Alliance Lite2

Service Description

This document describes the features and functions of Alliance Lite2, the system requirements, and the available operational services. In addition, the document describes the roles and responsibilities of Swift and the user in relation to Alliance Lite2.

19 June 2026

Link to this document: https://www2.swift.com/go/book/book126470

Table of Contents

Preface 3

Significant Changes 5

1 Overview of Alliance Lite2 6

2 Features and Functions 9

2.1 Alliance Lite2 Subscription and Delivery 9
2.2 Live and Test Environment 12
2.3 Browser-based Screens 12
2.4 AutoClient 14
2.5 Integration Options 16
2.6 Types of End Users 20
2.7 Security Features 20
2.8 Accessing the Alliance Lite2 Software 23
2.9 Accessing Swift Messaging Services 24
2.10 Protection of Customer Information 25
2.11 Service Availability 26

3 System Requirements 28

4 Third-Party Software 30

5 Ordering 31

6 Support and Care Services 32

6.1 Support 32
6.2 Care Alliance Lite2 32

7 Swift Training 33

8 Roles and Responsibilities 34

8.1 Swift Integration Layer and Alliance Lite2 Direct Link Licences 34
8.2 Users' Responsibilities 35
8.3 Swift's Roles and Responsibilities 41

9 Contractual Framework 44

Appendix A List of Available Configuration Changes 46

A.1 Standard Configuration Changes 46
A.2 Specific Configuration Changes 47

Appendix B Alliance Lite2 Service Levels 50

Legal Notices 52

Preface

Purpose of the document

This service description describes the features and functions of Alliance Lite2, the system requirements, and the available operational services. In addition, the document describes the roles and responsibilities of Swift and the user in relation to Alliance Lite2.

Note *This service description together with the* Swift General Terms and Conditions *and other relevant Swift contractual documentation is an integral part of the contractual arrangements between Swift and its customers for the provision and use of Alliance Lite2.*

Audience

This document is for the following audience:
- those who intend to subscribe to or use Alliance Lite2
- Alliance Lite2 users
- Alliance Lifeline users

Swift-defined terms

In the context of Swift documentation, certain terms have a specific meaning. These terms are called Swift-defined terms (for example, user, customer, or Swift services and products). The definitions of the Swift-defined terms appear in the Swift Glossary.

Related documentation

- Alliance Connect / Alliance Connect Virtual Service Descriptions
- Alliance Lite2 Administration Guide
-
- *Alliance Lite2 AutoClient Release Letter* (see the Alliance Lite2 page)
- Alliance Lite2 AutoClient User Guide
- Alliance Lite2 Direct Link User Guide
- Alliance Lite2 Security Guidance
- Alliance Lite2 support page
- Alliance Lite2 User Guide
- FIN Service Description
- HSM Card, Reader & Token Terms and Conditions
- Price List for Swift Messaging and Solutions
- Pricing and Invoicing - Ordering, Invoicing, and Payment
- Swift Care Services Service Description
- Swift By-laws
- Swift Certificate Centre Personal Token Software Installation Guide
- Swift Certificate Centre Portal User Guide
- Swift Community and Advanced Support Service Description
- Swift Services Terms and Conditions
- Swift Corporate Rules
- Swift Customer Security Controls Framework Detailed Description
- Swift General Terms and Conditions
- Swift Personal Data Protection Policy
- SwiftNet Messaging Operations Guide
- SwiftNet Online Operations Manager User Guide
- SwiftNet Service Description

- SwiftRef Products Terms and Conditions

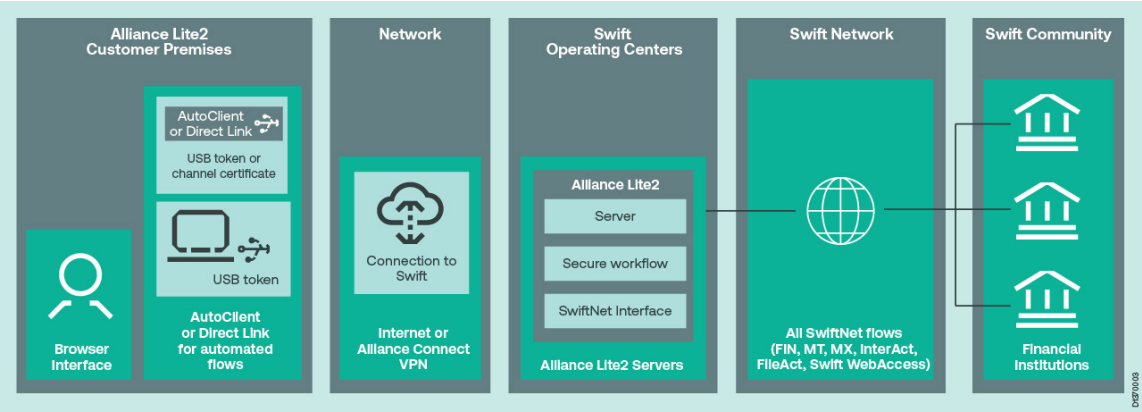
Significant Changes

The following table lists all significant changes to this service description since the previous edition. This table does not include editorial changes that Swift makes to improve the usability and comprehension of the document.

Updated information	Location
Swift Integration Layer is no longer offered to new customers.	Overview of Alliance Lite2 on page 6 Integrating with Business Applications on page 16 Solution Configuration on page 19 Swift Integration Layer and Alliance Lite2 Direct Link Licences on page 34

1 Overview of Alliance Lite2

Introduction



Alliance Lite2 is a hosted service operated by Swift, which allows customers to connect to the Swift network. Alliance Lite2 enables Swift customers to send and to receive all types of Swift messages and files, manual or automated, with a very light footprint. Alliance Lite2 also enables access to Swift Web Access services over SwiftNet upon separate subscription to these services.

Manual sending and receiving of Swift messages and files through browser-based screens

Alliance Lite2 enables customers to enter, approve, send, and receive Swift messages and files using a standard internet browser on a Windows PC, and a secure personal token provided by Swift.

Through the browser-based Alliance Lite2 screens, the customer can create and send Swift messages (MT, MX, and FileAct), while validation and approval are performed through a secure and auditable workflow. This workflow can be configured according to the customer's needs with 4-eyes control. The Swift Standards are built in, and Swift messages (MT or MX) are validated against the Swift Standards.

Customers can manually upload files and send to the counterparty on SwiftNet as individual Swift messages (MT or MX) or as entire files (FileAct) to the counterparty on SwiftNet.

Automated sending and receiving through AutoClient

Through its lightweight AutoClient software, Alliance Lite2 offers an easy, file-based way to integrate Swift messaging with customer applications. The AutoClient software runs in the background on a Windows PC, and automatically uploads and downloads messages and files to and from Swift counterparties in a secure and reliable way.

Swift Integration Layer - integration framework

Swift Integration Layer is a Swift generic integration framework that, in the context of Alliance Lite2, is paired with Alliance Lite2 AutoClient in order to address customers' specific message handling needs (for example, formats, protocols).

For more information about Swift Integration Layer, see the Swift Integration Layer Service Description.

Note *Swift Integration Layer is no longer offered to new customers.*

Alliance Lite2 Direct Link - integration framework

Alliance Lite2 Direct Link is an advanced version of Swift Integration Layer. It enables the communication with the Alliance Lite2 service and is designed to enable the creation of integration solutions beyond the file-based integration offered by Alliance Lite2 AutoClient.

Alliance Lite2 Direct Link is a framework for integration, not a turnkey product. It is an integration product that provides core transformation and connectivity services, in which custom logic is developed to address the specific integration requirements of a customer.

Swift Professional Services must design, develop, and test this custom logic for the customer's solution in the scope of a separate integration project. An integration project can be as simple as establishing a connection between a business application that already uses standard Swift message formats and Alliance Lite2, or can include custom logic needed to transform proprietary messages to standard Swift message formats.

When planning an integration project, Swift Professional Services and customer staff must work together to identify business needs. Swift Professional Services then use the Alliance Lite2 Direct Link development features to implement connectivity with a business application, develop custom logic for message transformation, and define integration flows. After testing, the integration solution is deployed in a customer's production environment for run-time use.

Integration projects can support services based on FIN, InterAct, or FileAct. Depending on a customer's Alliance Lite2 licence, single-BIC or multi-BIC configuration can be implemented.

In summary, a business application can connect to Swift over Alliance Lite2. The business application communicates with Alliance Lite2 Direct Link, which runs the custom logic to map these proprietary formats to the standard Swift formats that can be exchanged with Swift over Alliance Lite2.

For more information about how Alliance Lite2 Direct Link interacts with a customer's business application, see Integrating with Business Applications on page 16.

Other functions accessible through the browser-based screens

The browser-based screens also offer access to the following functions:
- Swift - BIC Directory
- Relationship Management Application (RMA) (see Other functions on page 14)
- Browse services on SwiftNet to which the customer has subscribed
- Message template management (see Message drafts and templates on page 12)
- Message search and report (see Message and file receipt on page 13)
- Security management (see Other functions on page 14)

The browser-based screens also enable trusted staff at the customer side to grant users access to Alliance Lite2, to assign permissions at various levels to these users, and, through the Swift Certificate Centre, to initialise a Swift secure personal USB token for each user.

VPN or Internet connectivity

Alliance Lite2 customers can use a broadband Internet connection to access Alliance Lite2 screens or to use AutoClient. However, Swift strongly recommends that Alliance Lite2 customers use Alliance Connect or Alliance Connect Virtual to connect to Swift and use Swift's Virtual Private Network (VPN), also called the Swift secure IP network (SIPN). A separate subscription is required to access Swift's Alliance Connect / Alliance Connect Virtual products.

The use of Swift's VPN through Alliance Connect or Alliance Connect Virtual is optional if the customer uses tokens, but is mandatory if the customer uses channel certificates. Customers

can ask Swift to disable Internet access for all their users, allowing access only through Swift's VPN.

For Alliance Lite2 Direct Link customers, it is mandatory to use Swift's Virtual Private Network (VPN). Customers must subscribe to one of Swift's Alliance Connect / Alliance Connect Virtual products.

Note *The subscription to the Swift secure IP network (SIPN) only becomes active after a subsequent Alliance Lite2 allowable downtime window (ADW, see Service Availability on page 26).*

Security

Alliance Lite2 offers the following security features:

- **Encrypted and authenticated communication**
  All communication between the user and the Alliance Lite2 servers is encrypted and protected by 2-way authenticated TLS sessions.
- **Hardware security tokens**
  The security tokens used on Alliance Lite2 are Swift-specific tamper-resistant hardware USB tokens, used for strong authentication and highly secure digital signing. When initialising a token, a 2048-bit PKI public/private key pair is generated on it and the user assigns a personal password to the token. The secret PKI private key never leaves the token and cannot be extracted from it. The public key is certified by Swift and the certificate is stored on the token.
  Only a person in possession of such a token, and who knows the password for that token, can access Alliance Lite2's browser-based screens and sign messages or files. The password of the token is used locally on the user's PC to access the token, and that password never travels over the Internet. The calculation of digital signatures occurs on the token. This provides strong two-factor authentication and signing.
- **Channel certificates**
  A channel certificate is an encrypted, disk-based profile file that provides a means for Swift to authenticate the identity of an application. On Alliance Lite2, channel certificates can only be used on AutoClient, not by operators to access the browser-based screens. Channel certificates are optional, and provide as advantage that the use of a USB token can be avoided on AutoClient. The use of channel certificates on AutoClient does require that AutoClient connects to Swift over Swift's Virtual Private Network (VPN) with an Alliance Connect product (VPN connectivity packs) owned by the same customer who owns the channel certificate.
  For more information about tokens and channel certificates, see Security Features on page 20, and Channel Certificates on page 35.

Swift certifies the PKI public keys using Swift's own Certification Authority (CA).

The specific security requirements for Alliance Lite2 must build on, and be integrated with, the customer's existing security infrastructure.

Customers have the ultimate responsibility for ensuring that they follow secure browsing practices.

For more detailed descriptions about how the customer can achieve these goals, see Security Features on page 20 and Users' Responsibilities on page 35.

