Service

Partner Programme

SWIFT Certified Application - Exceptions and Investigations

Label Criteria 2016

This document explains the criteria required to obtain the SWIFT Certified Application - Exceptions and Investigations 2016 label for your business application.

29 January 2016

Table of Contents

Preface

Purpose of the document

This document explains the criteria required to obtain the SWIFT Certified Application - Exceptions and Investigations 2016 label for your business application.

Audience

This document is for the following audience:

- Application Product Managers
- Developers

Related documentation

Documentation (User Handbook) on www.swift.com

- 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.

www.swift.com > Partner Programme

- 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

- Exceptions and Investigations Service Description
- *Exceptions and Investigations integration Guide*
- *Corporate-to-Bank - Standards MX Message Reference Guide*
- *Corporate-to-Bank - Standards MX Schemas*
- *Corporate-to-Bank - Standards MX Samples*
- *Corporate-to-Bank - Standards MX Samples with SWIFTNet InterAct Headers*
- *Corporate-to-Bank - Standards MX Samples with Alliance Access Headers*

1 SWIFT for Exceptions and Investigations

The aim of SWIFT for Exceptions and Investigations is to support banks and their customers in their effort to streamline their payment-related enquiries management processes. This is achieved by automating enquiries which have the potential to be automated, which also increases the efficiency in handling enquiries that still require some manual intervention.

The Exceptions and Investigations 1.2 release is currently available. This release relates to both the bank-to-bank environment and the corporate to bank environment.

Exceptions and Investigations requires the use of the following items:

- **4 case assignment and 12 case management XML messages to be used in a bank-to-bank and corporate-to-bank environment**

  The business content of the MXs used in the Exceptions and Investigations Bank-to-Bank space is the same as in the Exceptions and Investigations Corporate-to-Bank space. However, there is a slight difference in the header of the messages, hence the reference to two releases and two sets of documentation.

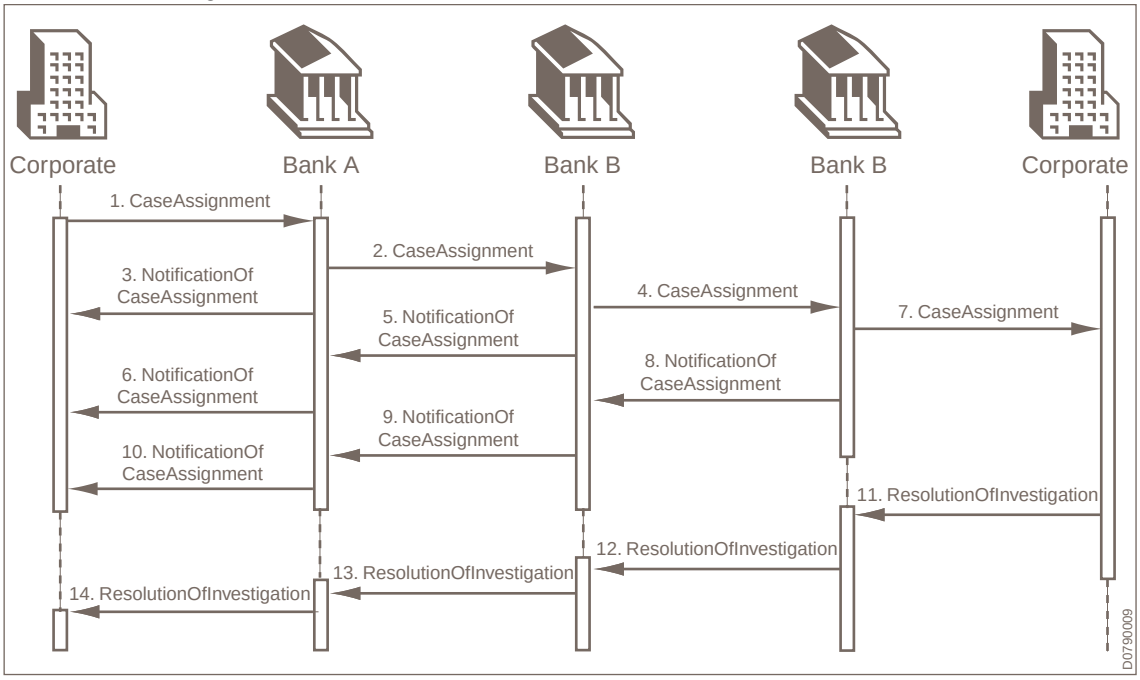
- **InterAct in store-and-forward mode**

  See the Exceptions and Investigations Service Description and the *Integration Guide* for a complete description of features and functions.

