

TOTAL SWIFT SOLUTIONS FOR FINANCIAL SECTOR

Minimum Investment, Maximum Saving



**SWIFT Alliance Gateway 7.0 and Alliance Access 7.0
SWIFT Connectivity & Messaging Infrastructure**

HOSTED BY
SWIFT SERVICE BUREAU OF SRI LANKA



TOTAL SWIFT SOLUTIONS FOR FINANCIAL SECTOR

Minimum Investment, Maximum Saving

Table of Contents

SWIFT ALLIANCE GATEWAY (SAG) 7.0 & ACCESS 7.0 (SAA) HOSTED BY LFSBL	3
Bundle of benefits from Hosted option of SWIFT Total Solution	5
Operational Framework of hosting environment	7
Requirements for Users	8
Common Standards of Operations of Hosting SAA	9
Time line for migration	13
Migration to Total SWIFT Solution – LFSBL basic steps to follow	14

**SWIFT Alliance Gateway 7.0 and Alliance Access 7.0
SWIFT Connectivity & Messaging Infrastructure**

HOSTED BY
SWIFT SERVICE BUREAU OF SRI LANKA



SWIFT ALLIANCE GATEWAY (SAG) 7.0 & ACCESS 7.0 (SAA) HOSTED BY LFSBL

BEST OPPORTUNITY TO REDUCE TOTAL COST OF OWNERSHIP OF SWIFT CONNECTION AND TO SAVE TIME AND FINANCIAL RESOURCES IN FUTURE UPGRADES IN HARDWARE & SOFTWARE.

Introduction

Lanka Financial Services Bureau Ltd (LFSBL) has been successful in providing the SWIFT connectivity through hosting SWIFT Alliance Gateway (SAG) and SWIFT Net Link (SNL) since April 2008. The resilience and reliability of network hosted by LFSBL has maintained beyond the expectation of 99.99999% for SWIFT connectivity over the years.

The company has now taken a step forward by delivering another hosted solution on SWIFT Alliance Access; hosting messaging software of SWIFT in order to offer a significant cost reduction on SWIFT connectivity to its connected Banks and financial institutions with the intention of becoming a regional player in hosting **'Total SWIFT Solution Provider'** to all potential regional and domestic customers.

The LFSBL is in compliance with all relevant SWIFT Standards. This is confirmed through a detailed independent audit conducted by the SWIFT Internal Audit Team from Belgium. LFSBL will be entitled to obtain "Best Practice Label" – SWIFT Ready Connectivity in due course as a result of being compliance with Risk Management, Resilience, Reliability, Change Management, Business Continuity Plans (BCP), Disaster Recovery Preparations and testing and Document management & reporting which are specified in the criteria for Best Practice Label.

The Business Model of LFSBL is based upon the interest of SWIFT User Community and generates cost benefits, while delivering dividends for their investments in the Company.

We, LFSBL invite you to exit the model of having own support services, infrastructure and to migrate to hosted services of SWIFT total Solution on messaging and connectivity in order to achieve greater cost benefits in terms of upgrades in both hardware and software, resilience, state of the art Disaster Recover Site.

If you are a light User on Alliance entry, you will be able to enjoy the luxury of Alliance Access at a relatively lower cost than using Alliance Entry, if you are a heavy User you will enjoy the luxury of having a greater capacity on future growth of traffic without additional costs of upgrading licenses for platforms (OS) and applications (SWIFT) and will enjoy benefits of future standards of payments and settlement platforms such as SEPA.

[\(http://ec.europa.eu/internal_market/payments/sepa/\)](http://ec.europa.eu/internal_market/payments/sepa/).

This document details the operational framework; standards and financial considerations for hosting SWIFT Alliance Gateway 7.0 & Access 7.0 by LFSBL.

Please review the details and contact support@lfsbl.com or open a case at www.lfsbl.com for a meeting to verify details.