2 Features and Functions

This section covers the following topics:
- The services and products included in the subscription (see Included Services and Products on page 9)
- The features available in the following two key components of Alliance Lite2:
  - Browser-based screens (see Browser-based Screens on page 12)
  - AutoClient (see AutoClient on page 14)
- The types of services offered (see Live and Test Environment on page 12)
- The types of Alliance Lite2 end users (see Types of End Users on page 20)
- Details about security management (see Security Features on page 20)
- The Alliance Lite2 software (see Accessing the Alliance Lite2 Software on page 23)
- The processing of messages and files (see Accessing Swift Messaging Services on page 24)
- The storage and retrieval of messages and files (see Protection of Customer Information on page 25)
- The availability of the Alliance Lite2 service (see Service Availability on page 26)

2.1 Alliance Lite2 Subscription and Delivery

2.1.1 Included Services and Products

Overview

The Alliance Lite2 subscription automatically includes a subscription to the following Swift services and products:
- SwiftNet PKI (including Alliance Lite2-related certificates)
- online access to the Bankers World Online BIC
- online access to the Knowledge Centre (User Handbook) for all the users that are registered to www.swift.com
- RMA Plus option
- subject to applicable eligibility criteria and other conditions, other Swift services and products accessed through Alliance Lite2, such as FIN (MT messages), InterAct (MX messages), or generic FileAct in real-time mode in a many-to-many environment, in a Market infrastructure and a Member-Administered Closed User Group or in SCORE.
  In the case of FIN, the Alliance Lite2 user also automatically subscribes to RMA for Live operations.

By optional subscription, Alliance Lite2 also supports access to Swift Web Access services on SwiftNet, subject to applicable eligibility criteria and other conditions.

Delivery and standard set-up services

Each Alliance Lite2 user is entitled to a **welcome package** that includes the following item:
- a set of 10 USB hardware security tokens (personal tokens)

The software driver for personal tokens can be downloaded from Swift Certificate Centre.

Alliance Lite2 comes with mandatory set-up services enabling a faster implementation and a more efficient usage of the Swift connectivity. The set-up services are tailored to customer requirements. They ensure that customers acquire a basic understanding of Swift terminology, understand how to send files and messages using Alliance Lite2, are able to conduct day-to-day Alliance Lite2 tasks, and receive a configuration corresponding to their needs.

Additional options are available such as integration services. Each customer subscribing to Alliance Lite2 will receive an Alliance Lite2 *Set-up Services Service Proposal*, detailing the service offering and the specific legal terms applicable to the set-up services. For more information about set-up services, customers can contact their Account Manager.

2.1.2 Payable Configuration Changes

Definition

Alliance Lite2 comes with a default configuration in terms of operator profiles, unit definition, and messaging flows. Customers can request Swift to customise their configuration as a payable service. The configuration customisation can be requested either during the initial Alliance Lite2 set-up, through the set-up services, or later on, for ad-hoc changes, through configuration change requests that customers can submit to Swift Support. Swift reserves the right to reject configuration changes.

Customers can request confirmation from Swift regarding the feasibility and the price to customise their configuration. Customised requests and configuration changes that are related to the implementation of a new business flow into Alliance Lite2, or that are triggered by the implementation of a new project within the customer's organisation will be treated through a bespoke *Services Proposal*.

The possible configuration changes are divided into standard configuration changes and specific configuration changes, each with a different price. For the list of possible configuration changes, see List of Available Configuration Changes on page 46.

Note *Removing a configuration change should also be requested from Swift Support and is subject to a charge that will be specified in a separate Services Proposal.*

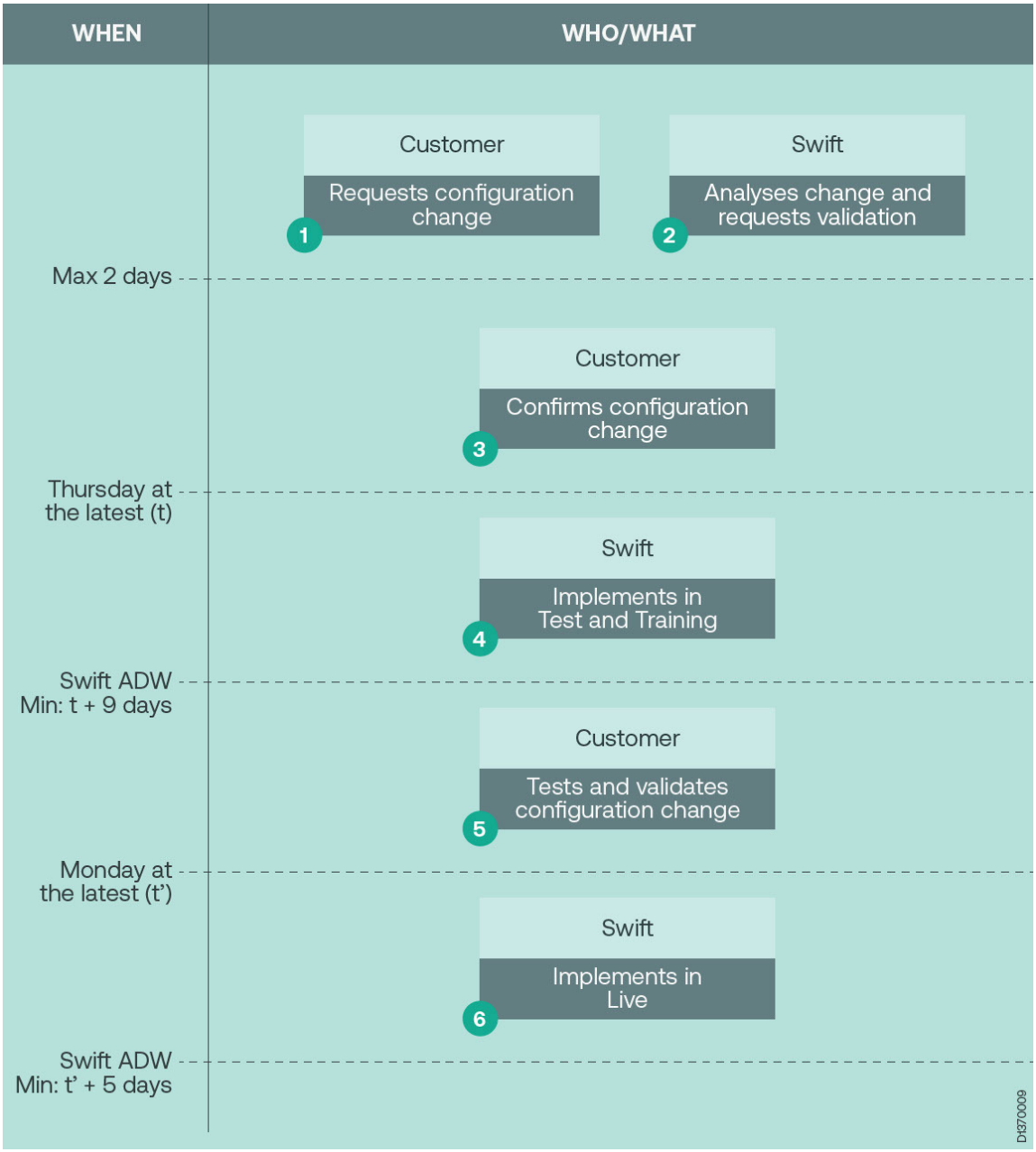
Implementation timeline for configuration changes

Swift analyses each configuration change request and confirms its findings with the customer. After customer confirmation, Swift first implements the change in the Test and Training environment, during an Alliance Lite2 allowable downtime window (see *Planned unavailability* in Service Availability on page 26), and then requests customer validation and confirmation in writing. When the customer has successfully validated and confirmed the change in the Test and Training environment, Swift implements the exact same change in the Live environment, during an Alliance Lite2 allowable downtime window (ADW).

A typical implementation thus requires a minimum of two Alliance Lite2 ADWs (that is, if provisioning is allowed during those allowable downtime windows) to have a configuration change implemented in the Live environment.

Alliance Lite2 configuration change estimated timeline

The implementation timeline of an Alliance Lite2 configuration change depends on the nature of the change request and the customer's prompt actions. The following table describes a typical configuration flow, for information purpose only:



Emergency requests

The implementation timeline (see Implementation timeline for configuration changes on page 10) is established based on the standard Swift change management process. Customers requiring the implementation of a configuration change sooner than the estimated default timeline can request this from Swift. Swift will review the request and accept or reject it at its full discretion. Swift will not implement those requests that will have an impact on the general availability of the Alliance Lite2 service. If accepted by Swift, an emergency request will be charged at an additional fee.

Cancellation requests

Once configuration changes are confirmed for implementation, requests to cancel the implementation will be considered as payable emergency requests. The same principle applies for requests to change the go-live date.

2.2 Live and Test Environment

The Alliance Lite2 offers two types of environments:

- **Live environment**
  This environment is used to send live business FIN (MT) messages, InterAct (MX) messages, and FileAct files, and to browse to live Swift Web Access services over SwiftNet (through an optional subscription).
- **Test environment**
  This environment allows users to exchange FIN (MT) Test and Training messages, InterAct (MX) test messages, and FileAct test files. It also allows users to test Swift Web Access services over SwiftNet (through an optional subscription).

Message validation in Test and Training

Swift implements the annual Swift Standards release in the test environment at least 6 weeks before the annual FIN Standards release changeover date, to enable customers to test in Test and Training mode.

For information about how to activate future mode testing, see Specific Configuration Changes on page 47.

2.3 Browser-based Screens

Features

The Alliance Lite2 browser-based screens offer various features as described in this section. The user's role profile determines which features the user can use.

Message creation

- Message creation through screens that indicate which fields are mandatory or optional, and that provide assistance in entering the values of fields, for example, with date pickers, code word drop-down lists, and BIC choosers.
  The message creation screens allow users to enter MT or MX messages, and support the full Swift Standards (all fields and options) of these MT and MX messages.
  Alliance Lite2 validates the messages against the Swift Standards syntax before sending them on to Swift, and reports any errors against the Swift Standard syntax to the user.
  Alliance Lite2 provides the possibility to use message drafts and templates (see Message drafts and templates on page 12).
- Optional creation of messages in 'fast' mode, which allows to enter (or copy and paste) a message in 'raw' MT or MX syntax.
- Upload of files with MT or MX messages
  Users can upload files with MT messages (RJE file format) or MX messages (XMLv2 file format). These messages can then be approved individually or in bulk on the screens.
- Alliance Lite2 supports the creation, modification, and reception of gpi-enabled messages.

Message drafts and templates

- Save messages as drafts

- Modify draft messages
- Save messages as templates
  Customer-defined templates allow the re-use of frequently used message data.
- Modify templates
- Create a message from a template

Message verification, approval, and sending

- Submission of messages for internal verification or authorisation, or for direct emission to Swift. The actions that are possible depend on the permissions of the user, and on the workflow as configured per the customer's requirements.
- 4-eyes authorisation of messages prior to emission.
- Verification of messages prior to authorisation. Verification is the blind re-key of important fields (such as amount) in the message by a second user that cannot see the value that was entered in that field by the first user.
- Message status and history (audit trail)
  Alliance Lite2 keeps track of the status of messages until they are sent. Alliance Lite2 reconciles acknowledgements (positive or negative) with the original sent message, and keeps track of a history (audit trail) per message. The audit trail indicates which users performed which actions on the message.

Note *Drafts or messages in an incomplete state will be kept available for a period of 14 days, after which they will be cancelled (completed).*

Messages awaiting approval will be kept available for a period of 14 days, after which they will be cancelled (completed).

Data retention

Alliance Lite2 keeps all messages and the related audit trails available online for a period of 124 days after the initial message emission or reception. After this 124-day period, as per a regular housekeeping process, Swift deletes the messages that are older than 124 days from the Alliance Lite2 database.

Note *Alliance Lite2 does not provide by default a local copy of all messages processed. If customers want to keep their messages for longer than the 124-day period, then they must request Swift to perform a configuration change that will ensure a local copy, throughAutoClient, of all their messages.*

Sending FileAct files

- Sending FileAct files
  Users can upload FileAct files using the browser-based screens of Alliance Lite2, enter the FileAct parameters on screen, and authorise (send) the file.
- FileAct get function
  Users can initiate a FileAct get using the browser-based screens of Alliance Lite2, to request the download of a FileAct file from a counterparty on SwiftNet.

Message and file receipt

- Receiving MT and MX messages
  Received messages can be viewed through the message search and report function.
- Receiving FileAct files
  Received FileAct files can be downloaded from the message search and report function.
- Viewing, searching, printing and reporting of messages in various formats (PDF, XLS, CSV, HTML)

Swift keeps all messages and related audit trails available online for a period of 124 days after the initial message emission.

