



SWIFTNet CONNECTIVITY via
“SERVICE BUREAU”
BCG, Business Computer Group





TABLE OF CONTENTS

1. Introduction
2. “Service Bureau” definition
3. Technical Features
4. Connectivity Infrastructure
5. Services offered
 - a. SWIFTNet connection for new users
 - b. SWIFTNet connection for SWIFTAlliance users
6. Customer Installed Based Figures
7. Annex
 - a. SWIFT Board Approval
 - b. “Service Level Agreement”
 - c. “Service Bureau Policy”

INTRODUCTION

As part of its corporate policy **S.W.I.F.T** has established the medium term objective of triple the number of SWIFTNet users, and the reduction of costs is the corner stone of this strategy which aims to increase the number of small and medium size institutions with more competitive options to access SWIFTNet. The “Service Bureau” is the S.W.I.F.T. strategy to achieve this goal, since its philosophy is based in total cost of ownership reduction, operative impact simplification and minimizing the financial terminal investment, along with its maintenance costs and communication infrastructure, offering at the same time several complementary alternatives for network connectivity, all these supported by economy of scales principles.



BCG, Business Computer Group, the SWIFT Business and Service partner for Northern Latin America, aligned to this corporate strategy is pleased to offer the following alternatives to connect to SWIFTNet through its Business Partner Service Bureau, which grants access to SWIFTNet FIN, among others SWIFTNet services. BCG offers connectivity options to banks located in several countries; from Mexico to Peru, plus the Spanish, French and Dutch Spoken islands of the Caribbean. It is important to stress this “Service Bureau” is based upon the SWIFTAlliance suite of products, such as Access, Gateway, Browser and SWIFTNet Link.



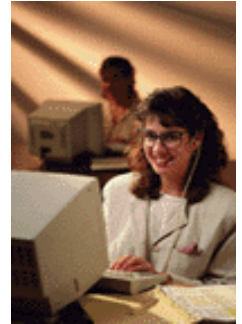
The Services offered in this proposal were designed to satisfy the operative of institutions looking for secure, low cost, fault tolerant and permanent connectivity to SWIFTNet; these services are established from the “Service Bureau”, either with the approach of a Alliance Workstation user or taking advantage of the SWIFT Alliance Gateway functionalities, RAHA, for those institutions who already have SWIFTAlliance Entry/Access licenses. The connectivity services are prepared to meet Disaster Recovery events, according to the SWIFT requirements.

Last but no least, it is important to mention BCG Business Partner Service Bureau has been approved by the “SWIFT Board of Directors”. Also it is audited and supervised by “third party” companies contracted by SWIFT, therefore meeting the criteria and conditions specified in the enclosed document “Service Bureau Policy”. Please note this Service Bureau is operated by the staff of engineers of Business Computer Group, which has been certified by the SWIFT “Service Partner Program” and also by the its Education Department. All of the above allow us to affirm our services meet the highest industry standards of quality.

“SERVICE BUREAU” DEFINITIONS

A “Service Bureau” is a center approved by SWIFT with the objective of granting access to the SWIFTNet InterAct, FileAct, Browse and FIN services. This last one, SWIFTNet FIN, allows the “on line”, real time, financial message exchange between institutions through a Multi Vendor Secure IP Network, MV IP-SIPN, architecture.

Additionally to the others SWIFTNet services, BCG Service Bureau offers SWIFTNet FIN connectivity to those institutions willing to exchange financial messages.



“SERVICE BUREAU” TECHNICAL FEATURES

This service center distributes its processing among its “Sites” located at Panama and Caracas, offering independent and complementary SWIFTNet connectivity, Technical Failures resistance and Disaster Recovery proved. Each site has available “Production”, “Back Up” and “Test and Training” environments.

As far as Servers architecture is concerned, each site has the following Technical Features:

I) SWIFTAlliance Access Production and Back Up:

Two Servers Dell, PowerEdge 1600SC, Processor Xeon, 2.0GHz, 1 GB RAM, 36 GB DD, HotSwap Raid 1.

II) SWIFTAlliance Gateway Production and Back Up:

Two Servers Dell, PowerEdge 1600SC, Processor Xeon, 2.0GHz, 1 GB RAM, 36 GB DD, HotSwap Raid 1.