Bundle of benefits from Hosted option of SWIFT Total Solution

1. **The Cost of connectivity to SWIFT Global Network** will be reduced immediately in terms of Annual recurring fees for SWIFT Net Link (SNL), Hardware Security Module (HSM) and SWIFT Alliance Gateway (SAG). The User need to pay only an annual subscription and a monthly subscription for connectivity.
2. **The Cost of Using SWIFT Alliance Access is reduced by 30-35%** immediately for all Users.
3. **Users who are using SWIFT Alliance Entry** will be able to **enjoy the privileges of using SWIFT Alliance Access at relatively lower Cost** than using Alliance Entry.
4. **No headaches** of preparation for updates in terms of procuring hardware, software, operating software, maintenance of infrastructure, manning the infrastructure and security. You just need to log in and send messages.
5. **No Cost** for consultation, experts in maintaining SWIFT Application Servers, environments, back-up procedures etc.
6. **At NO extra cost**, the provision of state of the Art Disaster Recovery facilities which has been inspected & approved by SWIFT Internal Audit for practice which is in compliance with SWIFT standards and standards of Central Bank of Sri Lanka.
7. Ability to perform all secure messaging tasks on a leveled platform which is maintained **in accordance with SWIFT Internal Audit Guidelines and under direct supervision of SWIFT Asia Pacific.**

8. **Resilience and reliability assured** on a Services Level Agreement which is bound by SWIFT Terms & conditions and all possible risks are covered by comprehensive insurance coverage.

9. **Proven** reliability and resilience of network availability at 99.99999% since 2008 (commencement of SWIFT Service Bureau in Sri Lanka)

Operational Framework of hosting environment

Connectivity – SWIFT Alliance **Gold & Silver** connectivity

Main site

SWIFT ALLIANCE GATEWAY (SAG) 7.0 2 SERVERS

HSM (Hardware Security Module) 2 Units

SWIFT ALLIANCE ACCESS (SAA) 7.0 2 SERVERS

SWIFT WEB PLATFORM 7.0 2 SERVERS

Disaster Recovery site

SWIFT ALLIANCE GATEWAY (SAG) 7.0 2 SERVERS

HSM (Hardware Security Module) 2 Units

SWIFT ALLIANCE ACCESS (SAA) 7.0 2 SERVERS

SWIFT WEB PLATFORM 7.0 1 SERVERS

Operating platform – Windows

Requirements for Users

Interface requirement

SWIFT Alliance Web Platform/ Workstation 7.0

System requirement

Alliance Web Platform desktops will be supported on the following systems.

Operating system	Browser
Windows XP Professional SP3	Internet Explorer 7.0 and 8.0
Windows Vista SP2	Internet Explorer 7.0 and 8.0
Windows 7	Internet Explorer 8.0

Alliance Workstation desktops will be supported on the following systems.

Operating system
Windows Vista SP2
Windows Server 2008 R2

Connectivity requirement (communication links)

The basic communication link of 64K could be used. However, Users are advised to increase band width to 128K, if they are using the SAA interface hosted by LFSBL, in accordance with the growth of traffic.

In accordance with resilience requirements, Users are strongly advised to obtain services from different network partners in case of line failures to ensure optimal resiliency.

License requirements

In the event of transferring the BIC code of the respective Users when migrating, the Users are expected to place orders for transferring required BIC codes. The transfer cost will be directly charged by SWIFT and will be added with an admin portability fee of USD 2,500.

Common Standards of Operations of Hosting SAA

Please note the below mentioned operating guidelines are defined by SWIFT Design and Consulting guidelines which are used to standardize the operations of all SWIFT Service Bureaus in the world and strict compliance is mandatory for all Users, Bureaus and Service Partners

Obligations/responsibilities of LFSBL

1. One unit will be assigned to each BIC code to ensure security and confidentiality of data with a naming convention which will carry the first 4 characters of the respective BIC.

E.g. – ABCDLK001 (The naming convention is following as first four characters of BIC code). Further a User would require to create more UNITS department wise SWIFT will follow the naming convention as ABCDLK001treasury etc. (UNIT can be defined maximum up to 24 characters alphanumeric).