Other functions

- Access to reference data: the entire BIC Directory, all ISO country codes and currency codes.
- Access to the Relationship Management Application (RMA)
  Alliance Lite2 allows users to exchange RMA authorisations with correspondents for the Relationship Management Application. Viewing and revoking RMA is supported, as well as RMA queries and answers.
- Use of security management functions
  Security management functions are under the sole control of the customer's Alliance Lite2 security officers and include the creation and the deletion of users on Alliance Lite2, and the assignment of roles to these users. These functions also include access to Swift's Online Operations Manager for the creation of SwiftNet distinguished names, the generation of initial activation codes for personal certificates and for channel certificates, and the assignment of SwiftNet roles (RBAC roles) to users.
- Swift Web Access over SwiftNet
  Customers who have subscribed to the Swift Web Access service on SwiftNet can browse to that service through Alliance Lite2.
- Extraction of information from event journals or audits trails
  Alliance Lite2 does not allow customers to extract information from event journals or audit trails. In the exceptional circumstance where the investigation of a problem requires information from event journals or audit trails, customers can request Swift to extract the information by referring to specific logs (for example, date, operator ID). Swift is not in a position to act upon general or extensive requests to retrieve data from those databases.

Related information

Users' Responsibilities on page 35
Alliance Lite2 User Guide
Alliance Lite2 Administration Guide

2.4 AutoClient

Features

AutoClient is an application that provides file-based communication to and from the FIN, InterAct, and FileAct services through the Alliance Lite2 server.

With AutoClient, users can send and receive the following types of messages and files in a fully automated way:

- **FIN MT messages in a simple text file format (RJE format, XMLv2)**
  Files that use the same format as on Alliance Access or Alliance Entry. These files can contain any MT message, including system messages (for reception only), with the exception of Select/Quit and MT 047. Received files can also contain the positive or negative acknowledgements for sent messages.
  Several RJE or XMLv2 messages can be included in a single file.

  Note *To receive files in XMLv2 format, a configuration change in AutoClient is required and can be requested toSwift.*
- **MX messages in XMLv2 file format**
  Files that use the same format as on Alliance Access or Alliance Entry. These files can contain any number and type of MX messages. Note that to use this feature, AutoClient version 1.2.1 or above is required.

- **FileAct files**
  Files of any format (proprietary, domestic, national or counterparty-specific format) and formatted to the extent required by the specifications of the Closed User Group or the service provider.
  To send FileAct files, AutoClient requires parameters. These parameters are contained in a parameter file (also called companion file) that can be in either of the following three formats:
  - Text format, compatible with Alliance Lite2
  - XML format, compatible with Alliance Lite2
  - XMLv2 format, compatible with Alliance Access

A configuration file can be used, by the Alliance Lite2 administrator, to avoid that the customer's application has to provide these parameters.

Folders

Users prepare files on a back-office application for transmission, and then AutoClient directs the files to the Alliance Lite2 server through a directory structure.

AutoClient makes received files available to a customer's back-office application using the same directory structure. The received files can contain messages from other Swift users, messages about the status of the files sent through AutoClient, or can be FileAct files. By default, ACKs/NAKs of messages created in the browser are not returned to AutoClient. Using AutoClient customers can download a maximum of 30 days of messages. AutoClient downloads received files only once.

AutoClient processes the content of the following pre-defined folders:

- **Emission folder**
  Contains all files that Alliance Lite2 is due to transmit.
- **Reception folder**
  Contains all files that Alliance Lite2 receives for the correspondent.
- **Errors folder**
  Contains errors generated by AutoClient (FIN, MX, and FileAct).
- **Archive folder**
  Contains any file that has successfully been transmitted by Alliance Lite2.

Message handling

On the Alliance Lite2 browser-based screens, operators can view individual FIN and MX messages that AutoClient has imported through RJE files and XMLv2 files. They can approve or reject these messages, either individually or in bulk.

By default, files and messages submitted through AutoClient to the Alliance Lite2 server do not require an approval. However, customers can request a manual approval configuration.

Files exchanged between the customer back-office and the AutoClient software can be locally checked for authentication and integrity of the information.

Operation

1. AutoClient runs in the background and therefore does not have a user interface.
2. Operators can check the AutoClient icon in the Windows taskbar to see the status of AutoClient, that is, whether it is running or not. Operators can click this icon to start or to stop the AutoClient monitoring. Alternatively, operators can use the Windows command line to check the status of AutoClient, and to start or stop it.

3. Operators must monitor that the uploaded files are moved from the emission folder to the archive folder, which indicates the successful upload of the file, and they must check the error folder for files that fail to be uploaded. They must also ensure that acknowledgements are received in the reception folder for sent MT or MX messages, and that files with a `.ok` extension are received in the reception folder for sent FileAct files.
4. Operators can start AutoClient from the Windows taskbar, from the Windows start menu, or from the Windows command line.
5. The customer's security officers can activate several AutoClient tokens, or AutoClient channel certificates, if desired. This allows to set up several standby instances of AutoClient. Only one AutoClient instance should be active (started and running). If two or more AutoClient instances are running at the same time, then they will all receive the same messages and files. If a (standby) AutoClient instance is started, then it will automatically receive all files that this instance has not yet received, up to maximum 30 days history.

Related information

Users' Responsibilities on page 35
Alliance Lite2 AutoClient User Guide

2.5 Integration Options

Features

For the users of the Alliance Lite2 platform who have more complex requirements for message processing,Swift offers two products, Swift Integration Layer and Alliance Lite2 Direct Link, as outlined in Overview of Alliance Lite2 on page 6.

Alliance Lite2 Direct Link is an integration product providing core transformation and connectivity services, in which custom logic is developed to address the specific integration requirements of customers connecting to SwiftNet using Alliance Lite2.

This section outlines the features and functions included in Alliance Lite2 Direct Link and Swift Integration Layer.

Wherever this document specifies that a task is the customer's responsibility, that task may be performed, at the customer's choice, by one of the following entities or means:

- the customer
- Swift Professional Services

Related information

Users' Responsibilities on page 35
Alliance Lite2 AutoClient User Guide
Alliance Lite2 Direct Link User Guide

2.5.1 Integrating with Business Applications

Connectors for business application connectivity

Swift Integration Layer, the Swift integration technology embedded in Alliance Lite2 Direct Link, provides a large number of low-level connectivity libraries, often referred to as 'qualified adapters'. Some of the most commonly used are, for example, File, Web services, IBM MQ. These libraries enable customers to build connectors for most business applications.

Note *Swift Integration Layer is no longer offered to new customers.*

Swift Message standards

Alliance Lite2 supports the following message standards:

- MT message structure that can be found in Swift libraries, which are located in and used by the mapping tool of Alliance Lite2 Direct Link .
- MX messages (Universal Standards Archives available from Swift or schemas available from the ISO 20022 web site)

Data, file, formats, and transformations

Business applications can exchange information with Alliance Lite2 Direct Link in almost any format. Some examples of formats are comma-separated value (CSV), fixed-length records, Microsoft Excel files, or RJE files. The custom logic defined as part of an integration project can transform the content from a proprietary format to a Swift standard format, and vice versa.

Content of a file to be sent from a business application to Alliance Lite2 can be transformed to contain MT or MX messages.

Likewise, flows handling files received from Alliance Lite2 can transform the content to messages in a proprietary format, MX-formatted messages, or MT-formatted messages.

File content for pass-through flows in either direction is transparent to Alliance Lite2. A pass-through flow can include messages in any format relevant for the sender and the receiver.

2.5.2 Message Validation and Transformation

Message validation requires custom logic

Alliance Lite2 Direct Link does not provide any message validation out of the box. A customer must work with Swift Professional Services to determine specific validation needs in the scope of an integration project. Based on the agreed needs, custom logic for validation can be developed for use in a customer's environment.

Optional proprietary message validation

Custom logic can be implemented to validate content of proprietary messages before they are transformed to MT or MX messages.

Optional MX schema validation

Custom logic can be implemented to support MX schema validation. Swift Professional Services can develop any custom logic needed to perform cross-field validations or other validations.

Optional FIN semantic validation

Custom logic can be implemented to support FIN semantic validation. Swift Professional Services can develop any custom logic needed to perform cross-field validations or other validations for ISO 7775/15022 message formats.

Support for message format transformation

Alliance Lite2 Direct Link does not include any pre-built transformation services for business messages. Swift Professional Services can implement any necessary transformation logic, using the features provided with Alliance Lite2 Direct Link.

On the flow from a business application to Alliance Lite2, custom logic implemented in Alliance Lite2 Direct Link can transform proprietary messages to Swift standard message formats. Custom logic must also be developed to transform the related ACK/NAK or notifications.

On the flow from Alliance Lite2 to a business application, custom logic implemented in Alliance Lite2 Direct Link can transform standard MT, MX, or FpML messages to the customer's proprietary format.

Transformation tools

Alliance Lite2 Direct Link includes a mapping tool to assist Swift Professional Services in the development of custom logic for transforming proprietary messages to Swift standard messages and vice versa. Alliance Lite2 Direct Link includes utilities that Swift Professional Services can use for transformation to and from the structures needed for data exchanged with Alliance Lite2.

2.5.3 Business Flows Definition

Identify generic patterns

Swift Professional Services and customer staff must jointly discuss the processing needs for an integration project. Further analysis must then identify the relevant patterns to use when developing custom logic for business flows.

Alliance Lite2 Direct Link supports generic integration patterns. Under specific conditions, some of the following generic patterns could be used:

- **Single to single**
  A single message of one format is transformed to a single message of a different format. A file containing multiple messages is processed without transforming any messages in the file (that is, a pass-through flow).
- **Group to group**
  A group of messages, typically a file, is split into individual messages, each of which is transformed to a different format. The transformed messages are subsequently grouped again and sent for further processing.
- **Singles to group**
  Individual messages are grouped according to a set of criteria. The resulting group of messages is sent for further processing.
- **Group to singles**
  A group of messages is split into individual messages, each of which is transformed to a different format. The resulting individual messages are sent for further processing.

Combining patterns into flows

The generic patterns can be seen as building blocks. When these patterns are used with specific connectors and flow direction is considered, most basic integration activity can be modelled.

Swift Professional Services performs analysis using generic patterns and enterprise integration patterns in their activities to develop custom logic for integration projects. The mapping for proprietary message exchange requires more specific analysis and development.

2.5.4 Monitoring

Event logging

Swift Integration Layer, the Swift integration technology embedded in Alliance Lite2 Direct Link, generates both business-related events and technical events. These events are visible through the audit trail monitoring feature. The audit trail content can be viewed as XML or CSV.

E-mail distribution of events

Through Swift Professional Services, customers can configure Alliance Lite2 Direct Link to use e-mail to report events. The event reporting by means of e-mail is based on the severity level of events that Alliance Lite2 Direct Link logs. Such e-mail must be sent within the customer's SMTP infrastructure.

2.5.5 Resilience

Alliance Lite2 Direct Link is a lightweight and stateless product without any message storage. As such, it relies on the resiliency of the customer's business application connector and on Alliance Lite2.

To assure smooth recovery in the event of an outage of Alliance Lite2 Direct Link (due to process stoppage or hardware issues, for example) all aspects of the recovery procedure must be analysed. Swift Professional Services, together with the customer, must design, implement, and test recovery aspects in the scope of an integration project.

2.5.6 Solution Configuration

Connector configuration

The customer needs to configure connectors as appropriate to allow exchanging content between a business application and Alliance Lite2 Direct Link in respect to its specific requirements and infrastructure.

Note *Swift Integration Layer is no longer offered to new customers.*

Integration solution configuration

Swift Professional Services may develop custom logic that requires a customer to define configuration settings. Such settings could be related to connectivity with a business application, or could be related to parameters needed for integration logic to work properly. Alliance Lite2 Direct Link provides a mechanism allowing customer operations staff to define any required settings for the integration solution.

Storage of configuration settings

The configuration uses a properties file to store relevant values. The properties file provides a way to indicate if a value such as a password needs to be stored as an encrypted value.

If needed, configuration settings defined in a properties file can be updated after an integration solution has been deployed. Typically the updated values are available for use after a restart.

2.6 Types of End Users

AutoClient operator

An AutoClient operator, appointed by the customer, controls the running of the AutoClient application, and integrates it with the back-office application.

Business user

A business user can use the browser-based screens to create, view, and approve messages, access Swift Web Access services, and other screen functions, according to the roles assigned to this user by the customer's security officers.

