in store-and-forward mode | Any |

**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

### Overview

The application must support:

- Standards MT in the areas of payments and reporting, as documented in the User Handbook. The complete set of message types to be supported is listed in below table.
- the ISO 20022 standards as documented in the ISO 20022 Payment Initiation Message Definition Report and the ISO 20022 Schema's for Payment Initiation (www.iso20022.org).

**Note** *The same information can be found in the SWIFT for Corporates - Standards MX Message Reference Guides. The implementation of these standards must be in line with the rules and guidelines set out for the Standardised Corporate Environment (SCORE) which are documented in the Standards MX Payments Initiation Message Reference Guide and the Standards MX - Message Implementation Guide.*

The application must support all changes to the messages before their live release date on the SWIFT network (Standards Release 2018). When new messages are introduced or significant modifications have been made to existing messages, SWIFT expects the application provider to provide adequate testing time to its customers before these messages go live.

### FIN Payments mandatory and optional messages

| | Corporate-to-bank (C2B) | Bank-to-corporate (B2C) |
|---|---|---|
| **Mandatory** | MT 101 Request for Transfer<br>MT 199 Free Format Message<br>MT 999 Free Format<br>ISO 20022 (over FileAct)<br>MX: pain.001.001.03 Customer Credit Transfer | MT 199 Free Format<br>MT 940 Customer Statement<br>MT 942 Interim Transaction Report<br>MT 999 Free Format<br>MX: pain.002.001.03 Payment Status Report<br>MX: camt.052.001.02 Bank to Customer Account Report<br>MX: camt.053.001.02 Bank to Customer Statement<br>MX: camt.054.001.02 Bank to Customer Debit/Credit Notification |
| **Optional** | MT 104 Direct Debit<br>MT 192 Request for Cancellation<br>MT 195 Queries<br>MT 196 Answers (to MT 195 queries)<br>MT 920 Request Message<br>MT 995 Queries | MT 195 Queries<br>MT 196 Answers (to MT 195 queries)<br>MT 900 Confirmation of Debit<br>MT 910 Confirmation of Credit<br>MT 941 Balance Report<br>MT 950 Statement Message<br>MT 996 Answers |

The support of other standards (for example, CFONB, BAI, BACS) for payments is also possible, but these standards must be carried over FileAct.

## 3.6 Message Reconciliation

### Requirements

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

The application must be able to support FileAct in both real-time mode and store-and-forward mode. The implementation of FileAct must be in line with the rules and guidelines set out for the Standardised Corporate Environment (SCORE) which are documented in the *SWIFT for Corporates - FileAct Implementation Guide for SCORE*.

# 3.7 Message Validation

**Requirements**

The application must comply with message validation rules described in the *FileAct Implementation Guide for SCORE*, the *Standards MT - Message Implementation Guide - Volume 1*, the *Cash Management for Standards MX - Reference Guide*, and the *Payments Initiation for Standards MX - Reference Guide*.

# 3.8 Business Workflow

**Requirements**

The application must support straight-through processing (STP) principles and SWIFT usage guidelines as described in the Rulebooks.

# 3.9 User Profile Management

**Requirements**

The application must ensure the security of the financial institution processes. This includes ensuring that only authorised users (whether people or applications) can perform a specific task. Vendors must demonstrate how profile management is implemented and how access is denied to unauthorised users.

In a non-automated environment, the application must also be able to support the four-eyes principle.

# 3.10 Reference Data Integration (Optional)

The application must support the directories that are documented in this section. Optional directories are clearly identified as such.

## 3.10.1 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.

## 3.10.2 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

**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.

## 3.10.3 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
- 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.

## 3.10.4 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.

## 3.11 3SKey Support (Optional)

### Background

When a bank interacts with its corporate customers through electronic banking channels, it may need to authenticate received data to ensure that the individual customer employee is authorised to issue the instruction.

In practice, banks and their corporate clients must often manage and use several different types of personal signing mechanisms (for example, multiple tokens with different passwords). Using and maintaining different authentication methods in parallel adds to the complexity, and leads to higher operational risk and cost.

### 3SKey solution

To address this issue, SWIFT offers the 3SKey solution. SWIFT supplies tokens that include PKI-based credentials for 3SKey users (typically, corporates).

3SKey users set up their tokens with a personal certificate issued by the SWIFT PKI. 3SKey users use these credentials to sign messages and files exchanged with one or more 3SKey subscribers over any mutually agreed channel. The signature provides authentication of the 3SKey user and non-repudiation of the signed transactions.

### Application vendor requirements

The application vendor must provide workflow management for transaction and file signing with 3SKey.

The application must fulfil the following requirements:

- Transport the personal signatures together with the files, messages, and documents sent to the bank
- Support single and multiple signatures on files, messages, and documents

### Application vendor obligations

The application vendor must fulfil the following conditions:

1. Order the 3SKey developer kit and integrate 3SKey in the vendor application in accordance with the service and technical requirements, as documented in the 3SKey Service Description and the *3SKey Developer Guide*.
2. Send a transaction signed with 3SKey for verification purposes (PKCS#7).

Application vendors can find more information on www.swift.com.

# 4 Marketing and Sales

### Requirements

In order to maximise the business value of the SWIFT Certified Application - Cash Management 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