III) SWIFTAlliance Access y Gateway “Test and Traininig”:

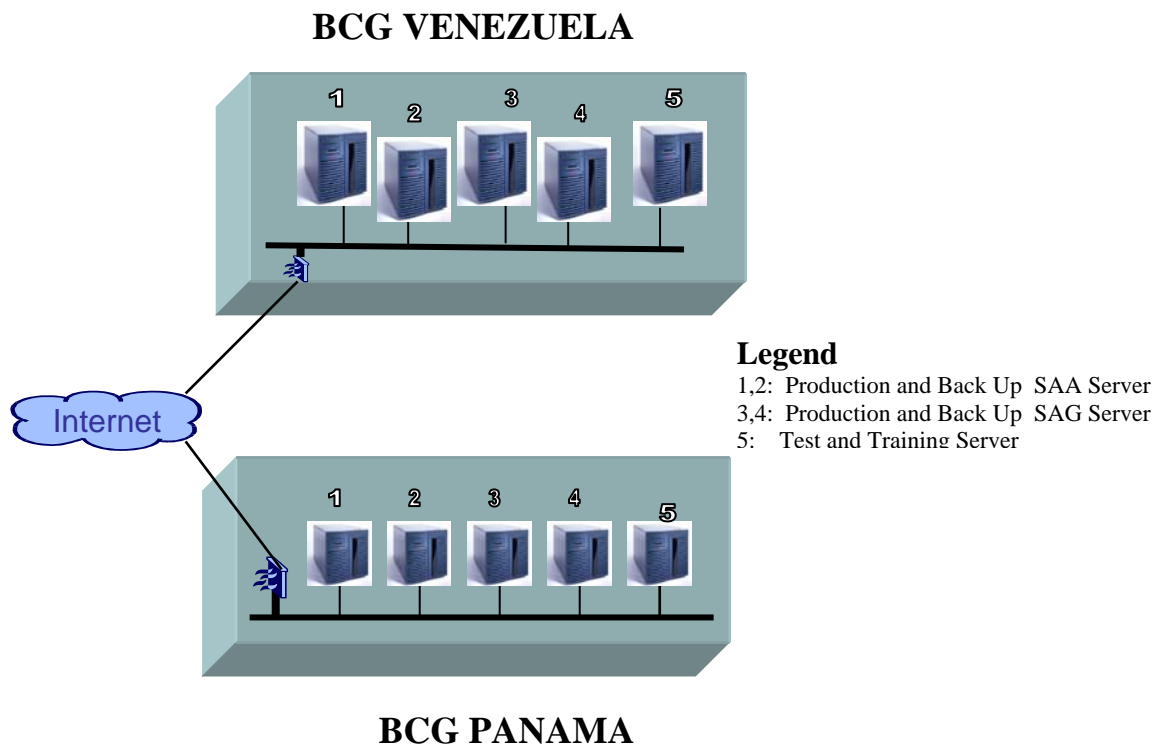
One Server Dell, PowerEdge 1600SC, Processor Xeon, 2.0GHz, 1GB RAM, 36 GB DD, HotSwap Raid 1.

Since the disks are configured for “Disk Mirroring”, failures recovery capacity is very powerful, also the “Hot Swap” technology allows them to be removed dynamically, making easier the maintenance and increasing the tolerance, obtaining as a result a resilience environment.

The Servers are protected against unauthorized user access by a couple of high availability Firewalls/VPN connected through a Master/Slave approach, via NSRP protocol. Both security equipments create a protected zone, which unique access is enabled by virtual tunnel IPSEC.

At Panama's site the Internet access is accomplished through a permanent 1024K bandwidth link, shared by two different Internet Service Providers (ISP), with a couple of routers connected using BGP protocol to dynamically balance the sessions of users, allowing high availability and creating an ISP failure tolerance connection. At Caracas Site the access is reinforced with an additional third ISP.

The Service Bureau is located in buildings with own power supply, with maximum external failure recovery capacity of 15 minutes. Also each of its sites has its own UPS with capacity of two hours of internal energy supply, which give operations autonomy from the external source.