Security officer

The two Alliance Lite2 security officers appointed by the customer are responsible for the following tasks:

- configuration of Alliance Lite2, and creation, maintenance, and deletion of the records of the business users
- generation of the initial activation codes for the personal certificates, and handover of the initial activation code to the intended user or AutoClient operator
- generation of the initial activation code for the channel certificates, and handover of the initial activation code to the intended AutoClient operator
- assignment of roles to business users

The Alliance Lite2 security officers must have access to the Swift Online Operations Manager and to the Swift Secure Channel application (for offline intervention requests in case online access is not available).

Swift recommends that security officers, through the Swift Online Operations Manager, request the generation of a report for all certificates on a monthly basis to be able to monitor the certificate expiry dates and to renew them on time.

Shared security officer

When subscribing to Alliance Lite2, the customer acknowledges and accepts that Swift is automatically appointed as shared security officer with respect to the storage and the management of the customer's SwiftNet PKI certificates. Swift applies the 4-eyes principle when performing SwiftNet PKI certificates management. Any other reference to security officers contained in this service description or other related documentation will be deemed to be made only with regard to the Alliance Lite2 security officers appointed by the customer himself as explained in Security officer on page 20.

Related information

SwiftNet Online Operations Manager User Guide

2.7 Security Features

Swiftpersonal hardware tokens (USB tokens)

The left Alliance Lite2 security officer receives from Swift a box of hardware tokens (USB tokens). The right Alliance Lite2 security officer receives by e-mail the initial token password that was assigned to all the tokens in the box.

To activate the tokens, the left and right security officers must first work together to submit a Secure Channel security request ('recover a pki certificate'). When Swift has processed the

request, the security officers receive an e-mail containing a link to the Swift Certificate Centre where they can activate their own token. The security officers then assign a password to their token, which is only known by themselves.

It is the responsibility of the Alliance Lite2 security officers to configure the tokens for the business users and for AutoClient. Swift offers the services of Swift-certified engineers to assist with this initial set-up.

Each Alliance Lite2 security officer and each Alliance Lite2 business user has a personal hardware token. The security officer or the business user must plug his own token into a USB port of the computer, and then must enter the token's password each time the token is used. After five consecutive failed attempts to enter the valid password, the token is locked.

A token contains a certificate and its private key, a processor chip, and the algorithm to calculate the digital signature on the token. The private key of the certificate never leaves the token. The certificate operates at a personal level. It is not possible to put other software or data on these tokens.

Channel certificates

A channel certificate is an encrypted, disk-based profile file that provides a way for Swift to authenticate the identity of an application. The Alliance Lite2 AutoClient application is authenticated through a 2048-bits PKI private key that is generated at customer premises.

Alliance Lite2 supports channel certificates as an alternative means to physical tokens for securing the connection between the Alliance Lite2 AutoClient or Direct Link instance at customer premises and Swift.

Alliance Lite2 supports channel certificates on Windows, yet channel certificates mandate the use of the Swift VPN connection over an Alliance Connect product (VPN connectivity packs) that belongs to the owner of the channel certificate. To prevent misuse of channel certificates, Swift ensures that channel certificates cannot be used by a VPN connectivity pack having an IP address outside the range of IP addresses that is linked to the BIC of the certificate. In addition, channel certificates are only permitted for application-to-application flows, not for human-to-application flows, such as browse services.

The policy ID for channel certificates is 1.3.21.6.3.10.100.1.

Token management functions

For token management functions, see the Swift Certificate Centre Portal User Guide.

Back-up security officer

Swiftstrongly recommends that the two Alliance Lite2 security officers appoint a third person as the back-up in case one of the two Alliance Lite2 security officers is not available. For example, if one of the Alliance Lite2 security officers has left the customer's institution, then the two remaining Alliance Lite2 security officers can perform the necessary actions, for instance, retrieve the USB token, revoke the certificate and remove the associated www.swift.com administrator account of the security officer that has left the customer's institution, grant the security officer role to new security officers. These actions require the authorisation of two security officers, therefore it is necessary that a third security officer token is created and approved.

If one of the security officers changes, then the customer must inform Swift by registering the new user on www.swift.com and then registering this new user as an offline security officer by means of the Swift Secure Channel application.

For more details about the procedure, see the Knowledge Base article 5017169.

4-eyes principle

The following operations are carried out under the 4-eyes principle:

- **Creation and modification of the Alliance Lite2 user records**
  Requires the approval of at least two Alliance Lite2 security officers.
- **Dual processing of messages created in the browser-based screens**
  A central workflow handles the message creation and approval. Alliance Lite2 security officers can configure the application in such a way that a second business user must approve a message before that message is released to Swift. Swift strongly recommends that the Alliance Lite2 security officers configure the application in such a way that two different business users must process a message before that message is released to Swift. Swift recommends that this dual processing of messages is performed on two different PCs.
- **Approval of transactions from AutoClient**
  By default, files and messages submitted through AutoClient to the Alliance Lite2 server do not require approval. Swift strongly recommends that Alliance Lite2 customers request Swift for a configuration change in such a way that the transactions from AutoClient must be approved before they are released to Swift.

Business user profiles

Business users can have specific profiles, such as creator, approver, or viewer. It is also possible, upon request, to make payable configuration changes, to define amount limits per transaction for the creation and the approval of transactions, and to establish an approved list of usable bank accounts, known as whitelisting.

PKI-based security

Alliance Lite2 customers are identified on SwiftNet using BICs, just like any other SwiftNet customer.

All SwiftNet messages or files initiated by, or intended for, Alliance Lite2 customers are signed with standard SwiftNet PKI certificates associated with the BICs of the customer, like any message exchanged between other SwiftNet customers.

Relationship Management Application authorisation messages must also be exchanged with Alliance Lite2 users when required, such as for authenticated FIN messages.

A BIC identifies each Alliance Lite2 customer, and the Alliance Lite2 user has two identities:

- one identity for access to the Alliance Lite2 server
- a second identity to exchange messages or files over SwiftNet. Only the second identity is visible to other SwiftNet customers.

An Alliance Lite2 user is authenticated towards the Alliance Lite2 server through a 2048-bit PKI private key that is generated at the user's premises. That PKI credential is protected in, and never leaves the FIPS 140-2-level3-compliant USB token.

The USB token uses the private PKI key to sign the most sensitive operations that the user creates and sends to the Alliance Lite2 server. To activate the USB token, the user must enter the password.

Encryption

All exchanges with Alliance Lite2 through the Internet are fully encrypted using standard HTTPS (TLS 1.2) and a strong encryption algorithm.

Note *A strong encryption algorithm means the highest priority with the Cipher Suite TLS_RSA_WITH_AES_256_CBC_SHA.*

Local Authentication option on AutoClient

Users can, optionally, configure AutoClient to check and produce a signature (Local Authentication [LAU]) that accompanies FIN MT (RJE or XMLv2) files, and/or FileAct files, and/or XMLv2 files. This LAU signature protects these files from tampering, when the files are in transit between AutoClient and the customer's application that produces or processes these files.

Implementing LAU is optional. When LAU is implemented, a secret key is shared between AutoClient and the customer's application at the time of configuration. Both the AutoClient and the customer's application verify and produce LAU signatures in accordance with the algorithm that is described in the Alliance Lite2 AutoClient User Guide. Swift strongly recommends configuring/using LAU between the customer's application and AutoClient.

2.8 Accessing the Alliance Lite2 Software

Key components

The Alliance Lite2 application consists of the following components:

- **The Alliance Lite2 browser-based screens**
  The Alliance Lite2 browser-based screens run inside a standard Internet browser. To connect to Alliance Lite2 GUI, it is required to have Web Connect or SConnect (until the end of the co-existence period) installed.
  To access the Alliance Lite2 browser-based screens, business users must insert their personal hardware security token into a USB port of the PC from which they access the application. To use this hardware security token, users must install driver software on the Microsoft Windows workstation. Users can find this driver software in the Swift Certificate Centre.
- **AutoClient**
  AutoClient has specific software that users must install on the AutoClient PC. Users can find the AutoClient software in the Alliance Lite2 box, or they can download the AutoClient software from the Download Centre.
  Users of AutoClient must insert an AutoClient hardware security token into a USB port of the PC on which AutoClient is installed. Alternatively, AutoClient can be configured with a channel certificate. In that case, no token or USB port is required to use AutoClient, however AutoClient must connect to Swift over Alliance Connect VPN connectivity packs.
  Windows administrator rights are required to install the AutoClient software. The same rights are required to install the driver software for the hardware security tokens for the Alliance Lite2 browser-based screens and AutoClient.
  Users can operate Alliance Lite2, both browser and AutoClient, from a Windows account that does not have Windows administrator rights.
- Swift Integration Layer and **Alliance Lite2 Direct Link**
  Swift Integration Layer and Alliance Lite2 Direct Link are supported on Microsoft Windows and Red Hat Enterprise Linux operating systems. Depending on the operating system, a customer can optionally run Swift Integration Layer as a Windows service or a daemon (on Linux). Note that hardware security tokens are not supported on Linux.
  Swift Integration Layer and Alliance Lite2 Direct Link do not provide a GUI.
  The lightweight nature of Swift Integration Layer and Alliance Lite2 Direct Link enables for an easy-to-manage, highly resilient integration solution. This lightweight nature also means that functions dependent on message storage, such as message archive and message investigation, are not available within Swift Integration Layer and Alliance Lite2 Direct Link.

Swift Integration Layer and Alliance Lite2 Direct Link are stateless and therefore do not persist business messages for recovery or message search. These functions are handled for the emission flow by either the business application or middleware, and for the reception flow by Alliance Lite2.

Limitations on use

Any software supplied as part of the Alliance Lite2 application, including any embedded third-party software, is for use by Alliance Lite2 users only, and must be used to access and use Alliance Lite2 only or other Swift services and products as authorised in other applicable documentation.

2.9 Accessing Swift Messaging Services

Alliance Lite2 servers

Swift operates Alliance Lite2 servers (see Overview of Alliance Lite2 on page 6). These servers contain a SwiftNet Interface, which includes a FIN interface also called computer-based terminal (CBT), an MX InterAct interface or CBT, a FileAct interface and a secure access to Swift Web Access services on SwiftNet (through an optional subscription). Swift operates these services to serve Alliance Lite2 customers.

Sending messages and files

Swift sends FIN (MT messages), InterAct (MX messages), or FileAct files over SwiftNet pursuant to instructions received from the Alliance Lite2 users.

The central infrastructure FIN or MX computer-based terminal or SwiftNet interface starts sending these messages or files within minutes of the customer's instruction to send (through the browser-based screens or AutoClient), and reports on (positive or negative) acknowledgements returned by SwiftNet. If applicable to the FIN message, this FIN computer-based terminal also reports MT 010 non-delivery warnings, MT 011 delivery notifications, MT 012 notifications, and MT 019 abort notifications.

For FIN messages that are sent from the Alliance Lite2 browser-based screens or AutoClient, the customer can choose the delivery option (that is, N, N2, U1, or U3). For MX messages, the customer can specify that the normal priority is used to send messages. In all cases, the Alliance Lite2 interface reports the status of the sent message.

For manually entered messages, the messages should have a **Swift completed** status within 10 minutes after final approval. Messages sent using AutoClient should appear in the Alliance Lite2 interface within 30 minutes (with a **Swift live** status), and then have a **Swift completed** status within 10 minutes. These time limits are valid if the permitted usage (see "Permitted usage" of Service Availability on page 26) is not exceeded. If it is not the case, then the customer must contact Swift Support to investigate.

Alliance Lite2 customers can send and receive RMA messages in Live and Test and Training mode.

Swift rejects FileAct files that are sent with parameters (for example, service name) that are not permitted by the customer's profile.

Receiving messages

Swift processes all FIN and MX messages in real-time mode. They are displayed on the browser-based screens for Alliance Lite2 users, and Swift also forwards them to the customer's AutoClient.

Swift GPI unique end-to-end transaction reference (UETR) field

For certain FIN messages, Alliance Lite2 automatically generates a unique end-to-end transaction reference (UETR) in the MT header. A UETR is a unique end-to-end transaction reference in the MT header: field 121. This field provides an end-to-end reference across a payment transaction.

For more information, see the Alliance Lite2 User Guide.

Swift's responsibilities

Swift performs certain verifications on the signature of messages, as set out in the requirements described in the FIN Service Description.

Swift is responsible for the protection and the use of the SwiftNet PKI certificates of the Alliance Lite2 users.

Swift signs messages and files on behalf of the Alliance Lite2 user with its PKI certificates.

Swift keeps and protects customer's data, messages, and files on Swift systems as further detailed in Protection of Customer Information on page 25.