- **A Rulebook**

  The Rulebook sets out the rules and describing best practice guidelines applicable to all Exceptions and Investigations users. This includes specific workflows supporting each exception or investigation process, that is, Request for Cancellation, Request for Modification, Unable to Apply and Claim Non Receipt.

  The following workflow diagram describes the generic flow of messages for an enquiry from creation to closing:



2 SWIFT Certified Application - Exceptions and Investigations Label

Introduction

To integrate SWIFT for Exceptions and Investigations into existing applications or databases and to fully automate the information flows, service users must enhance their existing application infrastructure or obtain new applications. They can develop applications in-house or outsource this to a third-party software vendor. The integrated solution links a SWIFT interface to back-office applications.

Purpose of the Exceptions and Investigations label

The purpose of this label is to ensure that third-party applications are interoperable with each other, supporting the Exceptions and Investigations standards and rules as described in the User Handbook.

Therefore, the SWIFT Certified Application - Exceptions and Investigations label criteria focus on the ability of an application support for:

- **Messaging**

  The InterAct messaging flows defining the request-response communication between sender/receiver and the store-and-forward service.

- **Standards and Rulebook**

  All Exceptions and Investigations MT/MX standards and Usage Rules as outlined in the Exceptions and Investigations - Message Definition Reports and Schemas.

- **Business workflows**

  A workflow defines the series of messages to be exchanged and the sequence they must be sent in.

The SWIFT Certified Application label requires automation based on local application intelligence to support the communication workflows.

For example, the application must automatically generate and return a NotificationOfCaseAssignment when forwarding a case to the next party in the payment chain.

Note Integration is bank-specific and must be included in the bank requirements.

3 SWIFT Certified Application - Exceptions and Investigations Criteria 2016

3.1 Certification Requirements

New label

Vendors applying for the SWIFT Certified Application - Exceptions and Investigations label for the first time must comply with all criteria as defined in this document.

Existing label (renewal from previous year)

Vendors that have been granted the SWIFT Certified Application Exceptions and Investigations label in 2016 are required to prove compliance to the Standards Release (SR) 2016.

In case the vendor has upgraded its application, details of the new functionalities will be requested by SWIFT and demonstrated by the vendor (for example, New Functional validation required).

3.2 Installed Customer Base

Live customer reference

A minimum of one live customer must use the application.

By **customer**, SWIFT means a distinct financial institution 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.

Note If the partner successfully passes all certification steps to obtain the 2016 label for its application, but fails to have a customer using the application as described earlier in the document, then its application will receive a conformance statement. This statement will automatically be transferred into the SWIFT Certified Application label once the partner has a customer that uses the Exceptions and Investigations solution to send and receive live traffic.

3.3 Connectivity

3.3.1 Direct Connectivity

Requirements

For direct connectivity, the vendor application must integrate with Alliance Access. A business application that does not connect directly to Alliance cannot be considered for a SWIFT Certified Application label.

The direct connection from the business application to Alliance Access can be achieved using one or more of the Alliance Access adapters:

- MQ Host Adapter (MQHA)
- Automated File Transfer (AFT)
- SOAP Host Adapter

The vendor must develop and test SWIFT application integration using Alliance Access 7.0. Proper support of Alliance Access 7.0 is mandatory for the 2016 label.

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

When connecting directly to Alliance Access, the business application must:

- add the specific Alliance Access messaging interface header to the request payload (the request payload consists of application header + Exceptions and Investigations business message)
- support the XML v2 data format

Mandatory adapters

Messaging service	Standards	Interface	Mandatory adapter
InterAct in store-and-forward mode	MX	Alliance Access 7.0	AFT or MQHA or SOAP

Note If the application supports several of the previously mentioned adapters, then the vendor may provide the appropriate evidence for some or all of them during the technical validation. SWIFT only publishes information for which evidence has been provided.

SWIFTNet Release 7.2

A mandatory upgrade to the underlying technology behind SWIFT's interface products is planned for 2017. The aim of the release is to continue to provide a highly secure and efficient SWIFT service for our customers in the years ahead.

Note Release 7.2 support will become a mandatory requirement in 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.

3.4 Messaging

The application must support InterAct and its mandatory associated features, as listed in the Exceptions and Investigations Service Description and the *Exceptions and Investigations Integration Guide*.