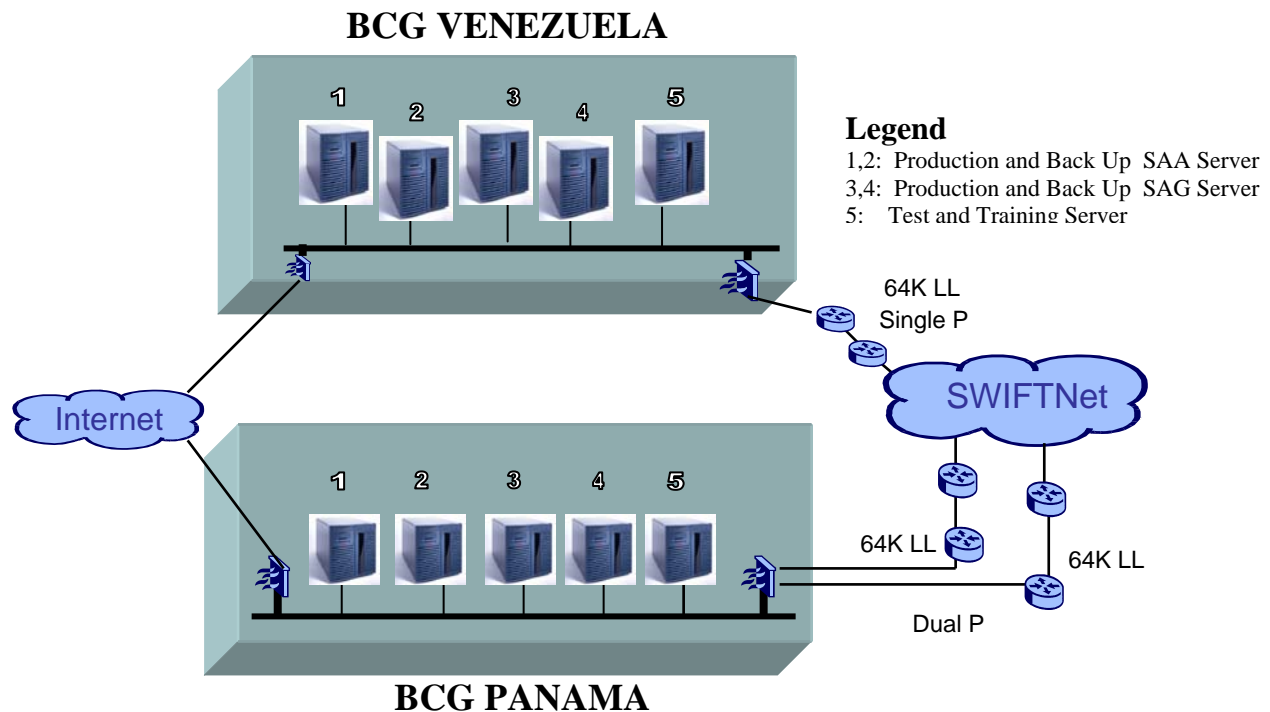


CONNECTIVITY INFRASTRUCTURE

As consequence of the SWIFTNet migration, one of the factors to watch carefully is how the network connectivity is implemented and which connectivity option is chosen, accordingly it is extremely important to select a configuration resistant to potential Network partner's communication failures. The Dual P model proposed by SWIFT was created to support failures related to communication lines at VPN box level. Complementary the Single P model brings permanent connection in order to implement the MULTILINE connectivity mode, designed to be Disaster Recovery proved.

BCG Service Bureau sites are supported by a mixed scheme of Dual P and Single P communication model, implementing a MULTILINE access of three dedicated channels with a bandwidth of 64K each one, with communication routers, Firewalls and VPN boxes for creating "Secure Tunnel". For BCG Panama's Dual P site, the VPN Boxes are interlinked and constantly performs "hand shake" verification procedure; accordingly in case of failure of the primary connection channel, instantaneously the idle channel automatically takes control of the connection.

Both sites are connected to SWIFTNet in ACTIVE-ACTIVE mode through two different Network Partners, which makes the Service Bureau also tolerant to failures at this level, being the traffic of messages concurrent at BCG premises.