2.10 Protection of Customer Information

Data retrieval

Alliance Lite2 is provided from and data is processed at Swift's Operating Centre(s) in the Netherlands and Switzerland. Swift will inform customers in advance of any changes to these locations.

Messages and files sent or received by the Alliance Lite2 user are stored by Swift on the Alliance Lite2 servers, located in the active data centre in the European Union, and are available for consultation or download by the Alliance Lite2 user. In case of unplanned unavailability (see Service Availability on page 26) and disaster recovery (see Alliance Lite2 Service Levels on page 50), the above messages and files are stored by Swift on the Alliance Lite2 servers located in Switzerland.

Customers can find more information about the consultation and download of messages from the Alliance Lite2 servers in Browser-based Screens on page 12, and more information about the download of files in AutoClient on page 14.

User space

Swift provisions each customer with a user space on the Alliance Lite2 server that can be used by operators to perform manual file uploads. Swift provides this user space as a temporary file storage. Customers are responsible for removing files from this location after successful file emission. Swift will automatically delete from these individual user spaces the files that have not been modified during the past 10 days.

2.11 Service Availability

Operational status

Swift displays the operational status of the Swift services at www.swift.com > MySwift > Swift Service Alert.

It is the customer's responsibility to consult any notifications about the operational status of the Swift services.

Planned unavailability

Swift plans for specific dates and times when the service, or the Swift Web Access, FIN, FileAct or SwiftNet service will be unavailable.

Planned unavailability can be for various events including the following:
- downtime due to scheduled equipment maintenance
- scheduled system or service changes
- business continuity activities

Swift performs system changes and maintenance during planned unavailability windows.

During these downtime windows, Alliance Lite2 may be unavailable either for the whole duration of the downtime, or only intermittently.

For information about the scheduled downtime, see the Planned maintenance page on swift.com.

Swift notifies customers in advance of planned unavailability. Swift recommends that customers subscribe to the products and services notifications to be notified of any maintenance updates. For more information about the notifications subscription, see the Swift Service Alert page on swift.com (Subscribe to notifications).

Unplanned unavailability

If Swift becomes aware of a problem in the Alliance Lite2 service, then Swift will initiate any recovery or fallback operation for which it is responsible and that is necessary to restore the service.

In the extreme event that the operating centre where Alliance Lite2 is running becomes unavailable, Swift will restore the Alliance Lite2 live services in a standby infrastructure located in another operating centre. the standby disaster recovery infrastructure then becomes the main infrastructure.

The standby operating centre is deployed as a cold standby infrastructure. This means that the standby server infrastructure is ready and configured, and that the configuration data it contains is identical to the data that was on the primary site at the time of the last data synchronisation. Customers will need to undertake certain actions to be able to continue using Alliance Lite2. These actions will be detailed in a disaster recovery guide that will be distributed to customers as and when required.

The Alliance Lite2 service is available through the Internet. the availability of the Internet network route between the customer and the Alliance Lite2 servers is not under Swift's control. Therefore Swift disclaims any liability for unavailability of the Internet network route. Users seeking service level guarantees on the connection between their premises and the Alliance Lite2 server should use Swift's VPN with the Alliance Connect or Alliance Connect Virtual products of Swift, and use lines from Swift's network partners with guaranteed service levels.

The levels of service that this document specifies assume normal operating conditions. These include resilient operations during most single-component failure scenarios within the active Swift operating centre where Swift runs the Alliance Lite2 service. the Alliance Lite2 service is designed to handle many anomalous events without impact to the activities of the Alliance Lite2 subscribers and users. However, under certain, very unlikely, disaster scenarios (for example, the complete unavailability of a Swift operating centre, dual failures of similar components), Swift may be unable to meet these levels of service, in whole or in part.

Availability

Outside the allowable downtime windows and the cases of planned unavailability as described above, Swift provides the Alliance Lite2 service 24 hours per day, 7 days per week, all year long.

Permitted usage

Alliance Lite2 has been designed to meet the needs of most customers with regard to traffic volumes, performance, and resilience. Customers with specific requirements that are beyond what can be considered as standard usage are not permitted to use Alliance Lite2 and are advised to use an on-premise infrastructure. In case the usage of an existing Alliance Lite2 customer evolves over time to a point where it is no longer considered as permitted usage, Swift reserves the right to terminate the customer's Alliance Lite2 subscription at any moment.

Swift recommends the use of on-premises FIN and SwiftNet interface solutions for Market Infrastructures such as central banks and Central Securities Depositories (CSD) that want to connect to Swift. This connectivity option ensures the highest level of business continuity for Market Infrastructure customers and the communities they serve. Alliance Lite2 should not be used by Market Infrastructures to operate their own service to their community (such as an RTGS, or a SwiftNet browse service for CSD application). For other types of usage, even though not recommended, Alliance Lite2 could be offered, on a case by case basis, after acceptance from the Market Infrastructure of the current Cloud services capabilities in terms of volume, throughput and latency. Authorisation to use Alliance Lite2 should be granted by Swift.

Usage limits: Alliance Lite2 supports the following:

- Daily volume
  - FIN: 10,000 messages per day in each direction
  - MX: 8,000 messages per day in each direction
  - FileAct: 1,200 files per day in each direction

  A total of 24,000 messages per day in both directions for FIN and MX combined.
- GUI/browse users
  - up to 10 concurrent users
  - up to 20 defined users (maximum 20 tokens)
- Throughput
  - maximum 2,500 FIN messages per hour
  - maximum 2,000 MX messages per hour

  These maximum throughput volumes are achievable only if multiple messages per file are submitted to the AutoClient by means of back-office message batching.
- Business flows configuration
  Alliance Lite2 supports simple and a limited number of business flows configurations.

3 System Requirements

Operating systems for use with Alliance Lite2

Alliance Lite2 is qualified to operate with Microsoft Windows. Customers can find details about the operating system levels and releases in the Alliance Lite2 Administration Guide, the Alliance Lite2 AutoClient User Guide, and the Alliance Lite2 Direct Link User Guide.

Note *Alliance Lite2 can be installed and used on a Windows system running under virtualisation technology. The use of Swift's security hardware tokens requires that the virtualisation technology supports USB ports. Channel certificates do not require USB support. Given the variety of possible virtualisation technologies, Swift refrains from formally qualifying its software, including Alliance Lite2 AutoClient, on such virtual environments. Instead, customers should seek assurance and support from the vendor of the virtualisation technology. Swift has not qualified the release under any virtualisation technology.*

Operating systems for use with Alliance Lite2 Direct Link

For system requirements related to Alliance Lite2 Direct Link, see to the Alliance Lite2 Direct Link User Guide.

Connectivity

Alliance Lite2 requires the following connectivity:

- Customers are strongly recommended to use Alliance Connect or Alliance Connect Virtual from Swift. Customers can also use standard broadband Internet access with minimum 128 kbps (for example, ADSL). Dial-up connections are not supported.
- HTTPS over TLS 1.2 over standard TCP port 443 for the Alliance Lite2 web interface and for AutoClient. When using the AutoClient configuration tool to create a channel certificate, TCP port 49171 must also be open.
  The TCP connections are always initiated by the browser or AutoClient, towards the Alliance Lite2 servers.
  The Alliance Lite2 servers never initiate TCP connections towards the customer.
- Alliance Connect or Alliance Connect Virtual when channel certificate is used.

Alliance Lite2 Direct Link requires connection to Swift's Virtual Private Network (VPN). Customers must subscribe to one of Swift's Alliance Connect / Alliance Connect Virtual products to use the Swift VPN, also called the Swift Secure IP Network (SIPN). For connectivity details, refer to the selected Alliance Connect / Alliance Connect Virtual product documentation.

Compatibility with other security tokens

To be able to use the USB security token (SafeNet eToken PRO, SafeNet eToken 5110), Alliance Lite2 requires the appropriate SafeNet driver. The SafeNet driver installed by Alliance Lite2 can replace SafeNet drivers or DataKey drivers or Alladin drivers that were already present on the PC. Customers who still need these previous versions of the drivers must install Alliance Lite2 on a different PC.

The use of other USB security tokens at the same time as the Alliance Lite2 token can lead to conflicts. Therefore, Swift recommends that users only insert and use the Alliance Lite2 token and that no other tokens are inserted in USB ports of the same PC.

Web Connect or SConnect is required to connect to the Alliance Lite2 user interface. For more information about how to install Web Connect or SConnect, see the Alliance Lite2 Administration Guide.

To connect to Alliance Lite2 and the recommended setting during the hybrid period, see KB tip - How to connect to Alliance Lite2 GUI (6000534).

Related information

Alliance Lite2 AutoClient User Guide
Alliance Lite2 Direct Link User Guide
Alliance Connect product page

4 Third-Party Software

The following third-party software is embedded in the Alliance Lite2 AutoClient:

- Oracle Java 2 Standard Edition (J2SE) (Runtime Environment)
- Bouncy Castle Java

Swift Integration Layer, the Swift integration technology embedded in Alliance Lite2 Direct Link, embeds certain third-party software, in whole or in part, which is described in the *Swift Integration Layer Installation Notice*. This Installation Notice is contained within the software medium.

The customer acknowledges that it may not under any circumstances use any third-party software (whether specifically identified in this service description or not) embedded as part of Swift Integration Layer for any function other than as an integral part of Swift Integration Layer. Any misuse of such third-party software by the customer may subject the customer to a revocation of the right to use Swift Integration Layer.

5 Ordering

Order Swift services and products

To use Swift services and products, a customer must subscribe to, or order, the relevant services and products.

Related information

For information about Swift's online ordering facility and how to order, see www.swift.com > MySwift > Ordering.

New and existing customers

New customers who order Alliance Lite2 will first be requested to register as a Swift customer before the order is processed. Existing customers who are already connected to Swift, can migrate their existing connection (BIC) to Alliance Lite2, or order Alliance Lite2 as an additional connection (for an additional BIC).

Export restrictions

Due to export control and other sanctions programmes, Alliance Lite2 may not be supplied or made available to certain customers. If you have any questions about your particular status regarding the various export control and/or sanctions programmes, then contact your regional support centre.

Alliance Lite2 also incorporates certain third-party technologies. These items are controlled by the U.S. government and authorised for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) identified in ordering documents. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorised ultimate consignee or end user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorised by U.S. laws and regulations.

6 Support and Care Services

6.1 Support

Support for Swift customers

By default, Swift Support is the single point of contact to report all problems and queries that relate to Swift services and products. Swift Community Support is available to all Swift customers.

Individuals within a customer organisation must register on swift.com to use the Support service. On top of the Swift Community Support, customers can purchase the Advanced Support and Care Services.

Swift automatically registers the Alliance Lite2 customer security officers, specified at ordering time, as users of the Support service. Other users within a customer organisation must register to get access to the Support service.

Subscription to Alliance Lite2 includes the Swift Community Support package.

For more information about the different services that Swift offers as part of the Swift Advanced Support and Care Services and the procedure to order support, see Support and Care Services on swift.com.

Swift provides support for Swift services and products only. For example, Swift does not offer support for the underlying hardware and software systems (operating system, third-party messaging middleware) which are used in conjunction with the Swift product. In case of problems or queries that relate to those third-party hardware or software systems, customers must contact the responsible vendor.

Related information

For more information about Support services, see the Service Description related to the applicable support package: Support documentation.

6.2 Care Alliance Lite2

Alliance Lite2 customers can opt to purchase the Care Alliance Lite2 offering. By default, when customers contact a Swift Support Centre, Care Alliance Lite2 includes the 'Remote Access' and 'Hands-On Assistance' service modules. Customers can purchase additional service modules from the Advanced Support and Care Services portfolio to include 'Case Reviews and Management Escalation' and 'days of Swift effort' related to maintenance activities. For full details, see the Swift Care Services Service Description.

7 Swift Training

Swift provides training about standards, products, and services to suit different needs. From tailored training to self-paced e-learning modules on Swift Smart, a range of training options is available for all Swift end users.

Swift Smart

Swift Smart is an interactive, cloud-based training service that offers a large variety of courses for different levels of knowledge. The courses contain exercises and quizzes and are available in multiple languages. The Swift Smart catalogue provides a list of courses that are organised into these learning tracks:

- General knowledge
- Work with messages
- Deploy and manage Swift software solutions
- Security and audit
- Compliance and shared services

Swift Smart is accessible from the desktop or a mobile device. No installation is required.

Swift Smart is available to all connected Swift end users and registered Swift partners with a swift.com account. For more information, see How to become a swift.com user.

Tailored training

A full range of tailored programmes is available to meet specific training needs. For more information, visit the Training web page.

