



## SWIFT Certified Application

# Trade and Supply Chain Finance for Corporates

Label Criteria 2018

This document explains the business criteria required to obtain the SWIFT Certified Application for Corporates - Trade and Supply Chain Finance 2018 label, which is aimed at Corporate applications.

26 January 2018

# Table of Contents

<b>Preface</b> .....	3
<b>1 SWIFT for Corporates - Trade and Supply Chain Finance Solution</b> .....	4
<b>2 SWIFT Certified Application for Corporates - Trade and Supply Chain Finance Label</b> .....	6
<b>3 SWIFT Certified Application for Corporates - Trade and Supply Chain Finance Criteria 2018</b> .....	7
3.1 Certification Requirements.....	7
3.2 Installed Customer Base.....	7
3.3 Messaging.....	8
3.4 Direct Connectivity.....	8
3.5 Standards.....	9
3.6 Message Reconciliation.....	14
3.7 Message Validation .....	14
3.8 Business Workflow.....	14
3.9 User Profile Management.....	19
3.10 Reference Data Integration (Optional).....	19
3.11 3SKey Support (Optional).....	22
<b>4 Marketing and Sales</b> .....	24
<b>Legal Notices</b> .....	25

# Preface

## Purpose of the document

This document explains the business criteria required to obtain the SWIFT Certified Application for Corporates - Trade and Supply Chain Finance 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.

- [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 > [Trade and Supply Chain](#) > Trade and Supply Chain Finance resource centre

- [Trade for Corporates - Drivers](#)

The document provides a value proposition of the SWIFT for Corporates (trade) solution.

- [TSU - Corporate-to-Bank Guidelines for ISO 20022 Standards](#)

This document introduces the general principles and guidelines of the TSU corporate-to-bank (TSU C2B) project.

- SWIFT for Corporates > [Implement your project](#)

- [FileAct Implementation Guide for SCORE](#)

- [Standards MT - Message Implementation Guide - Volume 1](#)