3.5 Standards

The application must support all case assignment messages and all case management messages following the rules as described in the Exceptions and Investigations - Message Definition Reports and Schemas as well as the related FIN messages.

List of messages required for SWIFT Certified Application - Exceptions and Investigations

Request Type	Request Name	Incoming/Outgoing
camt.007.002.02	RequestToModifyPaymentV02	✓
camt.008.002.02	RequestToCancelPaymentV02	✓
camt.026.001.02	UnableToApplyV02	✓
camt.027.001.02	ClaimNonReceiptV02	✓
camt.028.001.02	AdditionalPaymentInformationV02	✓
camt.029.001.02	ResolutionOfInvestigationV02	✓
camt.030.001.02	NotificationOfCaseAssignmentV02	✓
camt.031.001.02	RejectCaseAssignmentV02	✓
camt.032.001.01	CancelCaseAssignmentV01	✓
camt.033.001.02	RequestForDuplicateV02	✓
camt.034.001.02	DuplicateV02	✓
camt.035.001.01	ProprietaryFormatInvestigationV01	✓
camt.036.001.01	DebitAuthorisationResponseV01	✓
camt.037.001.02	DebitAuthorisationRequestV02	✓
camt.038.001.01	CaseStatusReportRequestV01	✓
camt.039.001.02	CaseStatusReportRequestV01	✓

Request Type	Request Name	Incoming/Outgoing
	and	
MT192/MT292	Request for cancellation	✓
MT195/MT295	Queries	✓
MT196/MT296	Answers	✓
MT199/MT299	Free Format Message	✓

All changes to the messages must be supported by the application before the live release date on the SWIFT network. When new messages are introduced or those existing are significantly modified, we expect the application providers to provide adequate testing time to their customers prior to these messages going live.

Library of XML message templates

To minimise the need for manual entry, the application must provide an automated process or an operator with a library of all available standard Exceptions and Investigations XML messages.

Correct payload structure

The application must be able to generate the correct payload structure of the 16 XML schemas.

MT/MX co-existence

Since the XML-based messages (MXs) for Exceptions and Investigations today co-exist with the formatted FIN (MT) enquiry messages, the application must be capable to send/receive the Exceptions and Investigations MXs as well as the MT messages listed in this section.

The application must also be able to automatically generate or forward an investigations message to the next party in the payments chain in the appropriate syntax (MX or MT), that is, depending on the Exceptions and Investigations readiness status of this next party. The readiness status of Exceptions and Investigations customers can be found in the *SWIFTNet Services Directory*. This directory lists all test and live users that participate in Exceptions and Investigations. The application must enable a user to upload and manually update the available information from the Directory.

The application is required to incorporate the Unique Case ID in the generated MT or MX message.

Note The *SWIFTNet Services Directory* can be accessed using you swift.com account if you have the right to do so.

Bank-to-bank and corporate-to-bank message flows

The Exceptions and Investigations solution is set up in two distinct SWIFTNet services to support the corporate-to-bank or the bank-to-bank message flows.

Based on the information downloaded from the *SWIFTNet Services Directory*, the application must be able to decide in which Exceptions and Investigations service the message has to be sent, that is, the Exceptions and Investigations corporate-to-bank service or the Exceptions and Investigations bank-to-bank service, in the Test and Training or the live environment.

The application must provide the messaging interface with the above information to enable the appropriate header to be generated.

The service name for Exceptions and Investigations for corporate-to-bank (swift.corp.eni) in the header of the InterAct message differs from the one used in the bank-to-bank environment (swift.eni).

For example:

Sender	What	Addressee	Service name in live environment	Service name in Test and Training environment
Corporate	Investigation	Bank	swift.corp.eni	swift.corp.eni!p
Bank	Investigation (forward of investigation initially sent by Corporate to Bank)	Bank	swift.eni	swift.eni!p
Bank	Notification	Corporate	swift.corp.eni	swift.corp.eni!p

3.6 Message Reconciliation

The application must be able to reconcile technical messages such as SWIFTNet acknowledgements and delivery notifications. If the application connects to Alliance Access, then the reconciliation of the local Alliance Access message status is also required.

3.7 Message Validation

All MX messages must be validated against the relevant XML schemas and against Extended Validation Rules that are provided in the Rulebook and Exceptions and Investigations - Message Definition Reports and Schemas.

