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.
# Table of Contents

Preface .......................................................................................................................................................... 4

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.............................................................................................................................................. 15
   2.5 Types of End Users............................................................................................................................... 17
   2.6 Security Features................................................................................................................................... 18
   2.7 Accessing the Alliance Lite2 Software................................................................................................... 20
   2.8 Accessing SWIFT Messaging Services................................................................................................. 21
   2.9 Protection of Customer Information....................................................................................................... 22
   2.10 Service Availability................................................................................................................................. 23

3 System Requirements ............................................................................................................................ 26

4 Ordering ................................................................................................................................................. 27

5 Operational Services ............................................................................................................................. 28
   5.1 Support.................................................................................................................................................. 28
   5.2 Alliance Lite2 Peace of Mind Support Pack........................................................................................... 28

6 Users’ Responsibilities ............................................................................................................................. 30
   6.1 Users’ Systems...................................................................................................................................... 30
   6.2 Channel Certificates.............................................................................................................................. 30
   6.3 Tokens and Passwords.......................................................................................................................... 31
   6.4 General Security Safeguards................................................................................................................. 32
   6.5 Other Responsibilities of Alliance Lite2 Users....................................................................................... 34

7 Contractual Framework .......................................................................................................................... 36
   7.1 SWIFT General Terms and Conditions................................................................................................. 36

A List of Questions and Assistance Covered by the Peace of Mind Pack ................................................. 38
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

Significant changes
The following table lists all significant changes to this service description since the release of December 2016. This table does not include editorial changes that SWIFT makes to improve the usability and comprehension of the document.

<table>
<thead>
<tr>
<th>Updated information</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addition of new Alliance Lite2 Direct Link option</td>
<td>Overview of Alliance Lite2 on page 6</td>
</tr>
<tr>
<td>Addition of cancellation requests</td>
<td>Payable Configuration Changes on page 10</td>
</tr>
<tr>
<td>Addition of Customer Security Programme information</td>
<td>General Security Safeguards on page 32</td>
</tr>
</tbody>
</table>

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 Lite2 support page
• Alliance Connect Service Descriptions
• Alliance Lite2 Administration Guide
• Alliance Lite2 Administration Guide - RMA
• Alliance Lite2 AutoClient User Guide
• Alliance Lite2 AutoClient Release Letter
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 the use of all SWIFTNet browse services offered 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 Explorer browser on a Windows PC, and a secure USB 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.

**Automated sending and receiving through Direct Link**

Direct Link for Alliance Lite2 provides an alternative Alliance Lite2 connectivity for automated flows, which removes the need to use AutoClient. This software supports an interactive connection between the back-office and Alliance Lite2 as well as an ad-hoc integration and transformation capability.

**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 14)
- 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 are strongly recommended to use Alliance Connect VPN boxes to connect to SWIFT. Customers can also use a broadband Internet connection to access Alliance Lite2 screens or to use AutoClient. Subject to a separate subscription, Alliance Lite2 customers can use SWIFT’s Virtual Private Network (VPN), also called the SWIFT Secure IP Network (SIPN), through SWIFT’s Alliance Connect products (Alliance Connect Bronze/Silver/Silver Plus/Gold). Note that the subscription to the SWIFT Secure IP Network (SIPN) only becomes active after a subsequent Alliance Lite2 allowable downtime window (ADW, see Planned unavailability on page 23).

The use of SWIFT’s VPN through Alliance Connect is optional if the customer uses tokens, but is mandatory if the customer uses channel certificates. Depending on the services used, customers can ask SWIFT to disable Internet access for all their users, allowing access only through SWIFT’s VPN.

**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 box) owned by the same customer who owns the channel certificate. For more information about tokens and channel certificates, see [Security Features](#) on page 18, and [Channel Certificates](#) on page 30.

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 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 18 and [Users' Responsibilities](#) on page 30.
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 2 key components of Alliance Lite2:
  - Browser-based screens (see Browser-based Screens on page 12)
  - AutoClient (see AutoClient on page 15)
- 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 17)
- Details about security management (see Security Features on page 18)
- The Alliance Lite2 software (see Accessing the Alliance Lite2 Software on page 20)
- The processing of messages and files (see Accessing SWIFT Messaging Services on page 21)
- The storage and retrieval of messages and files (see Protection of Customer Information on page 22)
- The availability of the Alliance Lite2 service (see Service Availability on page 23)

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
- online access to the BIC Directory
- online access to the User Handbook documentation repository for all the users that are registered to www.swift.com
- subject to applicable eligibility criteria and other conditions, other SWIFT services and products accessed through the 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 WebAccess 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 items:

- a set of 10 USB hardware security tokens (personal tokens)
- a separate mini-USB memory key that contains:
  - the Alliance Lite2 AutoClient software

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.