# 1 SWIFT for Corporates - Trade and Supply Chain Finance Solution

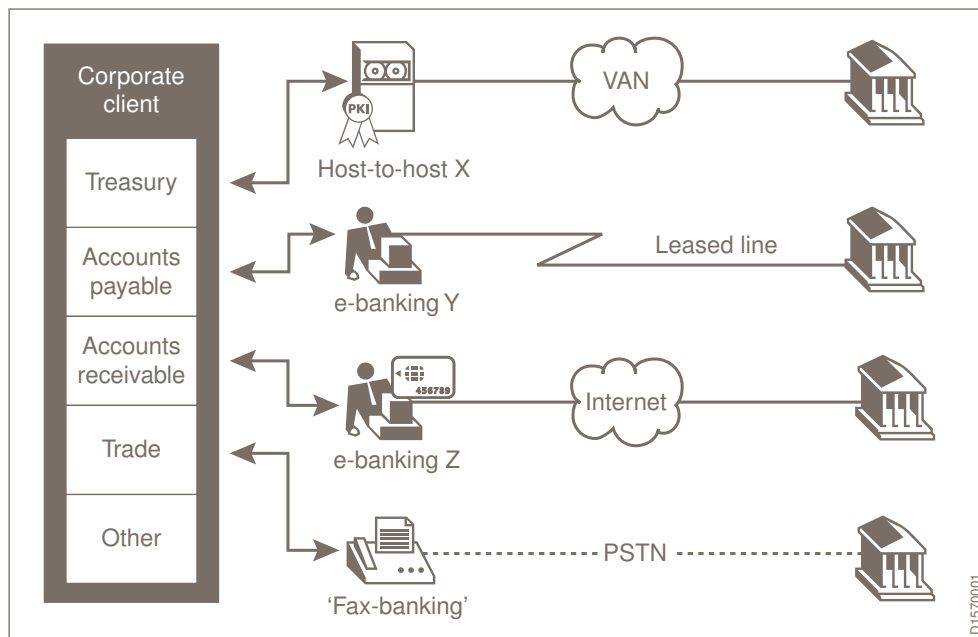
## Background

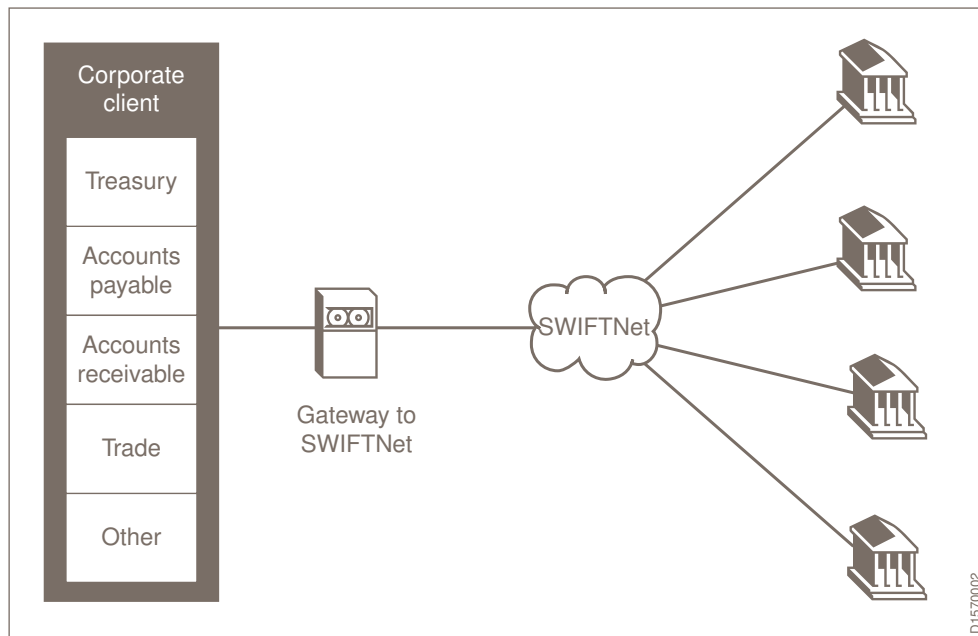
The corporate world has undergone significant changes in recent years. An ever more competitive, global, and regulated market is forcing corporates to rethink the way they operate.

Corporates 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, corporates 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, trade services or cash management). This enables corporates to reduce cost and risk, optimise their liquidity management, and strengthen security.

For trade finance, many corporates use up to 20 banks and more. The problems created by the use of multiple standards and protocols are therefore even more severe. Regulators are also becoming much more demanding, wanting (for example) more details about a corporate's trading activities in different parts of the world.

The SWIFT for Corporates - Trade and Supply Chain Finance offering encompasses the following components:

- **SWIFT standards**  
MT, MX
- **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
- **Message User Guidelines**  
Sets out guidelines for message standards that must be followed
- **Access models**  
SCORE, SCORE compliant MA-CUGs

## 2 SWIFT Certified Application for Corporates - Trade and Supply Chain Finance Label

### Overview

The SWIFT Certified Application for Corporates - Trade and Supply Chain Finance label aims at business applications that are capable of processing and exchanging trade flows (for example, application for issuance of a Letter of Credit (L/C), Documentary Credit Advice). It is granted to trade applications that work in a corporate back-office context, after a successful technical and functional validation by SWIFT experts.

To qualify for this label, applications must offer a set of business functions which involve the processing of the data that is ultimately exchanged over SWIFTNet.

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.

**Note** *For this specific label it is allowed to use separate software modules for MT 798 and bank payment obligations. It is the obligation of the software provider to inform SWIFT of this exception at the start of the certification process. Additionally, it must be indicated clearly in the profile sheet that is posted on [swift.com](http://swift.com) after a successful certification.*

# 3 SWIFT Certified Application for Corporates - Trade and Supply Chain Finance Criteria 2018

## 3.1 Certification Requirements

### **New label**

Vendors applying for the SWIFT Certified Application for Corporates - Trade and Supply Chain Finance 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 - Trade and Supply Chain Finance label in 2017 are required to prove compliance with the Standards Release (SR) 2018 and connectivity through Alliance Access 7.2.

In order to promote interoperability between vendor solutions, vendors solutions will have to be retested to demonstrate compliance against the MT 798 [Message Implementation Guide](#) (MIG) specifications. The test set-up, provided by SWIFT, will cover all sub-message types and will assess field formats and cross-field rules. Vendors will have to provide evidence of a successful retesting against this set-up.

- **Optional**

Enablement for 3SKey approval workflows

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. However, this requirement is not mandatory for 2018.

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.