8 Roles and Responsibilities

8.1 Swift Integration Layer and Alliance Lite2 Direct Link Licences

Overview

This section is applicable for Swift Integration Layer and Alliance Lite2 Direct Link licences for Alliance Lite2, Alliance Lite2 for Business Application Provider, and Alliance Lifeline qualified adapters.

Licence terms

Subject to the applicable licence terms set out from time to time in the Swift contractual documentation, including the Swift General Terms and Conditions or any third-party licence terms which shall be contained in an application installation notice, Swift grants the customer a non-exclusive and non-transferable right to use Swift Integration Layer, the integration technology embedded in Alliance Lite2 Direct Link, as contemplated by this service description and as permitted under the Swift Integration Layer base licence subscribed to by the customer.

Swift Integration Layer and Alliance Lite2 Direct Link base licences

Each base license must have an association with one active Swift BIC that grants the licensee the right to use all the low-level connectivity libraries that are part of the product. Optionally, depending on the type of customer (Alliance Lite2, Alliance Lite2 for Business Application Provider, or Alliance Lifeline) and the options the customer has purchased, Swift grants customers a licence to use the transformation engine (that is built into the product).

For further information, as well as the latest information about the calculation of the base licence, customers should contact their Swift Account Manager.

The base licence has no limit on the number of users or attached application systems.

Installation options

The Swift Integration Layer and Alliance Lite2 Direct Link base licences authorise the customer to install and run the respective product on all of the following environments:

- one production instance
- one test instance
- one contingency instance, potentially deployed in a different site

Not included in the base licence

The Swift Integration Layer and Alliance Lite2 Direct Link base licences do not include a connection to, or licence for Alliance Lite2 or Alliance Lifeline products.

The customer must subscribe to Alliance Lite2 or Alliance Lifeline separately.

Number of transformations deployed in Alliance Lite2 Direct Link

Swift Integration Layer, embedded in Alliance Lite2 Direct Link, allows the customer to define multiple business message transformations to integrate business applications into FIN, InterAct, or FileAct messaging services.

Information about licence bands

For further information, as well as the latest information about the Swift Integration Layer licence bands, customers should contact their Swift Account Manager.

Extension of the Swift Integration Layer base licence

A customer can extend the Swift Integration Layer base licence to include additional production, test, and contingency systems.

For pricing and other information about the Swift Integration Layer base licence extension, customers should contact their Swift Account Manager.

Note *Swift Integration Layer is no longer offered to new customers.*

8.2 Users' Responsibilities

8.2.1 Users' Systems

Secure and effective operation

The Alliance Lite2 user must ensure that the confidentiality, integrity, and availability of data, for instance, traffic, message and configuration data, are maintained at all times on those systems on which it decides to run the Alliance Lite2 interface or AutoClient.

The Alliance Lite2 user must ensure that only authorised software is installed on those systems on which it decides to run the Alliance Lite2 interface or AutoClient.

Swift is not responsible for any security problems, misuse, or malicious attacks that are due to a user's insecure systems, inappropriate browsing practices, negligence or fraudulent act of a security officer or any authorised business users, or any other breach of security by the user.

Internet access

The Alliance Lite2 user is responsible for the availability of the Internet connection and the resolution of any other problems caused by or arising during the Internet connection to the Alliance Lite2 server.

In particular, the Alliance Lite2 user must troubleshoot problems related to the user's Internet connection, or problems with the set-up of the Internet on the user's side.

VPN access

When using the VPN connectivity packs as ordered from Swift, the customer must comply with any guidelines or instructions in force given by Swift regarding the use of the equipment, in particular as detailed in the VPN Products Terms and Conditions and in the Alliance Connect Service Descriptions.

8.2.2 Channel Certificates

User's responsibility for channel certificates

The Alliance Lite2 user utilising channel certificates (for operational purposes in application-to-application flows) must be mindful of the relevant security features described in this document, for example, in Security Features on page 20. In addition, the user must assure that each password is linked to a single authorised person, that passwords cannot be easily deduced and are not written down or communicated to unauthorised people, and that the physical

environment does not allow unauthorised people to observe passwords being typed or keyed in. Passwords should be introduced only following prompting by the Alliance Lite2 application, not any other application.

Delegation or sub-contracting of rights or obligations

If the customer delegates or sub-contracts to a third party the exercise of its rights or the performance of its obligations (typically, the use or management of its token, channel certificate and AutoClient) it does so at its own risk and must ensure that the scope of rights granted to any such third party does not exceed those contracted with Swift. In all cases, the customer that delegates or sub-contracts to a third party the exercise of its rights or the performance of its obligations remains fully responsible to Swift for the performance and observance by any such third party of any obligations applicable to the customer.

What the user must do

For channel certificates, the customer's security officer has to set up the related distinguished name (DN) for recovery as part of the activity to renew such a certificate.

Related information

Security Features on page 20

8.2.3 Tokens and Passwords

User's responsibility for tokens

The Alliance Lite2 user is fully responsible for the security and the use of its tokens. In particular, it is the sole responsibility of the Alliance Lite2 user to prevent an unauthorised party from using its token and password to initiate a transaction.

Therefore, the Alliance Lite2 user must take the utmost care to protect its tokens physically from unauthorised borrowing, loss, and theft. The user must also take all necessary measures to prevent any unauthorised disclosure of the token's password.

The policy ID for token-based certificates is 1.3.21.6.3.10.100.2.

What the user must do

In particular, the Alliance Lite2 user must ensure to abide by the following non-limitative safeguards:

- ensure that each USB token is linked to a single, authorised person
- store the tokens in a locked safe when they are not needed
- revoke any unused or lost tokens
- introduce the password of the token only when requested by the Alliance Lite2 application and not by other applications
- If the customer delegates or sub-contracts to a third party the exercise of its rights or the performance of its obligations (typically, the use or management of its token), it does so at its own risk and must ensure that the scope of rights granted to any such third party does not exceed those contracted with Swift. In all cases, the customer that delegates or sub-contracts to a third party the exercise of its rights or the performance of its obligations remains fully responsible to Swift for the performance and observance by any such third party of any obligations applicable to the customer.

What the user must not do

The user must never:

- lend the tokens to others

- on the PC running the browser, leave the token inserted in the PC while Alliance Lite2 is not being used by an authorised person
- on the PC running AutoClient, leave the token inserted in the PC, unless the PC is in a secured area, protected from physical and logical (network) access by unauthorised people or applications
- write down any password or communicate a password to unauthorised people, especially the password to unlock the token
- use a password that can be deduced easily
- allow anybody to watch over the shoulder of a user who is typing a password

8.2.4 General Security Safeguards

What the user must do

The Alliance Lite2 customers must protect the systems used for Alliance Lite2 in line with industry security practices, such as:

- Protect the Alliance Lite2 PC from unauthorised physical and network access. The Alliance Lite2 user must use a firewall to shield that PC from incoming Internet traffic, and from unauthorised access over the internal network.
  The firewall must be both a physical one to protect incoming traffic, and a PC-local one to ensure that only authorised programs communicate with the outside.
- Install only authorised and required software on the Alliance Lite2 PC.
- Ensure that all software applications that run on the PC are regularly updated and patched. This includes Windows, the Internet browser, and additional features, called plug-ins like Shockwave, QuickTime, Real Player, and any others.
- Restrict outgoing traffic from the PC to business-critical sites, as well as to legitimate sites required for software updates.
- Use up-to-date virus scanners and malware scanners to protect the Alliance Lite2 PC from malware such as viruses, worms, keyboard loggers, trojans, and rootkits.
- Scan any file sent to or received from AutoClient.
- Ensure that all critical internal flows to or from the AutoClient PC are protected against disclosure and malicious changes, especially if the AutoClient files are transferred through a network. To achieve this, customers can use the Local Authentication (LAU) option on AutoClient. Customers can find more information about this option in Security Features on page 20.

The customer must ensure that its end users are following secure browsing practices, such as:

- Reserve certain PCs to access sites of the same criticality as Alliance Lite2 and only access those sites from those PCs.
- Always restart the browser instance before and after accessing the Alliance Lite2 site.
- Verify the Alliance Lite2 server's SSL certificate authenticity at each login to the Alliance Lite2, as described in Log in to Alliance Lite2 of the Alliance Lite2 User Guide.
- Be suspicious of e-mails that appear to come from Swift, and *never* provide the token or channel certificate password if asked. Swift *never* asks for a token or channel certificate password in an e-mail.

The Alliance Lite2 customers must implement the following management principles to alleviate the risks to its system:

- Establish user management practices to ensure that only authorised users are created and remain on the system.
  Because users change roles or leave the company, the customer must maintain an accurate and up-to-date list of authorised users.

- Establish entitlement management practices to ensure that customers are granted access to Alliance Lite2 functions only on a need-to-know or need-to-have basis.
  As an example, use this capability to whitelist bank accounts, and to set a limit on the maximum amount per transaction or per day.
- Use the dual approval features provided by Alliance Lite2 (see 4-eyes principle on page 22), ideally from two different PCs.
- Configure the application in such a way that the transactions from AutoClient must be manually approved before they are released to Swift.
- Ensure that only the person with the required permission has physical and logical access to the Alliance Lite2 PC, to the AutoClient PC, and to the backups.
- Reconcile daily traffic, to detect mismatches between authorised and actual traffic, both sent or received.

What the user must not do

- The user must not run AutoClient, or the browser on the PC where Alliance Lite2 is used, from a privileged Windows account, that is, an account with Windows administrator rights.
- The user must not browse to Internet sites that it believes may be unsafe, from the same PC on which it accesses Alliance Lite2.
- The user must not click links in e-mails that appear to come from Swift or anyone else, even if the link seems perfectly valid from a business perspective.
  Such phishing attacks may lead to a rogue site that can steal information or infect the PC.
  If the user can confirm a business need for visiting the site, then the user should re-type the link within the browser as it was visible in the e-mail.
- The user must not browse any other site at the same time as it accesses Alliance Lite2.
- The user must not accept a pop-up that asks to download and install executable software.
- The user must not delegate all the administrator roles to a single person who can then use the two different USB tokens.
- The user must not assign administrator and message-approval roles to a single individual.

Customer Security Programme

Alliance Lite2 comes with a set of features and functions designed to help customers to deploy and use it according to the customer security controls set out in the Swift Customer Security Controls Framework - Detailed Description. Nothing in the features and functions of Alliance Lite2 shall be construed or interpreted as Swift taking or accepting any responsibility or liability for customers' roles and responsibilities as set out elsewhere in the Swift contractual documentation, including but not limited to the obligation for each customer to duly protect and secure its Swift-related infrastructure and local environment.

Operating system updates are frequently released to address vulnerability fixes and software bugs. In the scope of the Swift Customer Security Programme, these updates are crucial for maintaining the security and stability of your system. In this regard, Swift recommends that customers frequently monitor the vendor's website to determine if their operating system must be updated.

8.2.5 Other Responsibilities of Alliance Lite2 Users

Overview

Subject to applicable eligibility criteria, usage rights, and other conditions, Alliance Lite2 permits users to exchange messages or files over SwiftNet using FIN (MT), InterAct (MX), or FileAct. Users can also access browse services over SwiftNet, in a many-to-many environment, in a Market infrastructure and a Member-Administered Closed User Group (CUG), or in SCORE.

Specific obligations and responsibilities apply to customers of these services, as set out in the relevant service description and other related Swift contractual documentation.

For the latest available versions of the relevant service descriptions and other Swift contractual documentation, see Knowledge Centre (User Handbook).

Unless performed by Swift as an integral part of the Alliance Lite2 release or not relevant in the context of the Alliance Lite2 release, Alliance Lite2 customers must also abide by these obligations and responsibilities when using the following services.

General operational tasks

In addition to the specific user responsibilities mentioned below, Alliance Lite2 customers must:
- ensure that the Alliance Lite2 security officers manage the RBAC roles for browse users to use browse services through Alliance Lite2
- take measures to identify the emission or reception of duplicate messages. As per the FIN Service Description, these measures can include detection of Possible Duplicate Message or Possible Duplicate Emission trailers, or other means of identifying duplicate messages (for example, end-of-day reconciliation, message ID identification).

FIN

The Alliance Lite2 customers accessing FIN must in particular:
- use the appropriate Swift Standards. Customers can find more information about the use of FIN message standards in the FIN Service Description.
- take all necessary steps to receive all messages queued to them during local working hours, and before the applicable cut-off time. Swift reserves the right, in exceptional circumstances, to delay the cut-off time.
- never ignore the receipt of a message. A customer that receives a message from another customer cannot just reject or ignore the message. The receiving customer must either process the message or promptly revert to the sender.