2. A delegated LSO (Left Security Officer), RSO (Right Security Officer) will be created for each institution Unit by LFSBL. E.g. LSO_ABCD, RSO_ABCD. Initial Passwords for delegated LSO and RSO of respective institution will be provided by LFSBL and respective User must immediately change the passwords with NEW Alpha numeric passwords with 6-20 characters with a mandatory minimum of 3 numeric characters.
3. LFSBL will possess one key profile for monitoring which will be granted the below rights.
 - a. Monitoring SAA and Killing (terminating) sessions at AWP which are not properly terminated.
 - b. Monitoring scope will consist of the following.
 - i. Login details of all connected parties
 - ii. Message traffic, i.e. no of messages in queues/ overflow etc.
 - iii. Event journals
 - iv. System processes, utilization of Hard Disk etc.
 - v. Message sessions – in order to terminate improper log outs.
4. LFSBL will define standardized routing e.g. one routing rule for Outgoing (to receive ACK / NACK) messages and one for Incoming messages per BIC and the UNITS (defined in no.1) will be assigned to each rule and set up routing in a way each bank gets 2 message partners; one for printing and one for “file output”.
5. ONE Message Partner for file input (to inputs the messages created by back office application) will be set up for Institutions (those who require). Institutions are expected provide the requirement of message partners in advance before they migrate.

E.g. MABCLKtreasury; MABCLKINT

6. LFSBL will set up 1 emission and 1 reception profile per BIC for RMA. Extra services like FileAct can be configured if needed.

7. LFSBL will import RMA agreements of each bank which should be provided by User in advance before migration.
8. LFSBL will be responsible for message archiving from the date of migration of each User. LFSBL will NOT be responsible for data before the date of migration.
9. LFSBL will create and customize security profiles that are the same in design for each bank that put proper restrictions in place. It will not be possible to take into account individual requirements per User.
10. LFSBL will not create operators; they must be individually created by the User.
11. LFSBL will make use of restricted delegations to achieve maximum security.
12. LFSBL will use a common BANK&BIC file and will NOT add individual changes to it.
13. LFSBL may customize the calendar for automated actions. For automation of defined actions, can be customized as per the calendar defined in the Alliance application. Some of the actions like Secure Login and Select are possible to be scheduled based per BIC.
14. LFSBL will archive event journal logs daily. The same logs will get backed up weekly. Backed up event logs are available to view for one month. Thereafter it will get backed up and removed from MAIN Live server. Upon requests in advance by Users, it will get restore to view for two days, subsequently it will get backed and remove from MAIN live server once again.

LFSBL will further archive / backed up the messages weekly. It is the responsibility of the respective bank/s to complete the messages **every day**. The entire archived message will be available for six months.

After six months archived messages will not be available on the MAIN Live server. Based upon the request in advance it will get restored back for two days, thereafter it will get backed and remove from MAIN Live server once again.

15. LFSBL will store data for maximum of 7 years as per Sri Lankan & Global Regulatory Standards.
16. LFSBL will levy an annual recurring fee for archived data exceeding 7 years as per individual requests by Institutions in accordance with respective requirements.
17. LFSBL will configure the parameters in Alliance application as per SWIFT's best practices in consultation with SWIFT Asia Pacific Consulting Team.
18. LFSBL may add future standards of operations periodically in accordance with SWIFT advice.