- **ISO2002 messages** (tsmt) for C2B (including bank payment obligation)

### Optional

- **Reference Data**

BIC Directory

Bank Directory Plus

IBAN Plus

See more information about reference data in section [Reference Data Integration \(Optional\)](#) on page 19.

## 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 - Trade and Supply Chain Finance 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

### FIN

The application must support Standards MT messages [as documented in the User Handbook](#), in the areas of trade.

The message type to be supported is as follows:

	Corporate-to-bank (C2B)	Bank-to-corporate (B2C)
Mandatory	MT 798 Proprietary Message and the mandatory sub-message types (flows)	MT 798 Proprietary Message and the mandatory sub-message types (flows)

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 MT - Message Implementation Guide - Volume 1*.

Corporates need help from their vendors in order to implement the trade envelope for both corporate-to-bank and bank-to-corporate messages. The message and its related sub-messages cater for Import Letters of Credit, Export Letters of Credit, and Guarantees/Standby Letters of Credit.

<b>Import Documentary Credit</b>	Application for issuance of Documentary Credit - C2B
	Notification of Draft or issuance of Documentary Credit - B2C
	Request for amendment of Documentary Credit - C2B
	Notification of amendment of Documentary Credit - B2C
	Notification of Acceptance/Refusal of Amendment - B2C
	Advice of Discrepancy - B2C
	Response to Advice of Discrepancy - C2B
	Notification of Advice of Payment/Acceptance/Negotiation - B2C
	Notification of Advice of Discharge - B2C
	Notification of Advice of Refusal - B2C
	Notification of Advice of Reimbursement or Payment - B2C
	Settlement of Import Documentary Credit - B2C

<b>Export Documentary Credit</b>	Advice of Documentary Credit - B2C
	Advice of amendment or Confirmation of Documentary Credit - B2C
	Advice of Third Bank Documentary Credit - B2C
	Advice of Transfer Documentary Credit - B2C
	Advice of Acceptance/Refusal of Amendment - C2B
	Response to Documentary Credit presentation - B2C
	Response to Advice of Discrepant Presentation - C2B
	Notification of authorisation to Pay, Accept or Negotiate - B2C
	Notification of Advice of Payment/Acceptance/Negotiation - B2C
	Notification of Advice of Discharge - B2C
	Notification of Advice of Refusal - B2C
	Notification of Advice of Reimbursement or Payment - B2C
	Request for Transfer of a Documentary Credit - C2B
	Notification of Transfer of a Documentary Credit - B2C
	Settlement of Export Documentary Credit - B2C

<b>Guarantee/Standby Letter of Credit</b>	Application for issuance of Guarantee/Standby Letter of Credit - C2B
	Notification of Guarantee/Standby Letter of Credit - B2C
	Request for amendment of Guarantee/Standby Letter of Credit - C2B
	Notification of amendment of Guarantee/Standby Letter of Credit - B2C
	Query to extend or pay Guarantee/Standby Letter of Credit - B2C
	Response to extend or pay Guarantee/Standby Letter of Credit - C2B
	Notification of claim for payment of Guarantee/Standby Letter of Credit - B2C
	Settlement of Guarantee/Standby Letter of Credit claim for payment and/or charges - B2C
	Request for Guarantee/Standby Letter of Credit Reduction/Release - C2B
	Advice of Guarantee/Standby Letter of Credit Reduction or Release - B2C
<b>Common Group</b>	Free Format Message - C2B
	Free Format Message - B2C
	Notification of Settlement of Charges - B2C
	Request for Settlement of Charges - B2C
	Response to a Draft Undertaking - C2B
	Request for Cancellation - C2B
	Ancillary Message - C2B
	Ancillary Message - B2C

Vendors can find more information and specifications of the flows in the *Standards MT - Message Implementation Guide - Volume 1*.

All changes to the MT 798 must be supported by the application before they are live on the SWIFT network (see [Standards MT release dates](#)). When new flows are introduced or significant modifications have been made to existing flows, SWIFT expects the application provider to provide adequate testing time to its customers before these messages go live.

### FileAct

For some types of trade data exchange, the FileAct messaging service may be more appropriate. Specific trade request types enable corporates and banks to identify files in a formal manner. Trade

documents and images can be sent over SWIFT, and FIN messages for one transaction can be grouped together. Transparency, classification, routing, and processing are all improved.