Customers can find more information about their obligations and responsibilities regarding the receipt of FIN messages in the FIN Service Description.

InterAct MX

Alliance Lite2 users receiving InterAct MX messages must:
- take all necessary steps to receive all messages queued to them
- never ignore the receipt of a message

InterAct MX messages can be sent and received by Alliance Lite2 over InterAct in store-and-forward or in real-time mode. Customers can find more information about InterAct in the SwiftNet Service Description.

FileAct

Alliance Lite2 users using FileAct in a many-to-many environment must accept having their participation published in the generic Directories Over FileAct Implementation Guidelines, part of the SwiftNet Services Directory (restricted area). These users must also adhere to the policies and other customer responsibilities in the SwiftNet Messaging Operations Guide.

Market infrastructure and Member-Administered Closed User Group

Alliance Lite2 users participating to a market infrastructure must verify with the Market Infrastructure service administrator that they are allowed to connect to this market infrastructure through Alliance Lite2. Furthermore, Alliance Lite2 users participating in a market

infrastructure or Member-Administered Closed User Group acknowledge and agree that the market infrastructure or Member-Administered Closed User Group service administrator must approve their participation. Also the market infrastructure or Member-Administered Closed User Group service administrator may at all times request Swift to withdraw them from the market infrastructure or Member-Administered Closed User Group. These users must also adhere to the service parameters and any operational rules that the market infrastructure or Member-Administered Closed User Group service administrator defines from time to time in respect of the use of Swift services and products in their market infrastructure or Member-Administered Closed User Group.

Information consultation or download from the central infrastructure

It is the sole responsibility of the Alliance Lite2 customer to consult or download all necessary information from the Alliance Lite2 central infrastructure within the relevant period of time.

Customers can find more information about the consultation or download of messages or files from the Alliance Lite2 servers in Browser-based Screens on page 12 and AutoClient on page 14.

Distinguished Names (DNs) and certificates for personal tokens

For the personal tokens, the customer can create Distinguished Names (DNs) anywhere in the customer's 8-character BIC DN tree, and assign a certificate of type **Personal** (policy ID 1.3.21.6.3.10.200.2) to them. This certificate will be generated and placed on the customer's personal token when the token is activated through the Swift Certificate Centre.

Swift can automatically create one or more DNs starting with `cn=%n` (where `n` is a number between 1 or 01 and 99) under such a personal token DN. Each of these sub-DNs will automatically be associated with a SwiftNet PKI certificate, which will be stored in the Swift OPC-based HSMs for the purpose of signing browse traffic initiated by that token.

The customer can create and manage (revoke, set up for recovery, disable, and so on) a personal token's certificate of type **Personal** (policy ID 1.3.21.6.3.10.200.2). The customer is not allowed to create or manage any sub-DNs or certificates under personal token DNs.

Other Distinguished Names (DNs) and certificates

Some DNs and related certificates are reserved by Swift. For more information, see the Alliance Lite2 Administration Guide.

Data protection responsibilities

By subscribing to Alliance Lite2, the customer instructs Swift to process financial messages, and end user information in the context of using the Alliance Lite2 service for the purposes of processing financial messages through the Alliance Lite2 product in accordance with the present service description. Customers acting as Data Controller are responsible for complying with all applicable laws, including privacy, data protection and information security laws for processing such data for their own purposes as part of their use of Alliance Lite2.

In its role as data controller, it is the customer's sole responsibility (amongst others):

- to determine for which purposes it will use such data
- to ensure it can rely on an appropriate legal basis to process such data, such as compliance with a legal obligation, legitimate interest, or public interest
- to ensure that its own use of such data complies with any applicable data transfer restrictions
- to determine by which means it will process such data once downloaded on its systems, provided the customer implements appropriate technical and organisational security

measures to protect such data against accidental or unlawful destruction, accidental loss, alteration, and unauthorised disclosure or access, and
- to comply with any obligations resulting from applicable personal data laws and regulations when processing such data. In particular, the customer must assess whether it must comply with notice requirements to individuals or can rely on exemptions from such notice requirements, and whether it must respond to access and correction requests from individuals or can rely on exemptions from such obligations.

8.3 Swift's Roles and Responsibilities

Data protection responsibilities

In the sections describing Swift's and the customer's data protection responsibilities, the words data controller, data subject, personal data, process or processing and data processor shall have the meaning given to these terms in the EU General Data Protection Regulation (EU) 2016/679 (GDPR).

The Swift Personal Data Protection Policy describes the Personal Data processing activities conducted by Swift for its own purposes as Data Controller.

In addition, Swift acts as a data processor with respect to the processing of financial messages, and end user information in the context of providing the Alliance Lite2 service. Swift only processes these personal data on behalf of and in accordance with the instructions of the customer which are documented in this service description and any document referred to in the service description.

The subject matter, nature and purpose of the processing, and the duration of the processing are set out in the service description, notably in Overview of Alliance Lite2, in Features and Functions, and in the present section. The categories of data subjects include the individuals mentioned in financial messages (typically ordering and beneficiary parties) and end users. The types of personal data processed on behalf of customer include identification data, financial data, event logs. Swift will not use or disclose such data for any other purposes.

In its role of data processor, Swift implements appropriate technical and organisational security measures to ensure a level of security for such data that is appropriate to the risks presented by the processing, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to such data transmitted, stored or otherwise processed.

In any case, Swift ensures that any Swift personnel having access to such data processes this data only in accordance with Swift’s instructions. In this connection, Swift shall only (internally) grant access to such data to Swift personnel that have agreed to confidentiality obligations or are under an appropriate statutory obligation of confidentiality.

If and as required under applicable law, Swift will notify security incidents that lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, such data to the customer without undue delay after becoming aware of the data breach.

Furthermore, Swift shall inform the customer of any formal requests it receives from individuals exercising their data protection rights. As explained above, Swift will not itself respond to such requests as it has no means to directly or indirectly identify any individual based on individual transaction data.

As data processor, Swift agrees that it does not currently subcontract any of its data processing operations related to such data to other (sub)data processors. In case any additional subcontracting would be considered in the future, Swift will inform the customer in advance, and provide an opportunity to present objections (on reasonable grounds pertaining to potential or actual violation of applicable data protection laws). In case the customer does not object, the customer will be deemed to have consented to the subcontracting. The parties will work together in good faith to address any possible objection presented by the customer. If Swift decides to retain the (sub)data processor, it will notify the customer having raised an objection, which will have the right to terminate the service.

Swift shall ensure it has signed a written agreement with the relevant subcontractor which imposes the same data protection obligations on the subcontractor as those included in this service description.

In case the subcontractor fails to fulfil its data protection obligations under the subcontracting agreement, Swift shall remain liable towards the customer for the performance of the subcontractor's obligations under such agreement.

- it will deal promptly and appropriately with all enquiries from the customer relating to the processing of such data
- it will, as appropriate and upon the customer's request, assist the customer in ensuring compliance with requirements under applicable data protection laws with regard to the personal data processed on its behalf, including data security, data breach notifications, data protection impact assessments, and prior consultations with data protection authorities. Swift may charge a reasonable fee for its assistance, to the extent permitted under applicable law
- it will immediately inform the customer if, in its opinion, any of the customer's instructions infringe applicable data protection laws
- it will make available to the customer all information necessary to demonstrate compliance with this service description and applicable data protection laws, and will allow for and contribute to requests for information from the customer's (own or external) auditors regarding such compliance

Swift hosts the data, including the personal data, processed in relation to Alliance Lite2 on its infrastructure located in the Netherlands and Switzerland. Swift will inform customers in advance of any changes to this location. In case any transfer of personal data outside of the European Economic Area would be considered in the future, Swift will inform the customer thereof in advance. The customer hereby authorises Swift to perform any such transfer if it is made (i) to any country formally recognised by the European Commission as providing an adequate level of data protection or (ii) to any other country, provided an appropriate and valid transfer mechanism is put in place that is recognised under EU data protection laws, such as the standard contractual clauses adopted by the European Commission.

Availability, integrity, and confidentiality

Swift prioritises the availability, authenticity, integrity, and confidentiality of customers' data, including personal information. Swift's commitment to the following security principles ensures that customers' data is handled with the utmost care and is protected throughout its life cycle.

- **Availability**
  Swift services are designed and operated using industry-standard practices to maintain their availability in line with their criticality.
- **Authenticity**
  Swift services authenticate the source of data through robust authentication mechanisms such as multi-factor authentication and/or digital signatures.
- **Integrity**

Swift services store data securely to prevent unauthorised modifications, through mechanisms such as access control lists, data integrity checks, and/or digital signatures.

- **Confidentiality**
  Swift services adhere to strict confidentiality protocols and industry-standard encryption methods to safeguard confidential information from unauthorised access and disclosure.

Customers' trust and privacy are of utmost importance to Swift. By adhering to these principles, Swift provides secure and reliable services that protect customers' data comprehensively.

For more information about Swift's Personal Data Protection Policy, see the Swift Personal Data Protection Policy.

Independent Assurance

Swift shall make available a yearly ISAE 3000 Type II report - or another report based on at least equivalent standards - covering Alliance Lite2. Customers can request such report by e-mail to AssuranceQuestions.Generic@swift.com with the following information:

- Recipient’s name (and title Mr or Ms)
- Recipient’s job title
- Recipient’s e-mail address
- User organisation’s BIC

The report is confidential, and distribution is restricted to named officials at the customer's organisation.

Subcontractors

Swift shall make available a list of subcontractors (if any) whose failure or deficiency would likely materially adversely impact the provision of Alliance Lite2 services. Customers can request such list and related information about how Swift manages such subcontractors by e-mail to AssuranceQuestions.Generic@swift.com with the following information:

- Recipient’s name (and title Mr or Ms)
- Recipient’s job title
- Recipient’s e-mail address
- User organisation’s BIC

The list and related information are confidential, and distribution is restricted on a strict need-to-know basis within the recipient's organisation.

9 Contractual Framework

Swift General Terms and Conditions

Together with this service description, the Swift General Terms and Conditions govern the provision and the use of Alliance Lite2, except otherwise provided in the Liability section with respect to Swift liability. Such section on liability shall prevail in the case of conflict or inconsistency with the Swift General Terms and Conditions.

For the latest available version of the Swift General Terms and Conditions, see www.swift.com > About Us > Legal > Terms & Conditions.

Liability

However, Swift's liability for the provision and the use of Alliance Lite2 to any and all Alliance Lite2 users shall together not exceed, in respect of any and all claims notified to Swift in each calendar year, an aggregate maximum of one million euro per calendar year.

This specific limit of Swift's liability does not apply to any liability for death or personal injury, or in respect of claims relating to physical damage or loss of the user's tangible property. Any limit to any such liability of Swift will be assessed according to the Swift General Terms and Conditions only.

The Swift General Terms and Conditions also apply to the provision and the use of SwiftNet PKI.

Hardware security tokens

The provision and the use of the tokens are governed by the HSM Card, Reader & Token Terms and Conditions.

SwiftRef Products

The provision and use of the SwiftRef Products are governed by the SwiftRef Products Terms and Conditions.

Swift services and products accessed through Alliance Lite2

The Swift General Terms and Conditions also govern the provision and the use of other Swift services and products accessed by users through Alliance Lite2 - for instance FIN and FileAct in a many-to-many environment; in a Market infrastructure and Member-Administered Closed User Group. It also governs the provisioning and use of other Swift services and products accessed by users through Alliance Lite2 Standardised Corporate Environment (SCORE), and Relationship Management Application (RMA).

Subject to the Alliance Lite2 customer complying with all obligations applicable to it, Swift accepts liability for the provision or the use of the Swift services and products accessed through Alliance Lite2 according to the Swift General Terms and Conditions or any other contractual documentation identified in a separate subscription form.

Services related to Alliance Lite2

The set-up services that customers must order together with Alliance Lite2 are subject to a separate *Services Proposal* which will be governed by the related Swift Services Terms and Conditions (available at Legal page on www.swift.com).

Configuration changes are support services governed by the Swift General Terms and Conditions. In some cases specified in this service description these support services will require a separate order form and a related service proposal.

Should Swift provide professional services related to Alliance Lite2 Direct Link, Swift's obligations and responsibilities will be governed by the applicable service proposal and the related Swift Services Terms and Conditions.