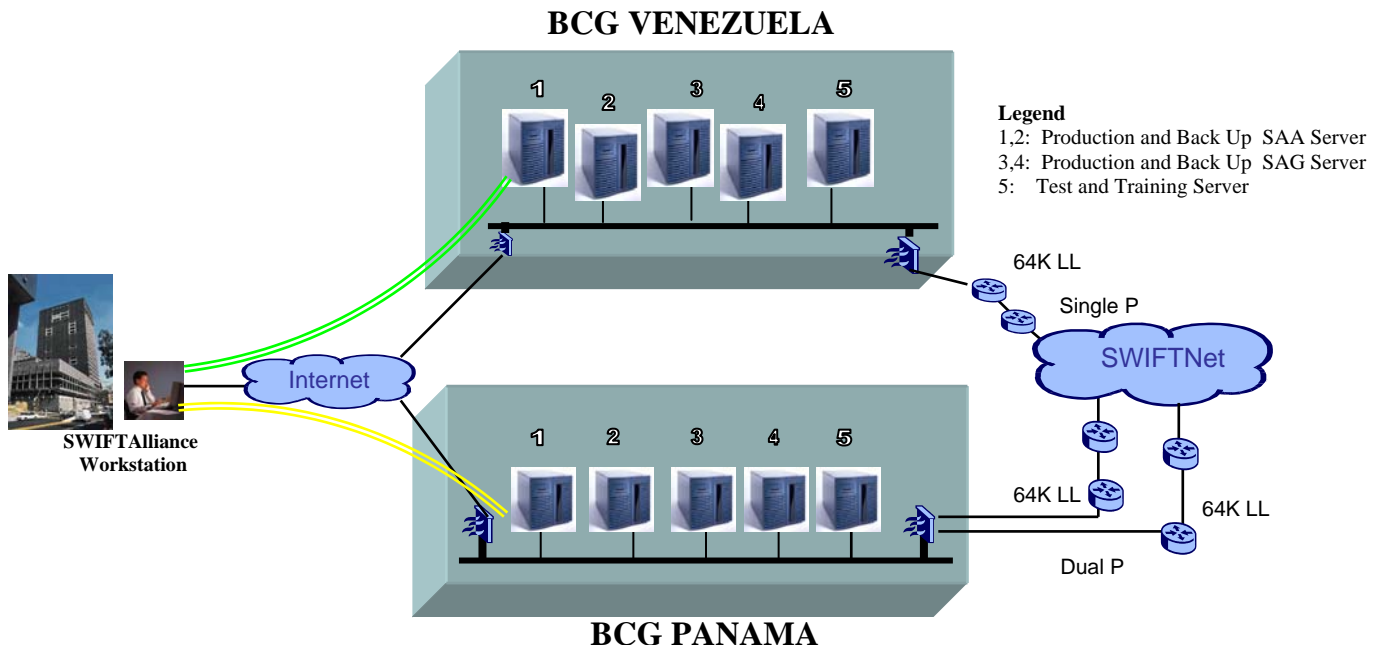
OFFERED SERVICES

1. SWIFTNet connection for new users

SWIFTAlliance Workstation: Within this option the financial institution installs at its facility a permanent connected workstation to the “Service Bureau” through two Internet based, IP Sec VPN tunnel. In order to protect the access to the “Service Bureau”, each user has installed two Firewalls/VPN boxes at his SWIFT Alliance workstation to create virtual tunnels towards the SWFT Alliance Server. On the other hand, the Service Bureau has three different secure internet access connection supplied by three different Internet Service Providers which offer high availability resilience scheme; and supports redundant communication channels from the SWIFT Alliance Access server to the SWIFT Alliance Workstation, located at the customer premises. Vis-à-vis the customer, it is highly recommended to contract two independent Internet Connection with different ISP’s to implement among them BGP protocol.

The Message Creation, Verification, Authorization Process, Message print, Login/Select to SWIFTNet FIN, Creation, Deletion or Modification of Pre Agreement, and the SWIFT Messages exchange is performed at the workstation session. The BKE environment preparation for the authentication of messages, as well as the certificates administration must be performed from the Service Bureau Alliance Access Server.

It is important to mention that on daily basis, the BCG Panama and BCG Venezuela Alliance Access servers perform asynchronic replications for the data base, accordingly after the “end of day” processes both servers are equalized.