### Mandatory

Trade Request Type	Items contained in files
tsrv.xxx.lettersofcredit	Items relating to letters of credit (L/C) in any agreed format: Examples: SWIFT Standards, EDIFACT, XML, scanned images
tsrv.xxx.gteesstandbys	Items relating to Guarantees/Standbys in any agreed format: Examples: SWIFT Standards, EDIFACT, XML, scanned images
tsmt.xxx.tradedocuments	Trade documents: Examples: invoices, certificates of origin, Bills of Lading
tsrv.fin.mt7xx.lettersofcredit	Items pertaining to L/Cs in FIN format
tsrv.fin.mt7xx.gteesstandbys	Items pertaining to Guarantees/Standbys in FIN format

Vendors can find more information about names and specifications of trade request types in the *FileAct Implementation Guide for Score*.

### ISO 20022

The following functions are required for corporate-to-bank communication:

- baseline establishment
- baseline amendment
- data set submission
- intent to pay

**Note** *Other functions exist in the Trade Services Utility, such as reporting, but have been put out of scope and have not been specifically tested. Financial institutions offer more complete reporting than TSU. Therefore using the existing Trade Service Utility reports would be of limited value in the corporate-to-bank space.*

### Mandatory

The list of TSU messages that are in scope is as follows:

Message Identifier	
InitialBaselineSubmissionV03	tsmt.019.001.03
BaselineReSubmissionV03	tsmt.012.001.03
DataSetSubmissionV03	tsmt.014.001.03
BaselineAmendmentRequestV03	tsmt.009.001.03

Message Identifier	
AmendmentAcceptanceV02	tsmt.005.001.02
AmendmentRejectionV02	tsmt.007.001.02
MisMatchAcceptanceV02	tsmt.020.001.02
MisMatchRejectionV02	tsmt.022.001.02
IntentToPayNotificationV01	tsmt.044.001.01

More information about the messages is available the following documents:

- XML schemas and documentation (Message Definition Report [MDR]) are available on [www.iso20022.org](http://www.iso20022.org), at the bottom of the page **Catalogue of messages**.
- *TSU - Corporate-to-Bank Guidelines for ISO 20022 standards*

## 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*.

In this case, the application must also be able to support the reference in the MT 798 (field 23X) to a related FileAct file.

## 3.7 Message Validation

### Requirements

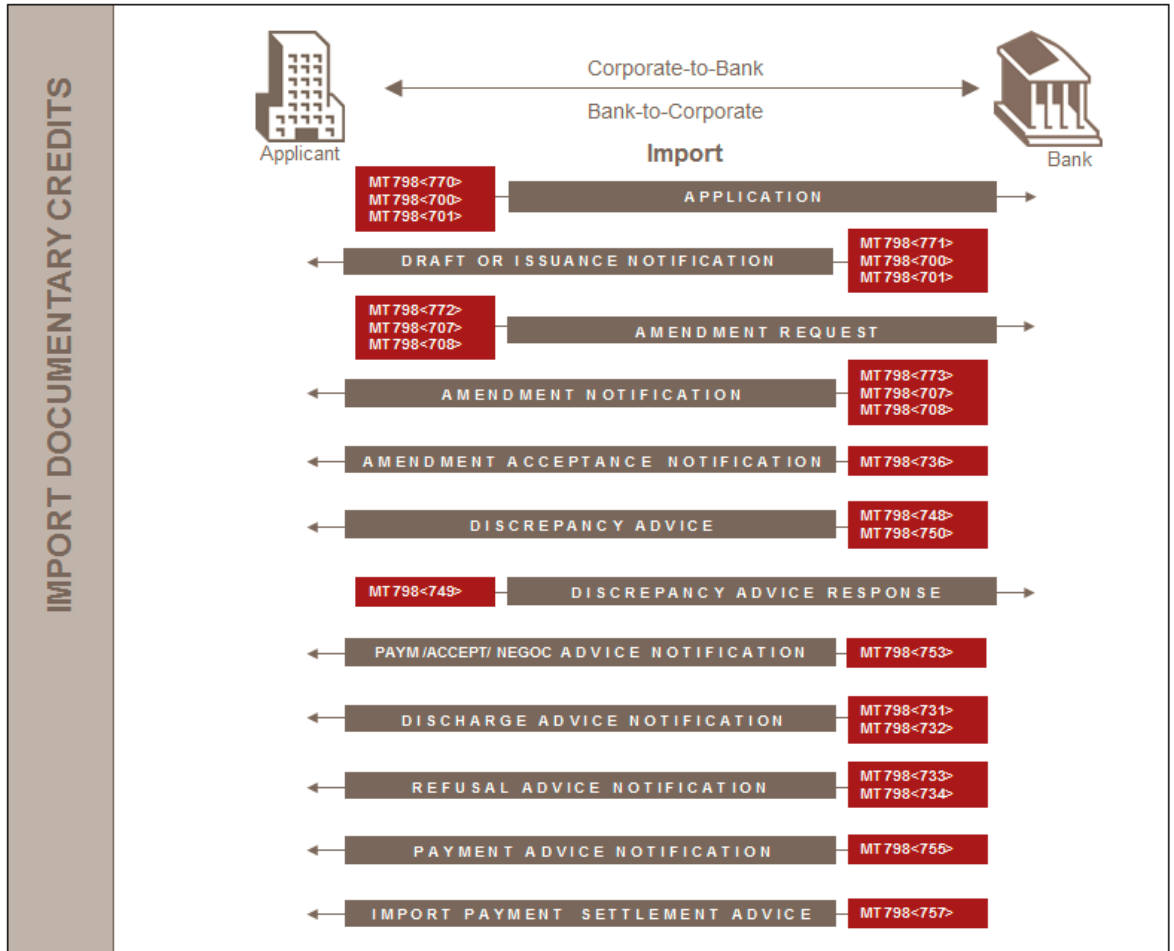
The application must comply with message validation rules described in the *Standards MT - Message Implementation Guide - Volume 1* and optionally the *FileAct Implementation Guide for SCORE*.