Customer testing

Customers must not conduct any performance or vulnerability tests on or through Swift services and products unless expressly permitted in the Swift Customer Testing Policy. If customers believe they have identified a potential performance or vulnerability threat, then they must immediately inform Swift thereof and treat all related information, data or materials as Swift confidential information.

Appendix A List of Available Configuration Changes

A.1 Standard Configuration Changes

Customers can order the following standard configuration changes, one by one, as payable changes:

Configuration change	Description	Reference
Add one unit for manual message processing.	By default, BIC8_Unit is assigned to all messages manually created or processed, and all operators are assigned to this BIC8_Unit. Additional units can be created for manual message processing to segregate the messages displayed to the operators.	Alliance Lite2 User Guide (Message Creation section)
Add or change one operator profile.	Additional operator profiles can be requested to customise the applications and the activities that the operators can perform.	The list of default operator profiles is available in the Alliance Lite2 Administration Guide (Default Operator Profiles section).
Add profiles with change expiry date and time privileges.	Additional profiles can be requested to grant operators on Alliance Lite2 the privilege to change message expiry date and time.	Knowledge Base article 6000869
Add one unpublished BIC.	An unpublished BIC is, by default, not included in the Alliance Lite2 BIC Directory. Adding an unpublished BIC in Alliance Lite2 will make it visible to all Alliance Lite2 users.	
Generate a PDF automatically for all the messages that are sent and/or received through AutoClient.	This configuration enables the customer to print, in PDF format, all the messages that are sent and/or received for a customer BIC in AutoClient. These messages are stored in a PDF folder in the reception directory of AutoClient.	Alliance Lite2 AutoClient User Guide (Additional Configurations section)
Change the FIN message default output format from RJE to XMLv2.	By default, the received FIN message files are available in RJE format. On request, Swift can change the default output format to XMLv2 per customer.	Alliance Lite2 AutoClient User Guide (Message File Preparation section)
Change the InterAct message output format to XMLv2 rev7	By default, the received InterAct message output format is XMLv2 rev3. On request, Swift can change the default output format to XMLv2 rev7 per customer.	Alliance Lite2 AutoClient User Guide (XMLv2 Format used by Alliance Lite2)
Change the message flow so that all messages sent to Swift through AutoClient require authorisation.	By default, files and messages that are submitted through AutoClient to the Alliance Lite2 server do not require authorisation and are sent directly to Swift. This message flow can be changed to force manual	Alliance Lite2 AutoClient User Guide (Successful Upload section)

Configuration change	Description	Reference
	authorisation before sending to Swift.	
Change the message flow so that the ACKs of all messages created manually are routed to the AutoClient directory.	By default, the ACKs of messages created manually are automatically completed. This message flow can be changed to have all the ACKs routed to the AutoClient directory.	Alliance Lite2 User Guide (Management of Messages section)
Segregate one received message flow into its own, separate subdirectory (for example, based on MT, correspondent, request type).	By default, all received messages are sent to the AutoClient Reception directory. This message flow can be updated to have part of it (for example, based on a message type or correspondent) routed to a new and separate AutoClient subdirectory.	Alliance Lite2 AutoClient User Guide (Reception Directory section)
Segregate the message flow to separate subdirectories based on the traffic type (for example, FIN, FileAct).	By default, all received messages are sent to the AutoClient Reception directory. This message flow can be updated to route messages of different types (for example, FIN, FileAct) to new and distinct AutoClient subdirectories.	Alliance Lite2 AutoClient User Guide (Reception Directory section)

A.2 Specific Configuration Changes

Customers can order the following specific configuration changes, one by one, as payable changes:

Configuration change	Description	Reference
Add one BIC11.	BIC11s are, by default, not defined as internal correspondents in Alliance Lite2. Swift can change the customer BIC11 definition to allow message sending from that BIC11.	Knowledge Base article 5017673
Change the message flow so that a subset of messages sent to Swift through AutoClient require verification or authorisation.	By default, files and messages that are submitted through AutoClient to the Alliance Lite2 server do not require verification or authorisation, and are sent directly to Swift. This message flow can be changed to force manual verification or authorisation of a subset of messages before sending to Swift.	Alliance Lite2 AutoClient User Guide (Successful Upload section)
Change the message flow so that a copy of all messages (including ACKs and manually created messages) is sent to the AutoClient Archive directory.	By default, the AutoClient Archive directory only contains the messages processed through AutoClient. This message flow can be changed to have a copy of all messages, including ACKs and manually created messages, sent to the AutoClient Archive directory.	Alliance Lite2 User Guide (Management of Messages section)
Change the message flow so that the ACKs (FIN, FileAct) are routed to a separate AutoClient subdirectory.	By default, the ACKs of messages sent to the Alliance Lite2 server through AutoClient are sent to the AutoClient Reception directory. This message flow can be changed to have those ACKs routed to a separate AutoClient subdirectory.	Alliance Lite2 User Guide (Management of Messages section)

Configuration change	Description	Reference
Change the message flow so that the delivery notifications (FIN, FileAct) are routed to a separate AutoClient subdirectory.	By default, the delivery notifications of messages sent to the Alliance Lite2 server through AutoClient are sent to the AutoClient Reception directory. This message flow can be changed to have those delivery notifications routed to a separate AutoClient subdirectory.	Alliance Lite2 User Guide (Management of Messages section)
Change the unit assignment of messages during message processing.	By default, messages are processed and routed without changing their unit assignment. This message flow can be changed to have the unit assignment modified while processing the messages.	Alliance Lite2 User Guide (Management of Messages section)
Change network configuration to disable Internet access for customers connecting through Alliance Connect.	By default, customers who are using an Alliance Connect connectivity pack to connect to Alliance Lite2 can also connect to Alliance Lite2 through the internet. Swift can change the access configuration to disable the Internet access for such customers.	Knowledge Base article 5018026
Import FIN message templates created in Alliance Access or created in an Alliance Lite2 test environment.	By default, there are no message templates defined in Alliance Lite2. Customers can create their own message templates. It is also possible to request Swift to import into Alliance Lite2 message templates previously created in Alliance Access or in an Alliance Lite2 test environment.	Alliance Lite2 User Guide (Use Message Templates section)
Import MX message templates, created in Alliance Access or in an Alliance Lite2 test environment.	By default, there are no message templates defined in Alliance Lite2. Customers can create their own message templates. It is also possible to request Swift to import into Alliance Lite2 message templates previously created in Alliance Access or in an Alliance Lite2 test environment.	Alliance Lite2 User Guide (Use Message Templates section)
Segregate the message flow to separate subdirectories based on conversion codes (sw:TRD).	By default, all received messages are sent to the AutoClient reception directory or the hybrid/truncate d directory if the customer is still subscribed to the in-flow translation service. This message flow can be updated to route messages to Swift pre-defined and distinct AutoClient subdirectories.	Alliance Lite2 AutoClient User Guide (Reception Directory section) Alliance Lite2 Customer Adoption Guide (Multi-Format MX with AutoClient section) Knowledge Base article 6000631 explains the available customisation options for Alliance Lite2 that are based on conversion codes.
UTI (Unique Transaction Identifier) Auto-Generate feature in Alliance Lite2.	The UTI is used in securities settlement to provide a reference interlinking all related messages in the same end-to-end settlement transaction. Alliance Lite2 can automatically generate a UTI in the MT payload	Knowledge Base article 6000653 explains the available customisation options for Alliance Lite2 for the UTI auto-generation.

Configuration change	Description	Reference
	for certain FIN securities messages based on a customisation request.	

Note *The following requests are part of the Community Support service provided to all Alliance Lite2 customers:*

- ***Request to switch FIN LTs into future mode testing***
  This allows customers to start testing a new Swift Standards Release before Live availability. Requests for future mode testing do not require a Swift maintenance window. When the tests are completed, the customer must explicitly request Swift to set the mode back to the original value.
  For more information, see Knowledge Base article 5019985.
- ***Request to create additional Alliance Lite2 LSOs and RSOs***
  By default, Alliance Lite2 is configured with one left security officer (LSO) and one right security officer (RSO). Customers can create additional LSOs and RSOs, but this requires the intervention of Swift.

Appendix B Alliance Lite2 Service Levels

As per the Swift General Terms and Conditions, Swift provides Swift services and products and complies with any applicable service levels in all material respects as set out in the relevant service description. This Appendix summarises the key service levels applicable to Alliance Lite2 and refers to additional service descriptions which describe other applicable service levels.

Service availability objective

Outside the planned unavailability, the monthly weighted Alliance Lite2 service availability objective is 99.900%.

Availability is the percentage of time during which the Alliance Lite2 service is available to customers during a specific period of time. The published availability figures are weighted to give a single overall availability percentage that reflects the impact of outages affecting only parts of the user base or parts of the service.

Service availability reporting to customers upon request

Alliance Lite2 customers can request to receive a copy of the Alliance Lite2 service availability report by contacting Swift Support. The Alliance Lite2 service availability report is updated on a monthly basis and reports on the year-to-date Alliance Lite2 weighted availability.

Service resilience

The Alliance Lite2 infrastructure consists of a set of hosts and related infrastructure that provide for resilient operations during most single-component failure scenarios within the active Swift operating centre where Swift runs the Alliance Lite2 service. The Alliance Lite2 service is designed to handle many anomalous events without impacting the activities of the Alliance Lite2 customers.

Recovery Time Objective

Recovery Time Objective is defined as the maximum amount of time required to restore the Alliance Lite2 service in another operating centre when the service becomes unusable in one site. The Recovery Time Objective is set to 8 hours.

If Swift is not able to meet this Recovery Time Objective, Swift will inform customers about the additional time required to recover the service. Customers agree that Swift's only responsibility is to inform them of such additional recovery time, and that such information will be their sole remedy in such circumstances.

Change management procedures

The change management procedures on the Alliance Lite2 infrastructure are in line with the change management procedures applied for FIN and SwiftNet. For more information about these procedures, see section *Change Management* of the *ISAE_3000 Report* (report available upon request).

For customer configuration changes, see Payable Configuration Changes on page 10.

Notification and reporting of major incidents to customers

Customers should subscribe to the Swift Service Alert on swift.com for the relevant Swift product or service.

Swift actions following failure

In the unlikely event of a failure that would affect the Alliance Lite2 service availability, Swift will take the necessary measures to minimise the service downtime. Swift will take all appropriate actions depending on the nature of the failure. If required, Swift will declare a major incident , with potential notification to the Swift Command Centre.

Disaster recovery procedures

In the extreme event that one of the operating centres where Alliance Lite2 is running becomes unavailable, Swift will restore the Alliance Lite2 live services in a standby infrastructure located in another operating centre. The standby disaster recovery infrastructure then becomes the main infrastructure.

The standby operating centre is deployed as a cold standby infrastructure. This means that the standby server infrastructure is ready and configured, and that the configuration data it contains is identical to the data that was on the primary site at the time of the last data synchronisation, which occurs every week after the live allowable downtime window (ADW).

Customers will automatically reconnect to the other operating centre as soon as it becomes operational. Customers will have to review and update their configuration data, to cover the period of time between the last configuration data synchronisation and the activation of the other operating centre.

For more information about service availability and disaster recovery, seeService Availability on page 26.

Swift has implemented monitoring processes to test the availability of the standby site and its readiness to take over.

Service continuity exercise

Swift does not need to involve Alliance Lite2 customers in service continuity tests for the Alliance Lite2 infrastructure because service continuity is provided by the active monitoring tools that are permanently checking the availability of the automated and manual flows. For automated flows, the monitoring tools are testing the sending and receiving of messages through AutoClient. The user interface availability is tested by simulating a user's activity. Additionally, the standby site infrastructure replicates the infrastructure of the primary site.

Swift has implemented business continuity plans and annual testing to meet the recovery time objectives (RTOs). Swift has in place information and communications technology security measures, tools, and policies in accordance with best industry practices and standards generally applicable to providers of similar services.

Alliance Lite2, Alliance Lifeline, and Alliance Remote Gateway shared components

The Alliance Lite2 infrastructure shares some system components with Alliance Lifeline and Alliance Remote Gateway. As a consequence, in the unlikely event of a malfunction of those shared components on Alliance Lite2, the Alliance Lifeline infrastructure and/or the Alliance Remote Gateway infrastructure could be impacted.

Legal Notices

Copyright

Swift © 2026. 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. SC. The following are registered trademarks of Swift: 3SKey, Innotribe, MyStandards, Sibos, Swift, SwiftNet, the Standards Forum logo, the Swift logo, Swift GPI with logo, the Swift GPI logo, and UETR. Other product, service, or company names in this publication are trade names, trademarks, or registered trademarks of their respective owners.