The application must provide validation on field and message level:

Level	Validation	More information
Field level	The data structure such as length and structure of currency, BIC/BEI, date format, and field length must be validated.	The user must be prompted to correct the information if this is not according to the specified rules.
Field content level	The data must be in line with the User Handbook or *Exceptions and Investigations Rulebook* (for example, a RequestToModifyPayment must never be sent to request the modification of the currency of the original payment instruction).	
Message level	The application must provide the correct mapping, that is, including business information in the right XML tag.	

The application must provide validation at different levels:

- On field level, the data structure such as length and structure of currency, BIC/BEI, date format, and field length must be validated. The user must be prompted to correct the information if this is not according to the specified rules.
- On field content level, the user must be stopped if its action is not in line with
- On message level, the application must provide the correct mapping, that is, including business information in the right XML tag.

Note It is important to specify the date/time usage in messages. An application often uses local date/time but without indication, so that the receiver does not know the sender's local time. It is therefore strongly recommended to provide a non-ambiguous way of specifying date/time by either referring to GMT time or by giving the time offset as required by the ISO date time used in the schema.

3.8 Business Workflows

Automating the case assignment messages

The application must have the ability to provide a minimum level of straight-through processing.

For the case assignment messages:

- when appropriate, the application must automatically generate a NotificationOfCaseAssignment
- before closing a case the application must automatically generate a ResolutionOfInvestigation
- when receiving a CaseStatusReportRequest, the application must be able to automatically generate a CaseStatusReport
- for all other messages (if not fully automated) the operator must be offered a drop-down list of appropriate (not all) messages to select from. The application must also provide automation such as pre-filling/copying fields, from the underlying payment message into the appropriate Exceptions and Investigations message and from an incoming Exceptions and Investigations message into an outgoing Exceptions and Investigations message

Support of the unique case identifier

The application must be able to generate a unique case identifier. This unique case identifier must not be changeable by the operator.

In order to make the case identifier unique for all the parties involved in a workflow, it is composed of the following two parts:

- the case creator identification (usually a financial institution BIC or non-financial institution BIC)
- a unique number (Casecreator reference)

If a sequential number is used for the Case creator reference, then the range of numbers must be large enough to avoid ambiguity when restarting the sequence. Alternatively, date and time can be used followed by a sequential number.

Re-use of the unique case identifier (case ID)

The case assignee must be able to re-use the unique case identifier (the combination of the case creator and case creator reference) in all its communications with both its case assigner and possible further case assignees during the case life cycle.

Implementation of the re-open flag

Closed cases can be re-opened and re-assigned. When this happens, the same unique case identifier as the one in the initial case must be used, with a flag indicating that this is a re-opened case.

The application must enable for a case to be re-opened and the same case identifier (Case ID) to be re-used. The case can be re-opened as a new type by the initiating party or the final party (that is, an UnableToApply can be re-opened as a RequestToCancelPayment).

The application must ensure that a message received with a re-open flag triggers the re-open flag to be passed on in all subsequent messages.

Relating the underlying permanent instruction identification to unique case identifier

When a case is assigned to a case assignee, the case assignee must first check the validity of the assignment.

If the assignment is valid, then the case assignee must check that there is no other case open on this underlying instruction.

Either of the following scenario applies:

- If there is no other case open for the same payment instruction, then the case assignee must accept the case. Acceptance is implicit.
- If there is an open case for the same payment instruction, then the case assignee will request the closure of one of the open cases. This is achieved by sending a ResolutionOfInvestigation message indicating that the case is a duplicate of another case (with the reference to the case). The receipt of the ResolutionOfInvestigation with the DuplicateOf filled in will close the current case.

  The application must also guide the investigator about the way to handle concurrent workflows by prompting the investigator to select the assignment which has priority, as stated in the following table, and close other assignment with an informative message.

When assignee is	Unable to apply	ClaimNonReceipt
Request to Modify Payment	Continue with Request to Modify Payment	Continue with Request to Modify Payment
Request to Cancel Payment	Continue with Request to Cancel Payment	Continue with Request to Cancel Payment
Unable to Apply	NA	Continue with Unable to Apply

  Some examples:

  – When a RequestToCancelPayment is received as well as an UnableToApply for the same payment, the application must be able to identify these investigation messages as relating to the same underlying payment and must update the case. The application must warn the investigator of the concurrent enquiry requests and prompt the investigator to take the appropriate action, that is, send a ResolutionOfInvestigation to the assigner of the

UnableToApply indicating that cancellation will follow and process the RequestToCancelPayment.