Obligations /responsibilities of Users

1. Users are expected to change the Passwords of LSO and RSO that are provided by LFSBL immediately after receipt. All Passwords must be “Alpha numeric” and must have minimum 6 and maximum of 20 characters which should consist with minimum 3 numeric characters.
2. Login to/out to SWIFT Network
 - a. Manual login has to be done as per routine requirements of the Users.
 - b. Automatic scheduling is possible in accordance with respective requirements of individual Users on written submission by respective User
 - c. Proper logout is Mandatory without closing the window or using other methods to close the window of login/out. Whenever User login to AWP, traffic will be using HTTPS protocol. Therefore a proper logout is mandatory.
3. Creation of additional profiles at Supervisor level is possible on written submissions with defined rights to be granted on a form provided by LFSBL. The form should be duly signed and authorized by the LSO and RSO of the respective User. The responsibility of the Usage and security of this/these profile/s will entirely be upon the LSO and the RSO of the respective institution and neither **LFSBL nor SWIFT will not undertake (if/any) liabilities arising out of the usage and/or security of this/these Supervisor profile/s.**
4. A User has the full right to create any number of operators for the Unit assigned to the respective institution.
5. Users are required to complete messages on daily basis as per SWIFT specified standards. Incomplete messages will NOT be (live) a part of archiving process by SAA default.
6. Users are expected provide the reasons / details of the additional Message Partners. Naming convention for message partner / exit points can follow as; first four letters of the BIC code of the bank, name of the message partner.
7. RMA profiles (emission and reception profiles) have to be activated on daily basis when ever daily login is done. Automated activation is possible on written requests authorized by respective LSO and RSO of the institution.
8. Users are required to create new template/s after migration which contains respective defined UNIT in the creation menu. It is the responsibility of the bank to remove the unwanted templates. Limitation of templates per banks is Five hundred (500).
9. Users are expected to follow Planned Down time published at www.lfsbl.com for any activity which requires “House Keeping” mode. Please note that any activity which requires “House Keeping” mode will be allowed only in a Planned down Time which will be displayed at www.lfsbl.com

10. Users, who require data archives exceeding 7 years, should notify LFSBL in writing with 12 months notice.
11. Users may use either SWIFT Alliance Web Platform (AWP)/SWIFT Alliance Workstation (AWS) to create, modify and approve/authorize messages. Users have the options of downloading messages in PDF/HTML format to a local hard disk required, through the AWP by clicking on the message instance.
12. Users should not keep SAW /AWP session open (ideal) for long time (more than 15 minutes. By default, 30 minutes is an inactivity time). As soon as work is over User should required closing the session.
13. All Users are required to change the password in 30 days.
14. Five (5) incorrect passwords will lock / disable the User account. It will be required respective LSO /RSO's intervention to unlock.
15. Users are expected to report all incident/trouble reporting in case management at www.lfsbl.com . All incident/trouble reporting on telephone has to be followed up with an e-mail or entry in case management at www.lfsbl.com

Time line for migration

USERS' DECISION

Users are advised to review the timeline for SWIFT payments at the beginning of each year. The termination notice must be given by the User and there will be a 90 days period from the date of termination which could be utilized for transfer, install and test the required applications and connectivity. This period will facilitate smooth migration from direct connectivity to shared infrastructure connectivity.

Please do not hesitate to contact support@lfsbl.com or gm@lfsbl.com for further information or clarifications. Meetings could be arranged at mutually agreed dates according to your requirements.

Migration to Total SWIFT Solution – LFSBL basic steps to follow

1. **User**
Send official email to gm@lfsbl.com
2. **LFSBL**
Provide guidelines to register
3. **User**
Send required details as per guidelines
4. **LFSBL**
Amend > guide>Accept / Revise
5. **LFSBL**
Upon acceptance the SLA will be signed by the parties.
6. **User**
Sign the SLA confirming the date of engagement
7. **LFSBL**
Send invoices for joining fees and one time charges for communications and applications
8. **User**
Settlement of payments
9. **LFSBL**
Upon the confirmation of payments, testing of communication links will commence and the establishment of communication links will be approved.
10. **User**
Approve the inclusion of required BIC codes to LFSBL license and confirm the technical information required
11. **LFSBL**
Upon approval User's BIC/s will be swapped to License of LFSBL.
12. **LFSBL**
Confirmation on BIC inclusion and communications links installation.
13. **User**
Internal Preparation for testing of communication and SWIFT messaging
14. **LFSBL**
Inform readiness for testing and check readiness at User level.
15. **User**
Commence testing (minimum 30 days maximum 60 days). Concurrently or after testing User may give termination notice to SWIFT
16. **LFSBL/User**
Upon success, LFSBL will advise on live cut over 100% and User may determine the date.
17. **LFSBL**
Final readiness check before Live cutover
18. **User**
Live cut over
19. **LFSBL**
Monitoring 24/7 -365days and maintain 99.99999% availability of network