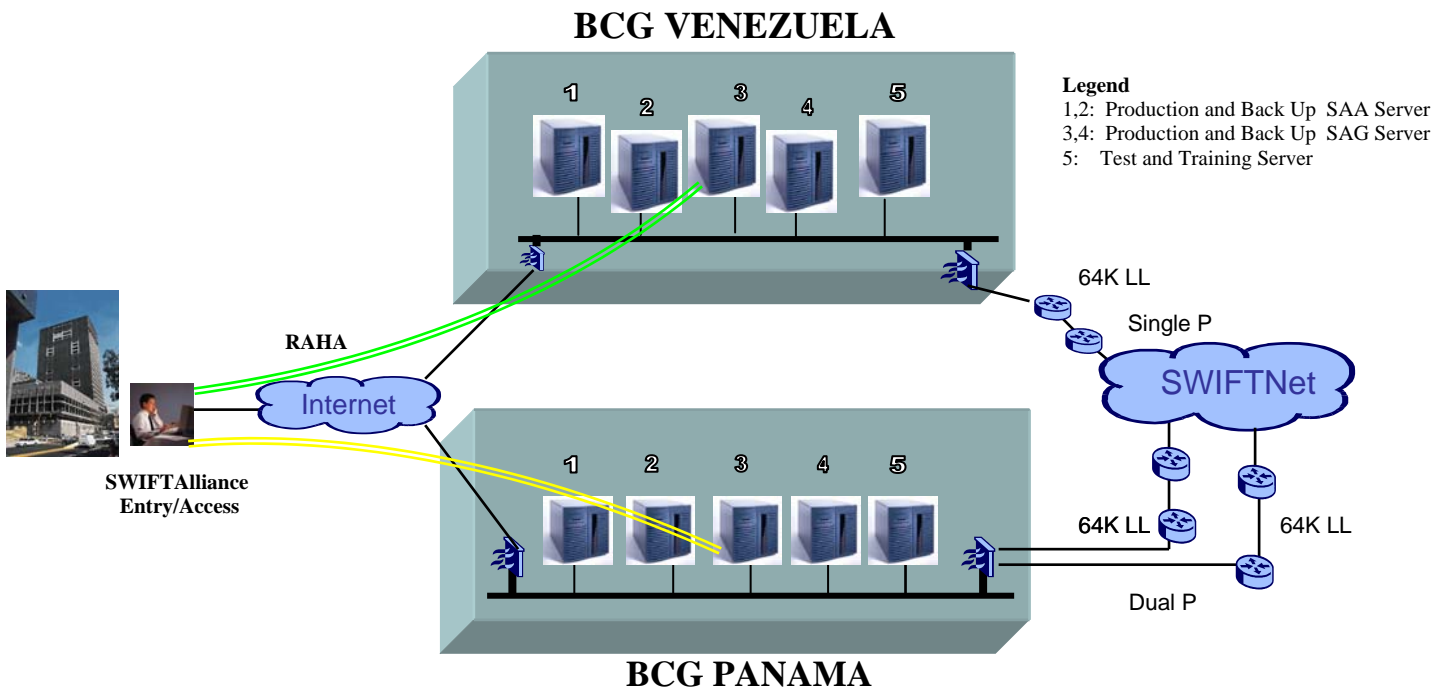


2. SWIFTNet connection for SWIFTAlliance Entry/Access users

This option is recommended for those users who already acquired SWIFT Alliance Entry/Access and wish to reduce the connectivity cost, leveraging at the same time the SWIFTNet technical infrastructure. The SWIFTNet link and SWIFTNet Access Port are discarded, along with their recurrent annual fee; and replaced by the SWIFTAlliance Gateway “Remote Api Host Adapter” RAHA component, which enables the financial message exchange from the bank to SWIFTNet, via the Service Bureau, lowering the cost and securing the permanent connection. In this option the financial institution is permanently connected to SWIFTNet FIN through two internet based IP Sec VPN tunnel, created by two VPN boxes from its premises to the Service Bureau facilities. Vis-à-vis the customer, it is highly recommended to contract two independent Internet Connection with different ISP’s to implement BGP protocol.

The Message Creation, Verification, Authorization Process, Message print, Login/Select to SWIFTNet FIN, Creation, Deletion or Modification of Pre Agreement, Sending/Receiving of SWIFT Messages and BKE environment preparation are performed within the SWIFT Alliance Entry/Access of the bank. The certificates administration as well the message routing to each users is responsibility of the Service Bureau.

It is important to highlight that the message exchange among the SWIFT Alliance Entry/Access and the SWIFT Alliance Gateway is protected by a VPN Virtual Tunnel plus the Firewalls and security certificates, which grant access only to authorized users.



CUSTOMERS INSTALLED BASE FIGURES DECEMBER 2006

- a. Connected Banks: **111**
 - i. Production: **105**
 - ii. Implementation phase: **6**

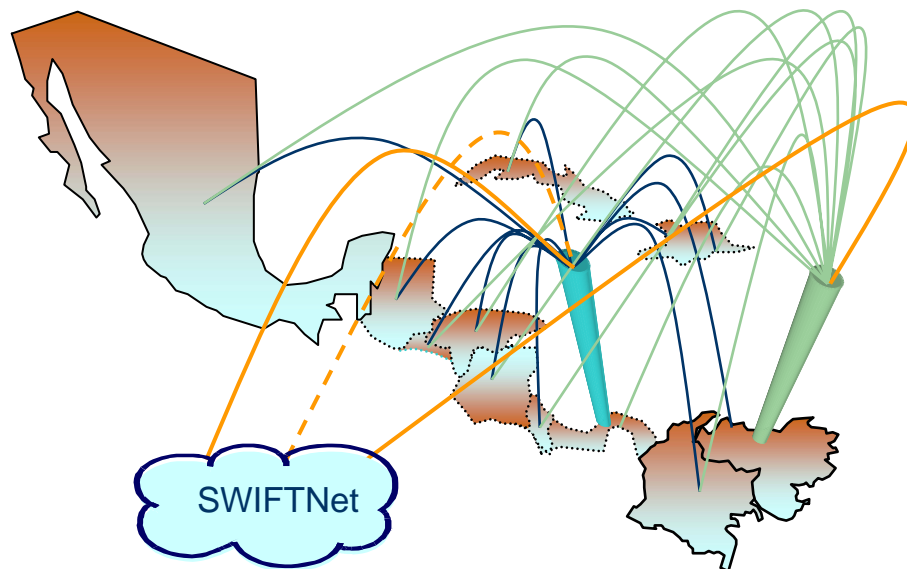
- b. Daily traffic x Bank:
 - i. Lower Level: **100 msg x day**
 - ii. Higher level: **2,000 msg x day**

- c. Service Bureau daily traffic: **10,500 messages**

- d. Central Banks Connected: **5**

- e. Connected Countries: **16**
 - i. North America: **2**
 - ii. Central America: **7**
 - iii. South America: **2**
 - iv. Caribbean: **5**

Belice	Cuba	Guatemala	México	Diminican Republic	Venezuela
Colombia	Curacao	Haití	Nicaragua	Saint Marteen	
Costa Rica	El Salvador	Honduras	Panamá	USA	



ANNEX



SOCIETY FOR WORLDWIDE INTERBANK FINANCIAL TELECOMMUNICATION

10 July 2003
BS-bm


BCG, Business Computer Group
Panama, S.A.
Mr. Felipe Rios
Executive Manager
World Trade Center, 53 Rd. Street
6th Floor, Office 605
PANAMA CITY
Panama

Dear Sir

We are pleased to advise you that the Board of Directors approved on 10 July 2003 the application of BCG as a not majority owned Service Bureau. However, please advise the name of the users to whom you will offer services, as these have to be communicated to our Audit Department.