Any other customisation request will be first assessed by SWIFT to confirm feasibility and price. 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 Consulting 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 39.

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 Consulting 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 (ADW, see Planned unavailability on page 23), 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 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:

<table>
<thead>
<tr>
<th>WHEN</th>
<th>WHO/WHAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max 2 days</td>
<td>Customer Requests configuration change</td>
</tr>
<tr>
<td>Thursday at the latest (t)</td>
<td>Customer Confirms configuration change</td>
</tr>
<tr>
<td>SWIFT ADW Min: t + 9 days</td>
<td>SWIFT Implements in Test and Training</td>
</tr>
<tr>
<td>Monday at the latest (t')</td>
<td>Customer Tests and validates configuration change</td>
</tr>
<tr>
<td>SWIFT ADW Min: t' + 5 days</td>
<td>SWIFT Implements in Live</td>
</tr>
</tbody>
</table>

**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 WebAccess 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 WebAccess services over SWIFTNet (through an optional subscription).

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 SWIFTStandards (all fields and options) of these MT and MX messages.

  Alliance Lite2 validates the messages against the SWIFTStandards syntax before sending them on to SWIFT, and reports any errors against the SWIFTStandard 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 days period, then they must request SWIFT to perform a configuration change that will ensure a local copy, through the AutoClient, 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, deleting, 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 WebAccess over SWIFTNet
  Customers who have subscribed to the SWIFT WebAccess 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 30
- Alliance Lite2 User Guide
- Alliance Lite2 Administration Guide
- Alliance Lite2 Administration Guide - RMA
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 Lite, 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 to SWIFT.

- **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 3 formats:
  - Text format, compatible with Alliance Lite
  - XML format, compatible with Alliance Lite
  - 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 30
[Alliance Lite2 AutoClient User Guide](#)
2.5 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 WebAccess 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 regards to the Alliance Lite2 security officers appointed by the customer himself as explained in Security officer on page 17.

Related information
SWIFTNet Online Operations Manager User Guide
2.6 Security Features

SWIFT personal hardware tokens (USB tokens)

The left Alliance Lite2 security officer receives from SWIFT a box of hardware tokens (USB tokens), and receives by e-mail his personal, one-time activation code. This activation code allows him to configure one of the tokens for his personal use.

The right Alliance Lite2 security officer receives by e-mail the initial token password that was assigned to all the tokens in the box. The mail also contains his personal one-time activation code allowing him to configure one of the tokens for his personal use.

By working together, the left and right security officers can each activate their own token, and assign a password to that token only known by themselves. Activating a token is performed through the SWIFT Certificate Centre, and results in the generation of a PKI public/private keypair on the token and the certification of the public key by SWIFT.

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.

It is mandatory to enter the token's password to access the certificate that is stored on the token. The certificate allows the security officer or the business user to log on to the Alliance Lite2 application. The certificate is also required to enable the certificate owner to perform sensitive actions, such as the sending of transactions.

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 box) 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 box 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

SWIFT strongly 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 on the procedure, see the knowledge base tip 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.  
TLS 1.0 and TLS 1.1 are still supported for compatibility reasons.

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 according to the algorithm that is described in the [Alliance Lite2 AutoClient User Guide](#). SWIFT strongly recommends configuring/using LAU between customer’s application and AutoClient.

2.7 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 Microsoft Internet Explorer browser. A Java plug-in (also called Java Run-Time Environment [JRE]) must be present on this Internet Explorer.

  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 an Alliance Connect VPN box.

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.

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

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 or other SWIFT services and products only.

### 2.8 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 WebAccess 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 23) 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’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 22.

## 2.9 Protection of Customer Information

**Data retrieval**

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 23) and disaster recovery (see **Alliance Lite2 Service Levels** on page 44), 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 15.

