This document explains the business criteria required to obtain the SWIFT Certified Application – RTGS Application 2016 label for RTGS applications.

29 January 2016
# Table of Contents

Preface.............................................................................................................................................3

1  SWIFT for the Real-Time Gross Settlement System (RTGS).........................................................4

2  SWIFT Certified Application - RTGS Application Label.................................................................7

3  SWIFT Certified Application – RTGS Application Criteria 2016..................................................8
   3.1 Certification Requirements.......................................................................................................8
   3.2 Installed Customer Base........................................................................................................8
   3.3 Messaging ...............................................................................................................................9
   3.4 Connectivity ..........................................................................................................................11
   3.5 Standards .............................................................................................................................12
   3.6 Message Reconciliation.........................................................................................................12
   3.7 Message Validation................................................................................................................13
   3.8 User Interface .......................................................................................................................14

4  Reference Data Integration ............................................................................................................15
   4.1 BIC Directory .........................................................................................................................15
   4.2 Bank Directory Plus ...............................................................................................................15
   4.3 IBAN Plus ..............................................................................................................................16
   4.4 SWIFTRef Suite .....................................................................................................................17

5  Marketing and Sales .......................................................................................................................17
   A.1 Incoming and Outgoing MT Messages ....................................................................................18
   B.1 Payments Clearing and Settlement (pacs)..............................................................................19
   B.2 Cash Management (camt).......................................................................................................19
   B.3 System messages (xsys).........................................................................................................19

Legal Notices .........................................................................................................................................20
Preface

Purpose of the document

This document explains the business criteria required to obtain the SWIFT Certified Application - RTGS Application 2016 label for RTGS applications.

Audience

This document is for the following audience:

- Developers
- Development managers
- Product managers
- SWIFT customers seeking to understand the SWIFT Certified Application Programme or involved in selecting third-party applications

Related documentation

- SWIFT Certified Application Programme Overview
  The document provides an overview of the SWIFT Certified Application Programme. It describes the benefits of the programme for SWIFT registered providers that have a software application they want to certify for compatibility with SWIFT standards, messaging services, and connectivity. This document also describes the application and validation processes that SWIFT uses to check such SWIFT compatibility. SWIFT's certification of an application is not an endorsement, warranty, or guarantee of any application, nor does it guarantee or assure any particular service level or outcome with regard to any certified application.

- SWIFT Certified Application Technical Validation Guides
  The documents explain in a detailed manner how SWIFT validates the application so that this application becomes SWIFT Certified.

- User Handbook: www.swift.com > Support > Resources > Documentation
1 SWIFT for the Real-Time Gross Settlement System (RTGS)

Overview

More than 80 High Value Payment Market Infrastructures (HVPMI) rely on SWIFT worldwide. 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

Moreover, SWIFT offers a highly secure and reliable channel called SWIFT WebAccess to enable HVPMI to 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 and is typically used to exchange batches of large reports such as operational and statistical reports, user directories, and reference data.

The following schemas illustrate the four options (re-grouped in two main categories: Y-Copy and V-shape) that an HVPMI can choose while using SWIFT.

A. Y-Copy

A normal message is transmitted straight 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.

1. Y-Copy RTGS flows with FINCopy and MT. This is complemented by SWIFT WebAccess and FileAct (see diagram 1).

2. Y-Copy RTGS flows with SWIFTNet Copy and ISO 20022. This is complemented by SWIFT WebAccess and FileAct (see diagram 2).

B. V-shape

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

3. V-shape RTGS flows with FIN MT. This is complemented by SWIFT WebAccess and FileAct (see diagram 3).

4. V-shape RTGS flows with SWIFTNet and ISO 20022. This is complemented by SWIFT WebAccess and FileAct (see diagram 4).
Diagram 1: Y-Copy RTGS flows with FINCopy and MT

Diagram 2: Y-Copy RTGS flows with SWIFTNet Copy and ISO 20022
Diagram 3: V-shape RTGS flows with FIN MT

Diagram 4: V-shape RTGS flows with SWIFTNet and ISO 20022
2 SWIFT Certified Application - RTGS Application Label

Overview

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. Moreover, the support of FileAct and SWIFT WebAccess is optional.

This label aims to ensure that RTGS 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:

- 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.
- Exceptions and Investigations case managers. These applications must apply for the Exceptions and Investigations label.
3 SWIFT Certified Application - RTGS Application Criteria 2016

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.

3.2 Installed Customer Base

Live customer reference

A minimum of 1 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 the list in "Standards" in Appendix A.

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 the list in "Standards" in Appendix B.