## 3.8 Business Workflow

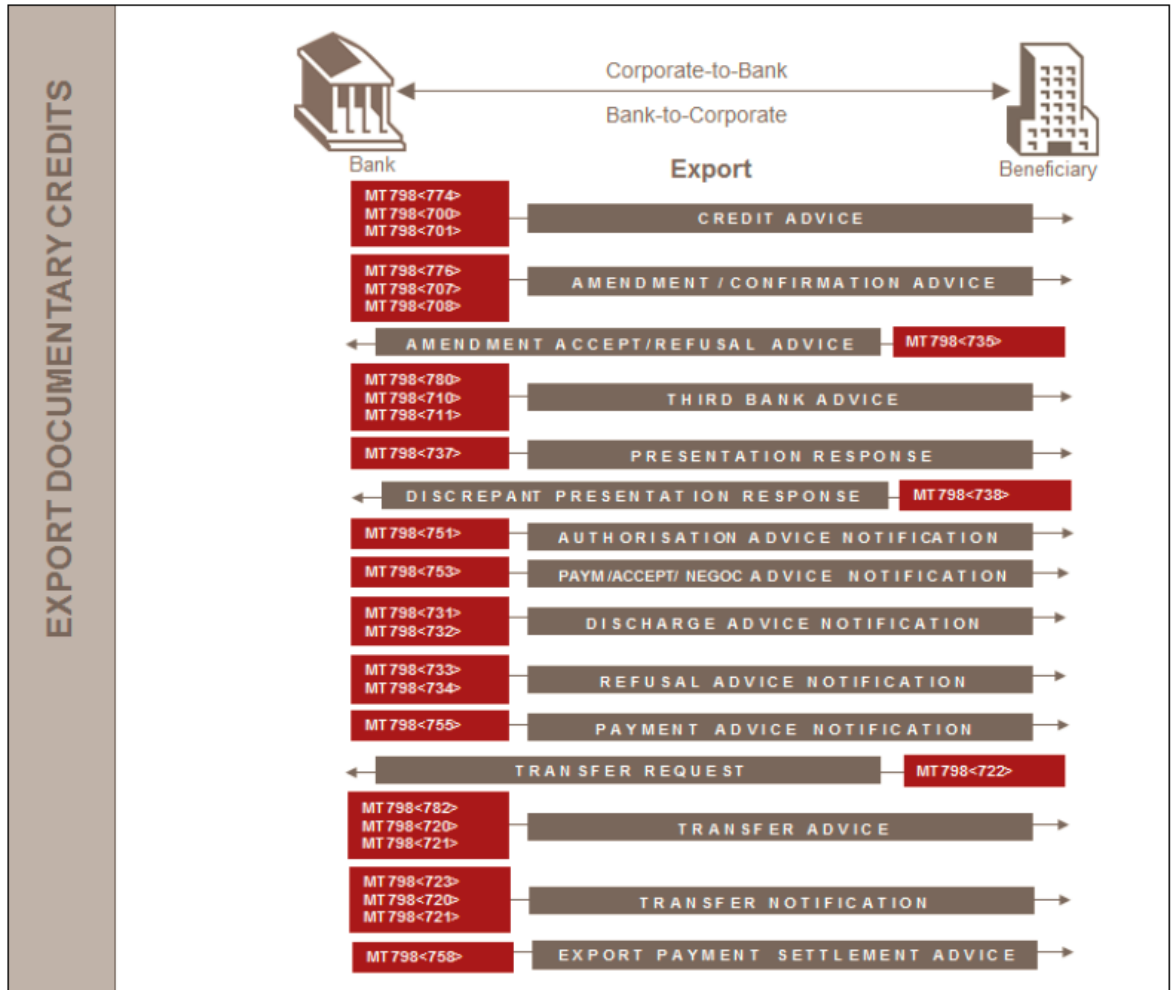
The banking application must support straight-through processing (STP) and SWIFT usage guidelines. For the MT 798 message, all related sub-messages and flows must be supported.