Yours faithfully


Brigitte Moens
Board Secretariat


Martine Loosen,
Manager, Board Secretariat

copy: Mr. H. Quintero, User Group Chairman, Banco Internacional de Costa Rica S.A.
Commercial Operations Services

S.W.I.F.T. SCRL

Avenue Adèle 1 - B-1310 La Hulpe - Belgium
Tel.: +32 2 655 31 11 - Fax: +32 2 655 32 26 - SWI1Q BE BB - www.swift.com
VAT: BE 413.330.856 - RC Nivelles: 51367

BCG Business Partner Service Bureau

SERVICE LEVEL AGREEMENT

Service Bureau Rules & Guidelines :

1. Introduction

The creation and use of a Service Bureau stems from the trend towards outsourcing of data processing to increase operational efficiency and global cost savings. This trend has been re-enforced by the evolution of telecommunication and computer technologies; the development of facilities management services and integrated banking solutions; the increasing specialisation of Financial Institutions and the engagement of the IT industry in the financial sector. Furthermore, groups of smaller Users also want to share the hardware and operating costs of their S.W.I.F.T. connections.

However, by placing S.W.I.F.T. interface operations with a Service Bureau, Users are potentially putting at risk one of their mission-critical business functions. Furthermore, the use of a Service Bureau may also jeopardise S.W.I.F.T.'s contractual commitments to other, directly connected Users for message confidentiality, integrity, availability, and system reliability.

For there to be complete confidence in Service Bureaux, the related areas of risk must be controlled to ensure secure and timely transmission and secure storage of information. To assist its Customers, S.W.I.F.T. has therefore defined a range of control measures to ensure adequate security in the relationship between Users and Service Bureaux.

According to the Service Bureau Policy, Service Bureaux must sign Service Level Agreements (SLA) with all Users to whom they provide services.

Topics to be included in such a Service Level Agreement are, amongst others:

- availability, including contingency planning
- capacity requirements
- documentation requirements
- functionality
- installation services
- performance
- procedures for fixing functional, performance or security problems
- quality
- reliability
- security
- support
- training

Auditable metrics for each of these areas should be specified. Since Service Bureaux act on behalf of their Users in managing access to S.W.I.F.T. and because of the need to maintain the integrity of S.W.I.F.T.'s network, it is imperative that Service Bureaux provide levels of service that are consistent with S.W.I.F.T.'s overall operations. This is particularly true, if a Service Bureau provides shared access to a wide variety of Users with divergent needs. If minimum service levels are not maintained, Users will not receive the service quality they expect and this will ultimately reflect poorly on S.W.I.F.T. itself.

2. Security Rules and Guidelines

The Security Rules & Guidelines detailed below are derived from S.W.I.F.T.'s own security policy, standards and practices and form an integral part of the Service Level Agreement.

In line with an expert's conclusion that technology is unlikely to provide a fool-proof solution to the risks involved with Service Bureaux, emphasis is placed on procedurally based control measures rather than technology-driven ones.

The areas of control covered are primarily:

- personnel;
- physical security, including network resilience, Uninterruptible Power Supply, selection of operating locations, and disaster recovery planning;
- data security;
- software controls.

2.1 General Controls

Processing activities for different Users utilising the same Service Bureau will be segregated.

- all data, encryption/authentication keys, cards, and other S.W.I.F.T.-related materials physically and logically separate for each of the Users utilising the same Service Bureau will be kept separate.

Implement a set of systematic, auditable processes for delivering services to the User

- an audit trail and evidence of work done will be created for each trade and be available through Service Bureau View – History Reports. The SWIFT acknowledgment will be available in this report.

Notify immediately breaches of confidentiality, integrity and availability to the User and SWIFT

Examples of such security breaches are:

- accidental or malicious disclosure of S.W.I.F.T. traffic and other sensitive data;
- accidental or malicious modification, destruction, loss of traffic or other sensitive data;
- unavailability of services.

The Service Bureau agrees to:

- notify S.W.I.F.T. of any problems which render the User's part of the network inoperative;
- identify, in consultation with the S.W.I.F.T. Customer Support Centre, whether the fault lies in the User's part of the network;
- correct the fault, if it lies in the User's part of the network;
- notify S.W.I.F.T. when the fault has been rectified and the User's part of the network is again functioning normally;
- respond correctly, if necessary, to recovery procedures initiated by S.W.I.F.T. to eliminate a fault in the S.W.I.F.T. part of the network;
- react correctly to fallback operations initiated by S.W.I.F.T. to bypass a failure in the S.W.I.F.T. network;
- perform the necessary procedures to revert from fallback operation to normal operation when the failure is cleared by S.W.I.F.T.