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

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

The application must support FileAct.
SWIFT WebAccess (optional)

SWIFT WebAccess provides a highly secure and reliable screen-based channel over SWIFT and can be used by users of the RTGS application 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 and must be able to integrate with SWIFT WebAccess and 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 Connectivity

Requirements

For direct connectivity, the vendor application must integrate with Alliance Access. A business application that does not connect directly to Alliance Access 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. Proper support of Alliance Access 7.0 is mandatory for the 2016 label.

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

Mandatory adapters

<table>
<thead>
<tr>
<th>Messaging service</th>
<th>Standards</th>
<th>Interface</th>
<th>Mandatory adapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIN</td>
<td>MT</td>
<td>Alliance Access 7.0</td>
<td>AFT or MQHA or SOAP</td>
</tr>
<tr>
<td>InterAct Store-and-Forward mode</td>
<td>MX</td>
<td>Alliance Access 7.0</td>
<td>AFT or MQHA or SOAP</td>
</tr>
<tr>
<td>FileAct in Store-and-Forward mode</td>
<td>Any</td>
<td>Alliance Access 7.0</td>
<td>AFT or MQHA or SOAP</td>
</tr>
</tbody>
</table>

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 2017. SWIFT recommends that you prepare for this change accordingly. More details on the SWIFTNet 7.2 release 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.

Note: Local Authentication support will become a mandatory requirement in 2017. SWIFT recommends that you prepare for this change accordingly.
3.5 Standards

**MT**

The application must support the messages that belong to categories 0, 1, 2 and 9, incoming and outgoing, listed in "FIN Messages Required for SWIFT Certified Application – RTGS application 2016 Label" in Appendix A, and according to Standards Release 2016. The application must be able to support all fields and all code words, both mandatory and optional.

The application must be able to:

- Generate all outgoing messages types in categories 0, 1, 2 and 9 (listed in Appendix A), 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.

**MX**

The application must support the messages that belong to the categories pacs, camt, and xsys, incoming and outgoing, as listed in "InterAct Messages Required for SWIFT Certified Application-RTGS application 2016 Label" in Appendix B, 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:

- Be in line with global market practice for the HVP market (see above)
- 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:

- Generate all outgoing messages types mentioned in "InterAct Messages Required for SWIFT Certified Application- RTGS application 2016 Label" in Appendix B, 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.

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 2016 for Category 0, 1, 2 and 9 messages (i.e. in line with network validation and usage rules). In addition, the application might 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 2016 Standards Release becomes effective in November 2016, but SWIFT expects the vendor to provide adequate testing time to its customers before these messages go live.

InterAct Store-and-Forward

InterAct Store-and-Forward 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 HVPS Global Market Practice for pacs and camt messages.
3.8 User Interface

The application must have a manual entry, display, and repair capability for the MTs and the MXs listed in Appendix A and B.

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) requires a second person to validate it before execution
4 Reference Data Integration

4.1 BIC Directory

Overview

The application must provide access to the BIC Directory both for message validation and as a look-up function in the message creation and message repair stations.

It is the responsibility of subscribers at all times to make sure that they use the latest version of the BIC Directory. As such, SWIFT expects the application to support the BIC Directory weekly update in an efficient manner without disrupting customer operations.

Retrieval functionality during message composition

The BICs contained in the BIC Directory can be used in various fields of the SWIFT messages. The absence of BICs in these fields is one of the major obstacles to straight-through processing (STP) and causes manual intervention on the recipient side. SWIFT expects vendors to provide an integrated interface within their application to make it possible for users to retrieve and input correctly formatted BICs into the proper fields.

Search functionality

The user must be able to enter a number of search criteria, such as bank name or location, to perform a search, and to get a list of results. From this result window, the user must be able to select the correspondent BIC and copy it into the message (that is, the transaction).

If the search criteria return no results, then the user must be alerted that no BIC is available. If the user manually enters a non-existent BIC, then the application must send an alert notifying the user that this BIC is not valid.

Available format and delivery

The BIC Directory is downloadable on www.swift.com in full or delta versions. It must either be copied into the application repository system or stored in the back office for access by the vendor application through a defined interface. It is available as well through FileAct.

4.2 Bank Directory Plus

Content

Bank Directory Plus contains the following information:

- All BIC-11 codes from the ISO registry (more than 200 countries), from connected and non-connected financial institutions and corporates.
- Name and address details for each BIC
- FIN service codes
- National clearing codes, including CHIPS, TARGET, and EBA data
- Bank hierarchy information
- Payment system routing data
- Country, currency, and holiday information
Available formats
Flat file in XML or TXT format

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

The file is also downloadable from the SWIFTRef download portal, which is available from the SWIFTRef access point. It is available as well through FileAct.