The application must be able to receive and process the messages with the appropriate counterparties (corporate, bank), as stated in *FIN* in the [SWIFT Certified Application- -Trade Finance Label Criteria](#).

### Import Documentary Credits

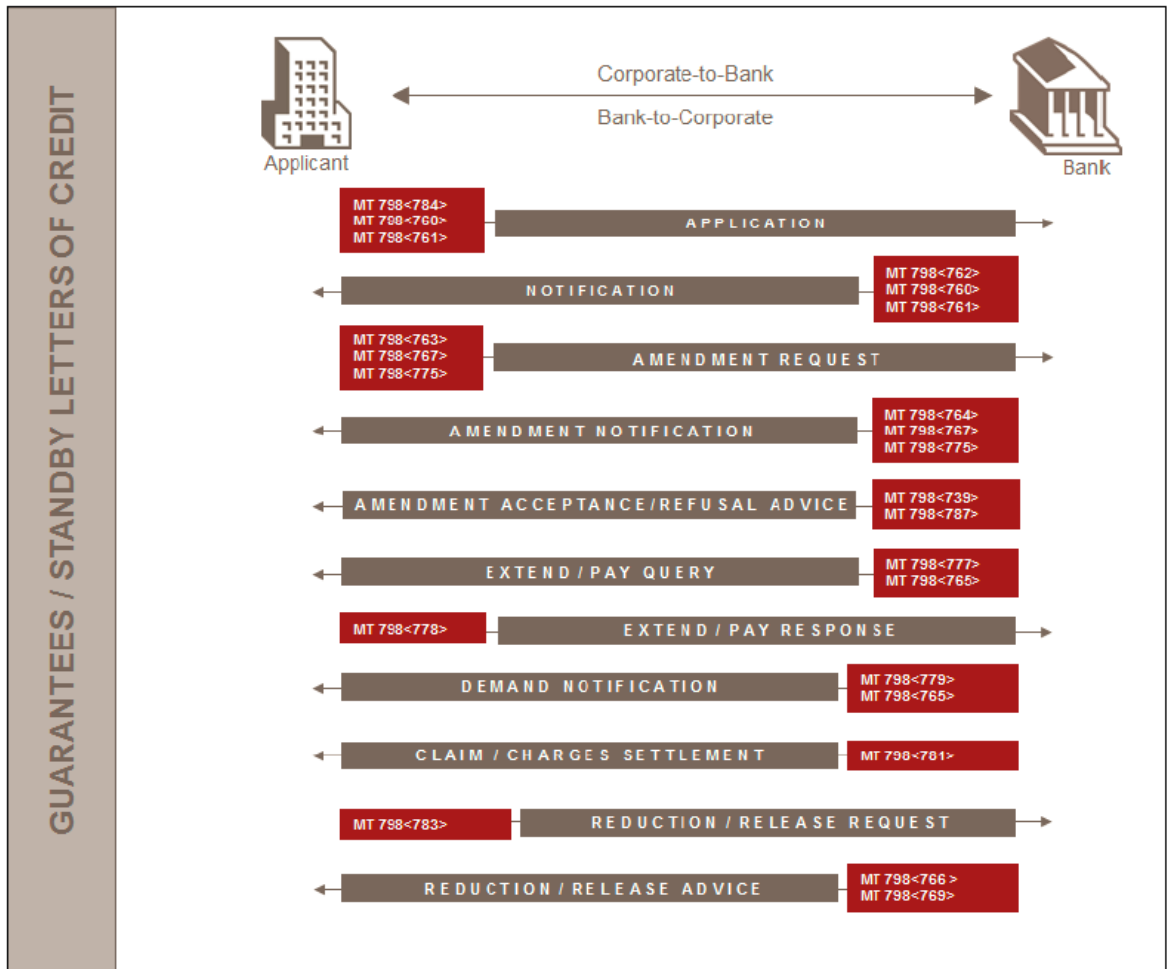


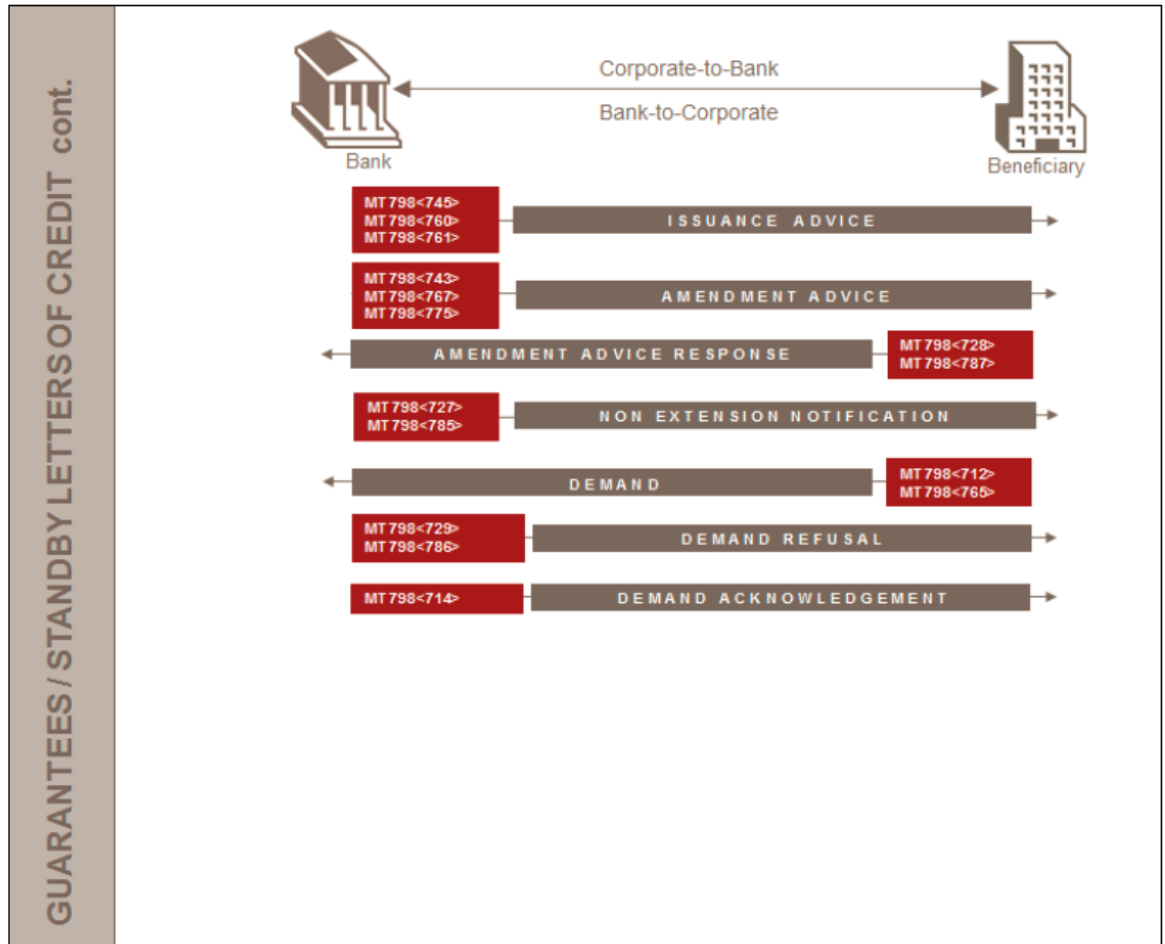