2.2 Confidentiality

2.2.1. General

Establish a Non-Disclosure Agreement (NDA) between the User and the Service Bureau

- the NDA contained in the the Service Bureau Participant Agreement will also encompass all SWIFT activity. In addition, no User will know about traffic statistics, authentication and encryption keys, pins, passwords, computer and network configurations, of another User of the Service Bureau.

Unless otherwise indicated, the SLA will be made available to S.W.I.F.T.'s Security Auditors

Establishment and management (modifications/termination) of bilateral authentication key exchange arrangements (pre-agreements) between correspondents is to be performed directly by the Service Bureau. BKE's will be exchanged within 24 hours of receipt of authorization from the User via e-mail.

Restrict access to authentication keys

- these keys will never be disclosed to operators or to non-owners of the keys.

Service Bureau staff will be granted only those privileges that are strictly necessary for the performance of their duties

- this 'least privilege', 'need to know,' or 'need to have' principle applies not only to computerised systems but also to any other written or oral information;
- segregation of duties is the division of responsibilities for actions between at least two individuals;
- in any act or transaction that is susceptible to fraud, major operational impact or other security risk, processes are segregated so that no single individual can act alone.

2.2.2. FIN specific

The Service Bureau will obtain their own SCR directly from S.W.I.F.T.

The Service Bureau will maintain the encryption keys between the SCR and the Service Bureau and the encryption key for storage of the authentication keys

2.3 Integrity

2.3.1. General

Guarantee integrity of traffic stored locally or awaiting processing at all times and under all circumstances

- the Service Bureau is able to provide supporting documentation for all processing, so that any transaction processed can be traced back to instructions originating from a User as per time periods documented in the Service Bureau Participant Agreement.

Formal procedures will ensure that all User messages are processed accurately and timely

This includes formal reporting to the User of all S.W.I.F.T.-related system activity obtained via S.W.I.F.T. reporting features so that:

- the sending User can verify that all messages sent are acknowledged by S.W.I.F.T
- the sending User can respond appropriately to abnormal circumstances such as negative acknowledgements.
- the sending and receiving Users can verify the proper management of system acknowledgements

2.3.2. FIN specific

USE Security Officer (USOF) functions will be maintained directly under the control of the Service Bureau
USE Key Management Officer (UKMO) functions will be maintained directly under the control of the Service Bureau

The Service Bureau will inform Users of the request for a Certificate and the blacklisting of a Certificate or SCR within 24 hours

- authentication keys must be renewed and activated according to formal, current procedures provided to the Service Bureau by the User;
- the procedures referred to must agree with the USE pre-agreement forms exchanged between Users.

Procedures are in place to ensure that all User messages are processed accurately, timely, once and only once

2.4 Availability

- the Service Bureau will ensure terminal availability; hence, terminals must be capable of handling peak traffic (incoming and outgoing) to be expected under normal conditions;
- procedures are in place that require both local and off-site data back-up and hardware redundancy where deemed necessary;
- access to sufficient back-up terminal capacity adequate to handle at least the urgent traffic (incoming and outgoing) in the event of failure of the main terminal(s) is in place;
- back-up of the prime terminal link can be provided through a leased line.

Notify Users if normal availability cannot be provided

- S.W.I.F.T. notifications regarding situations in S.W.I.F.T.'s realm of responsibility that could endanger timely delivery, enhanced with Service Bureau messages indicating local processing problems, must be forwarded to the User in due time.
- The User must know about and use the appropriate methods in both normal and abnormal operating conditions. In any determination of liability, consideration will be given to a User's responsibility for checking acknowledgements, delivery of messages and any notifications that another User or any part of the S.W.I.F.T. network is or will be down, and to their responsibility to take appropriate alternative action.

3. Installation, Operation, Training & Support Guidelines

3.1 Central Infrastructure

The Service Bureau will provide and maintain the required infrastructure

- The Service Bureau shall provide and maintain the required infrastructure to install and operate the central S.W.I.F.T. Interface on behalf of its customers in a secure environment, in line with S.W.I.F.T.'s criteria. This infrastructure will include : site provision, communication lines to customer site, modems, and other required peripheral devices.

3.2 Operations

Coordinate the central S.W.I.F.T. interface

- The Service Bureau will be responsible for the co-ordination of the central S.W.I.F.T. Interface installation and configuration on behalf of its customers.

Carry out daily operations

- The Service Bureau will agree with its S.W.I.F.T. customers on the responsibility and execution of customer-related data and security definitions and maintenance, daily procedures and operations of the central S.W.I.F.T. interface, as well as operations required on a regular basis (backups, reporting, updates, etc.).