4.3 IBAN Plus

Content
The IBAN Plus directory contains the following information:

• IBAN country formats
  – IBAN country prefix
  – IBAN length
  – Bank code length, composition, and position within the IBAN

• Institution name and country

• Institution bank and branch codes in the formats as embedded in IBANs

• Institution BICs as issued together with the IBANs to the account holders

• Data for the SEPA countries and the non-SEPA countries that adopted the IBAN

• Updates to the file when new IBAN country formats are registered with SWIFT in its capacity as the ISO IBAN registry

Available formats
Flat file in XML or TXT format

Delivery
The file is downloadable from the SWIFTRef download portal, which can be accessed from the SWIFTRef access point. It is available as well through FileAct.
4.4 SWIFTRef Suite

Introduction

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

Purpose

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

Related information

Additional information about SWIFTRef is available on swiftref.swift.com. It is available as well through FileAct.

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. 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 product roadmap for 2016 and 2017 containing the plans for further developments, SWIFT support, and new releases
- a complete set of documentation, including feature overview, SWIFT adapters, workflow engine capability, and user manuals

In addition, the vendor must dedicate a page of their web site to describe the SWIFT Certified Application used in a SWIFT context.
Appendix A

FIN Messages Required for SWIFT Certified Application – RTGS Application 2016 Label

A.1 Incoming and Outgoing MT Messages

<table>
<thead>
<tr>
<th>Mandatory/Optional</th>
<th>MT</th>
<th>MT Name</th>
<th>Incoming</th>
<th>Outgoing</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>103</td>
<td>Single Customer Credit Transfer</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>M</td>
<td>103+</td>
<td>Single Customer Credit Transfer</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>M</td>
<td>200</td>
<td>Financial Institution Transfer for its Own Account</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>M</td>
<td>202</td>
<td>General Financial Institution Transfer</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>M</td>
<td>202 COV</td>
<td>General Financial Institution Transfer</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>M</td>
<td>204</td>
<td>Financial Markets Direct Debit Message</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>M</td>
<td>900</td>
<td>Confirmation of Debit</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>M</td>
<td>910</td>
<td>Confirmation of Credit</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>M</td>
<td>940</td>
<td>Customer Statement Message</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>M</td>
<td>941</td>
<td>Balance Report</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>M</td>
<td>942</td>
<td>Interim Transaction Report</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>M</td>
<td>950</td>
<td>Statement Message</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>M</td>
<td>n91</td>
<td>Request for Payment of Charges, Interest and Other Expenses</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>M</td>
<td>n92</td>
<td>Request for Cancellation</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>M</td>
<td>n95</td>
<td>Queries</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>M</td>
<td>n96</td>
<td>Answers</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>M</td>
<td>n98</td>
<td>Proprietary Message</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>M</td>
<td>n99</td>
<td>Free Format Message</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>M</td>
<td>096</td>
<td>Authorization request</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>M</td>
<td>097</td>
<td>Authorization response</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
Appendix B

ISO 20022 Messages for SWIFT Certified Application – RTGS Application 2016 Label

B.1 Payments Clearing and Settlement (pacs)

<table>
<thead>
<tr>
<th>Mandatory/Optional</th>
<th>Message Name</th>
<th>Message ID (XML Schema)</th>
<th>Incoming</th>
<th>Outgoing</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>Payment Return</td>
<td>pacs.004.001.05</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>M</td>
<td>FIToFICustomerCreditTransferV05</td>
<td>pacs.008.001.05</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>M</td>
<td>FinancialInstitutionCreditTransferV05</td>
<td>pacs.009.001.05</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>M</td>
<td>Financial Institution Direct Debit V01</td>
<td>pacs.010.001.01</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

B.2 Cash Management (camt)

<table>
<thead>
<tr>
<th>Mandatory/Optional</th>
<th>Message Name</th>
<th>Message ID (XML Schema)</th>
<th>Incoming</th>
<th>Outgoing</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>ResolutionOfInvestigation</td>
<td>Camt.029.001.05</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>M</td>
<td>BankToCustomerAccountReport</td>
<td>camt.052.001.05</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>M</td>
<td>BankToCustomerStatementV05</td>
<td>camt.053.001.05</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>M</td>
<td>BankToCustomerDebitCreditNotificationV05</td>
<td>camt.054.001.05</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>M</td>
<td>FIToFIPaymentCancellationRequest</td>
<td>camt.056.001.04</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

B.3 System messages (xsys)

<table>
<thead>
<tr>
<th>Mandatory/Optional</th>
<th>Message Name</th>
<th>Message ID (XML Schema)</th>
<th>Incoming</th>
<th>Outgoing</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>Y-copy Authorisation or refusal</td>
<td>xsys.001</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
Legal Notices

Copyright
SWIFT © 2016. All rights reserved.

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.