### Export Documentary Credits



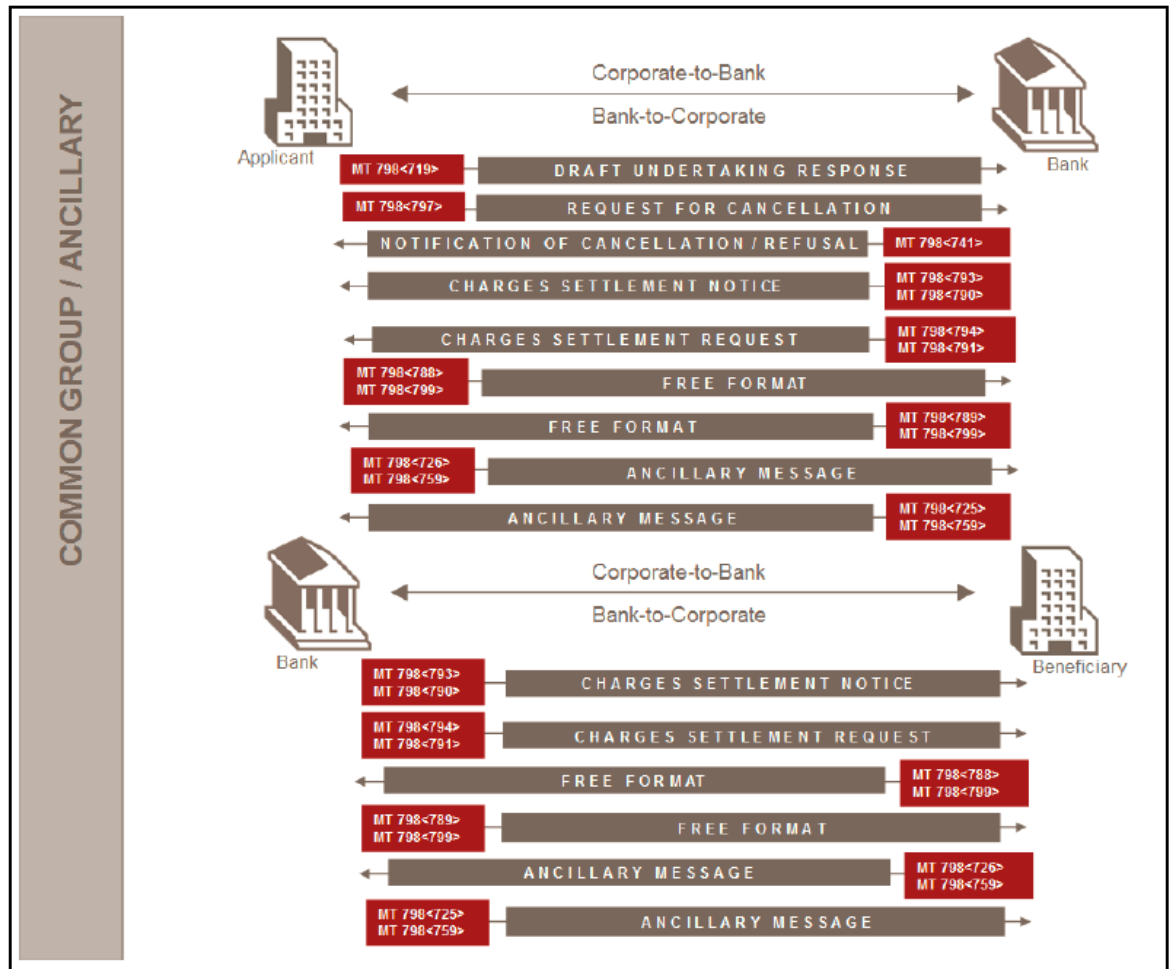


**Guarantees/Standby Letters of Credit**





### Common Group



## 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](http://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](http://www.swift.com).

## 4 Marketing and Sales

### Requirements

In order to maximise the business value of the SWIFT Certified Application - Trade and Supply Chain Finance 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

## Copyright

SWIFT © 2018. All rights reserved.

## 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, 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.