SWIFT may retrieve, use, and disclose traffic or message data from these Alliance Lite2 servers only in any of the following circumstances:

- when required for the provisioning of Alliance Lite2, as documented in this service description or other relevant SWIFT contractual documentation
- when permitted by the **SWIFT Data Retrieval Policy**

This does not affect any retrieval, use, and disclosure of traffic or message data of the Alliance Lite2 user as part of any other SWIFT services and products accessed through Alliance Lite2 (for example, FIN or FileAct in a many-to-many environment, in a Member-Administered Closed User Group or in SCORE), as permitted under the relevant contractual documentation.
Use of data for security monitoring and investigation purposes

In accordance with the SWIFT Data Retrieval Policy and the Distributed Architecture principles, SWIFT may process and store traffic and message data in order to support SWIFT’s protection measures and forensic capabilities against cybersecurity threats. SWIFT processes and stores such data on dedicated security systems and in strict accordance with its security policies and procedures and may analyse such data in the context of a specific security investigation as part of its security monitoring and investigation processes.

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 7 days.

2.10 Service Availability

Operational status

SWIFT displays the operational status of Alliance Lite2 and of the FIN, InterAct, and FileAct services at Operational status notifications.

It is the customer’s responsibility to consult any notifications about the operational status of the Alliance Lite2, FIN, InterAct, or FileAct. SWIFT recommends that customers subscribe to the products and services notifications (at Operational status notifications) to be notified of any maintenance updates.

Planned unavailability

SWIFT notifies customers in advance on www.swift.com of specific dates on which, and the time at which the Alliance Lite2, or the SWIFT WebAccess, FIN, FileAct or SWIFTNet service is unavailable.

Planned unavailability can be for the following events:

• downtime due to scheduled equipment maintenance
• scheduled system changes, for example, changes to software or hardware configurations or to business continuity testing

SWIFT performs system changes and maintenance during allowable downtime windows (ADW). For both the Test and the Live environment of Alliance Lite2, the allowable downtime window occurs from Saturday noon 12:00 UTC/GMT until Sunday morning 04:00 UTC/GMT.

During an allowable downtime window, the Alliance Lite2 service may be unavailable either for the whole duration of the allowable downtime window, or only intermittently.

For more information about scheduled downtimes, see the Availability statistics page. SWIFT recommends that customers subscribe to the products and services notifications (at Operational status notifications) to be notified of any maintenance updates.

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 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 unplanned 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 regards 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 wish 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: 1,200 messages per day in each direction
  - FileAct: 1,200 files per day in each direction

- **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 300 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 and the Alliance Lite2 AutoClient 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.

Connectivity

Alliance Lite2 requires the following connectivity:

- Customers are strongly recommended to use Alliance Connect VPN boxes 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.

Note TLS 1.0 and TLS 1.1 are still supported for compatibility reasons.

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 VPN boxes when channel certificate is used.

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.
4 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 > Ordering & Support > 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 sanctions programmes, then contact your regional support centre.
5 Operational Services

5.1 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. Support is available to all SWIFT customers.

Individuals within a customer organisation must register to use the Support service.

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 SWIFT's Standard Plus support package.

For more information about the different services that SWIFT offers as part of the support packages and the procedure to order support, see Comparison of support packages on swift.com.

Related information

For more information about Support services, see the service description related to the applicable support package:

Support documentation

5.2 Alliance Lite2 Peace of Mind Support Pack

Definition

SWIFT has designed a payable support service with new service features specifically for Alliance Lite2 customers - the Peace of Mind pack. The Peace of Mind Pack provides customers with handholding assistance, either over the phone or over the SWIFT remote support tool (included in the pack). With this, customers get direct access to experts, detailed explanation on Alliance Lite2 usage and guidance on tasks that are performed less often. Assistance with Relationship Management (RMA) can be included as an additional, payable option. The Peace of Mind Pack also includes entitlement to additional standard and specific configuration changes.

Handholding and remote assistance

Alliance Lite2 Peace of Mind customers receive handholding support and remote assistance when contacting the SWIFT Support Centres. Handholding support and remote assistance apply to those questions that relate to Alliance Lite2 usage, such as assistance to create a message, explanation of a NAK code, or assistance to unlock or reset security tokens. It includes a subscription to the SWIFT Remote Support tool to allow the SWIFT Support analyst to access the customer's Alliance Lite2 screens and AutoClient software. Through the SWIFT Remote Support tool, SWIFT can perform changes on behalf of, and under the supervision of, the customer, such as, creating new operators, creating templates, or creating a new AutoClient instance. See List of Questions and Assistance Covered by the Peace of Mind Pack on page 38 for a list of questions/actions covered by the Peace of Mind pack.