– When the same investigation has been received twice for the same underlying payment, the application must warn the investigator that a case is already open and prompt him to send a ResolutionOfInvestigation confirming duplication.

Support of the no by-pass rule

The **no by-pass** rule specifies that no party involved in the original payment transaction can be by-passed in the Exceptions and Investigations workflow. The application must prevent operators from violating this rule for example by prepopulating the party field with information from the underlying payment instruction.

Messaging grouping by case

The application must be able to allocate a message to the corresponding "case ID" and to present all messages that have been exchanged in relation to a specific case (ID). The application must group incoming and outgoing messages using, amongst others, date/time, Case ID, Assigner, Assignee.

The application must also be able to store the incoming and outgoing messages in the right order using date/time.

3.9 Reference Data Integration (Optional)

Introduction

The application must support the directories that are documented in this section.

Optional directories are clearly identified as such.

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

Search functionality

The user must be able to enter a number of search criteria, such as bank name or address, to perform a search, and to get a list of results. From this result window, the user must be able to select the required BICs and copy these into the different bank identifier fields of the message (that is, the transaction).

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

Available format and delivery

Flat file in XML or TXT format.

Delivery

The BIC Directory is downloadable in a manual or automated manner from the SWIFTRef Access Point in full and delta versions. Upon request it can also be delivered through FileAct.

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.

3.9.2 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 active on FIN, FileAct, and/or InterAct.
- All LEI (Legal Entity Identifier) from the endorsed LOUs (Local Operating Units).
- Name and address details for each BIC
- FIN service codes
- National clearing codes (160+ countries), including CHIPS, TARGET, and EBA data. For a limited number of countries (10+), national codes are also provided with name and address in local language (for example, China, Japan, Russia).
- Bank hierarchy information
- Country, currency, and holiday information
- Timezone information

Available formats

Flat file in XML or TXT format

Delivery

The Bank Directory Plus is downloadable in a manual or automated manner from the SWIFTRef Access Point in full and delta versions. Upon request it can also be delivered through FileAct.

3.9.3 IBAN Plus

Content

The IBAN Plus directory contains the following information:

- IBAN country formats

  - IBAN country prefix
  - IBAN length
  - Bank code length, composition, and position within the IBAN
- Institution name and country
- Institution bank and branch codes in the formats as embedded in IBANs
- Institution BICs as issued together with the IBANs to the account holders
- Data for the SEPA countries and the non-SEPA countries that adopted the IBAN
- Updates to the file when new IBAN country formats are registered with SWIFT in its capacity as the ISO IBAN registry

The directory is ideal for accurate derivation of BIC from IBAN, covering 68 IBAN countries (including all SEPA countries).

Available formats

Flat file in XML or TXT format

Delivery

The IBAN Plus is downloadable in a manual or automated manner from the SWIFTRef Access Point in full and delta versions. Upon request it can also be delivered through FileAct.

3.9.4 SWIFTRef Suite (Optional)

Introduction

SWIFTRef offers a suite of worldwide reference data products and services. This data 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 BICs, LEIs, MICs (Market Identification Codes), BRNs (Business Registration Numbers), GIINs (Global Intermediary Identification Numbers), national bank/sort codes, IBAN information, payment routing details (in SEPA and other payment systems), Standard Settlement Instructions, 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 is available on www.swift.com/SWIFTRef.

3.10 User Interface

The application must enable for manual entry/display capability and repair for XML and FIN (n92, n95, n96, n99) Exceptions and Investigations messages. The application must enable the creation of an MX/MT message and manual repair before re-inserting the message into the output queue.

SWIFT expects the application to offer a Graphical User Interface:

- enabling a user to manually input or modify any message
- offering normalised fields for input (independent from underlying syntax and business meaning)
- validating data input at field level - any invalid entry must be flagged, and the user prompted to correct the input
- providing the user with an intuitive method to follow the status of a particular case

3.11 User Profile Management

The application must provide a user profile management functionality to ensure that only authorised users can perform specific tasks. The partner must demonstrate how their application handles user profile creation, update, and deletion and that access is denied or an operation is refused if a user is not entitled to perform this operation.

The partner must also demonstrate 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 Marketing and Sales

Requirements

In order to maximise the business value of the SWIFT Certified Application - Exceptions and Investigations 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 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.

Legal Notices