Non-urgent request may not be handled immediately. If a knowledgeable support engineer is available, the handholding will start immediately. If not, the customer support centre will agree with
the customer on a time to perform the requested support. This also applies to requests that are received close to the closing time of the customer support centre.

For further information about remote Support, see the relevant SWIFT Support service description.

**Relationship Management (RMA)**

Alliance Lite2 Peace of Mind customers can order the option of RMA management by SWIFT personnel. Upon customer request to SWIFT Support, the support analyst will perform RMA management on the customer's behalf, through the SWIFT Remote Support tool. This requires the availability at the customer's site of a user with RMA management permissions who will give the instructions to SWIFT and will supervise SWIFT's actions.

**Additional configuration changes**

Alliance Lite2 Peace of Mind customers are entitled to request additional standard and specific configuration changes as part of their service subscription. The entitlement covers a reasonable number of configuration changes, to provide an Alliance Lite2 configuration that corresponds to the customer requirement, but is still in line with the Alliance Lite2 offering. SWIFT reserves the right to accept or reject any configuration change requests.

**Ordering**

To order the Peace of Mind pack, contact your SWIFT Account Manager. To order additional configuration changes, contact SWIFT Support.
6 Users' Responsibilities

6.1 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 a VPN box 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 Box Terms and Conditions and in the Alliance Connect Service Descriptions.

6.2 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 18. 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 18

6.3 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

6.4 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 18.

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 19), 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 in accordance with the customer security controls set out in the SWIFT Customer Security Controls Framework. 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.
6.5 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 Documentation (User Handbook Online).

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 security officers must manage the RBAC roles for browse users to use browse services through Alliance Lite2.

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 15.

**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.
7 Contractual Framework

7.1 SWIFT General Terms and Conditions

SWIFT General Terms and Conditions

The SWIFT General Terms and Conditions govern the provision and use of Alliance Lite2, except otherwise provided in section Liability on page 36 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.

Liability

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 security tokens are governed by the HSM Tokens and Cards 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).

Services related to Alliance Lite2

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

The configuration changes and the Peace of Mind Support pack 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 separate Consulting Services Proposal.
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, they must immediately inform SWIFT thereof and treat all related information, data or materials as SWIFT confidential information.
A List of Questions and Assistance Covered by the Peace of Mind Pack

Customers subscribed to Alliance Lite2 Peace of Mind Pack receive additional handholding support and remote assistance for the following activities:

• Assistance to create new user or AutoClient token
• Assistance to unlock or reset tokens
• Assistance to renew token certificates
• Ad-hoc explanation of message fields when manually creating FIN messages
• Assistance to create message templates
• Explanation of NAK code
• Assistance to create an RMA request (for customers who have purchased the RMA management option)
• Assistance to respond to (accept/reject) an RMA request (for customers who have purchased the RMA management option)
• Additional configuration changes (routing rules, profiles)
• Assistance with the AutoClient installation on another machine
• Assistance to locate a message (for example, has the message been sent to SWIFT?)
# List of Available Configuration Changes

## B.1 Standard Configuration Changes

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

<table>
<thead>
<tr>
<th>Configuration change</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add one unit for manual message processing.</td>
<td>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.</td>
<td><a href="#">Alliance Lite2 User Guide</a> (Message Creation section)</td>
</tr>
<tr>
<td>Add or change one operator profile.</td>
<td>Additional operator profiles can be defined to customise the applications and the activities that the operators can perform.</td>
<td>The list of default operator profiles is available in the <a href="#">Alliance Lite2 Administration Guide</a> (Default Operator Profiles section).</td>
</tr>
<tr>
<td>Add one unpublished BIC.</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Generate a PDF automatically for all the messages that are sent and/or received through AutoClient.</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Change the FIN message default output format from RJE to XMLv2.</td>
<td>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.</td>
<td><a href="#">Alliance Lite2 AutoClient User Guide</a> (Message File Preparation section)</td>
</tr>
<tr>
<td>Configuration change</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Change the message flow so that all messages sent to SWIFT through AutoClient require authorisation.</td>
<td>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 authorisation before sending to SWIFT.</td>
<td>Alliance Lite2 AutoClient User Guide (Successful Upload section)</td>
</tr>
<tr>
<td>Change the message flow so that the ACKs of all messages created manually are routed to the AutoClient directory.</td>
<td>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.</td>
<td>Alliance Lite2 User Guide (Management of Messages section)</td>
</tr>
<tr>
<td>Segregate one received message flow into its own, separate subdirectory (for example, based on MT, correspondent, request type).</td>
<td>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.</td>
<td>Alliance Lite2 AutoClient User Guide (Reception Directory section)</td>
</tr>
<tr>
<td>Segregate the message flow to separate subdirectories based on the traffic type (for example, FIN, FileAct).</td>
<td>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.</td>
<td>Alliance Lite2 AutoClient User Guide (Reception Directory section)</td>
</tr>
</tbody>
</table>
## B.2 Specific Configuration Changes

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

<table>
<thead>
<tr>
<th>Configuration change</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add one BIC11.</td>
<td>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.</td>
<td>Knowledge base tip <a href="#">5017673</a></td>
</tr>
<tr>
<td>Change the message flow so that a subset of messages sent to SWIFT through AutoClient require verification or authorisation.</td>
<td>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.</td>
<td><a href="#">Alliance Lite2 AutoClient User Guide</a> (Successful Upload section)</td>
</tr>
<tr>
<td>Change the message flow so that a copy of all messages (including ACKs and manually created messages) is sent to the AutoClient Archive directory.</td>
<td>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.</td>
<td><a href="#">Alliance Lite2 User Guide</a> (Management of Messages section)</td>
</tr>
<tr>
<td>Change the message flow so that the ACKs (FIN, FileAct) are routed to a separate AutoClient subdirectory.</td>
<td>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.</td>
<td><a href="#">Alliance Lite2 User Guide</a> (Management of Messages section)</td>
</tr>
<tr>
<td>Configuration change</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Change the message flow so that the delivery notifications (FIN, FileAct) are routed to a separate AutoClient subdirectory.</td>
<td>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.</td>
<td>Alliance Lite2 User Guide (Management of Messages section)</td>
</tr>
<tr>
<td>Change the unit assignment of messages during message processing.</td>
<td>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.</td>
<td>Alliance Lite2 User Guide (Management of Messages section)</td>
</tr>
<tr>
<td>Change network configuration to disable internet access, for customers connecting through Alliance Connect.</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Import FIN message templates created in Alliance Access or created in an Alliance Lite2 test environment.</td>
<td>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.</td>
<td>Alliance Lite2 User Guide (Use Message Templates section)</td>
</tr>
<tr>
<td>Import MX message templates, created in Alliance Access or in an Alliance Lite2 test environment.</td>
<td>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.</td>
<td>Alliance Lite2 User Guide (Use Message Templates section)</td>
</tr>
</tbody>
</table>
Note

The following requests are part of the Standard Plus 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. When requested to SWIFT, the change is activated at the next SWIFT ADW and remains active until the following SWIFT ADW.
  
  For more information, see Knowledge Base tip [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.
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.

Hours of service

The Alliance Lite2 Live environment is available from Sunday morning 04:00 UTC/GMT until Saturday noon 12:00 UTC/GMT unless otherwise notified in advance on the Operational status page.

Service availability objective

Outside the allowable downtime windows (ADW) and in the cases of unplanned unavailability as described in Service Availability on page 23, the monthly Alliance Lite2 weighted service availability is targeted at 99.9%.

Availability is defined as the percentage of time during which Alliance Lite2 is available to Alliance Lite2 users. The availability calculation is weighted to give a single overall availability percentage that reflects the impact of outages affecting only parts of the user base.

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_3402 Report (report available upon request).

For customer configuration changes, see Payable Configuration Changes on page 10.
Notification and reporting of incidents to customers

See sections Reporting and Service Incident of the Standard Plus Support Service Description.

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 an incident, with potential notification to the SWIFT Command Centre.

Disaster recovery procedures

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, 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, see Service Availability on page 23.

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 GUI availability is tested by simulating a user’s activity. Additionally, the standby site infrastructure replicates the infrastructure of the primary site.

Response time to customers requests

See section Call and Problem Management of the Standard Plus Support Service Description.
Legal Notices

Copyright

SWIFT © 2017. All rights reserved.

Disclaimer

The information in this publication may change from time to time. You must always refer to the latest available version.

Translations

The English version of SWIFT documentation is the only official and binding version.

Trademarks

SWIFT is the trade name of S.W.I.F.T. SCRL. The following are registered trademarks of SWIFT: the SWIFT logo, SWIFT, SWIFTNet, Accord, Sibos, 3SKey, Innotribe, the Standards Forum logo, MyStandards, and SWIFT Institute. Other product, service, or company names in this publication are trade names, trademarks, or registered trademarks of their respective owners.