3.2 Customer Installation and Training

Provide first-line support

- The Service Bureau will be responsible to provide first-line support to its S.W.I.F.T. customers to allow them to process S.W.I.F.T. transactions in a way that is in line with the responsibilities and liabilities that S.W.I.F.T. imposes on all its customers. This support typically includes minimum guarantees regarding :
 - ongoing customer training regarding interface changes & updates
 - provision of expert resource access to support customers' operations during office hours
 - first level contact for technical & operational assistance, problem investigation and analysis, provision of temporary solutions within required timeframe
 - direct liaison with S.W.I.F.T. help desk on behalf of customers for 'connectivity' problems (interface and/or comms).

1. Definition and General Principles

A “Service Bureau” for the purpose of this Policy is a non-S.W.I.F.T. organisation that provides facilities management and/or data processing services to one or more S.W.I.F.T. Users including operation of a S.W.I.F.T. interface for prime connection to the network and/or for disaster recovery.

A “Service Bureau” may only act on behalf of Users to use S.W.I.F.T. products and services.

A “Service Bureau” may not send or receive messages through the S.W.I.F.T. network for its own account and accordingly is not entitled to a S.W.I.F.T. address.

A “Service Bureau” connection should not diminish the security either of S.W.I.F.T.'s or of a User's systems.

2. Users Responsibilities

A User choosing to be connected via a “Service Bureau” is responsible for:

- a) Ensuring that the security features to access the S.W.I.F.T. system remain under its control so as to restrict access to authorised Users;
- b) Controlling how access to S.W.I.F.T. is managed by the “Service Bureau”;
- c) Ensuring that the “Service Bureau” does not act in a way contrary to that User's obligations and responsibilities towards S.W.I.F.T. and other Users;

- d) Ensuring that the same level of security standards for message confidentiality, integrity and systems availability applicable to it as a S.W.I.F.T. User is maintained by the “Service Bureau” to minimise the potential impact of an operational failure of the “Service Bureau”;
- e) Ensuring that the “Service Bureau” complies with all ownership, operational and security requirements;
- f) Ensuring that the “Service Bureau” complies with all User Handbook obligations incumbent upon Users;
- g) Defining the scope of its “Service Bureau”'s functions and obligations in an agreement with its “Service Bureau”;
- h) Notification of any non-compliance with and breach of the conditions specified in this “Service Bureau” Policy.

Users accept full responsibility for messages sent or received in their name through a “Service Bureau” connection; they recognise that delivery of a message to a S.W.I.F.T. interface operated by their “Service Bureau” is deemed to equate to delivery of that message to them. Users also recognise that they are responsible for any message passing through a S.W.I.F.T. interface at their “Service Bureau” and which thereby purports to emanate from them.

Users connected through the same “Service Bureau” shall be jointly and severally liable in case of breach of any of their above obligations. They agree to indemnify S.W.I.F.T. for any claims for losses or damages resulting from failure to comply with this “Service Bureau” Policy.

Failure to adhere to all obligations mentioned in this Policy may result in revocation of the “Service Bureau” connection to the S.W.I.F.T. network and accordingly result in the User's deactivation.

3. “Service Bureau” General Operational and Security Requirements

- a. A “Service Bureau” may only act on behalf of their User(s) in establishing a connection to S.W.I.F.T. and may not send or receive messages through the S.W.I.F.T. network for their own account.
- b. A “Service Bureau” may not allow non-S.W.I.F.T. Users to connect to or otherwise use a S.W.I.F.T. interface.
- c. A “Service Bureau” may not disclose any information related to S.W.I.F.T. operations, including but not limited to the contents of messages passing through the S.W.I.F.T. system, S.W.I.F.T. technical documentation, S.W.I.F.T. security tokens and S.W.I.F.T. network information, without the prior written consent of S.W.I.F.T. and the User(s) to whom they provide services.

- d. The interface used by a “Service Bureau” to access the S.W.I.F.T. network must be qualified and capable of supporting all features of the respective S.W.I.F.T. service.
- e. All S.W.I.F.T. FIN messages sent from one S.W.I.F.T. User to another S.W.I.F.T. User through a “Service Bureau” must be transmitted over the S.W.I.F.T. network.
- f. A “Service Bureau” may not sub-contract any of their obligations specified in this “Service Bureau” Policy to any third party without prior written consent of their User(s) and S.W.I.F.T.
- g. A “Service Bureau” must sign Service Level Agreements with all S.W.I.F.T. Users to whom they provide services. The Service Level Agreement between the “Service Bureau” and its Users must include the conditions specified herein. In addition, it must contain security arrangements, operations and availability requirements, back-up facilities and disaster recovery mechanisms, based upon the “Service Bureau” Rules and Guidelines document provided by S.W.I.F.T.
- h. A “Service Bureau” must acknowledge that failure to adhere to all obligations mentioned in this Policy may result in revocation of the “Service Bureau” connection to the S.W.I.F.T. network and accordingly result in the User's deactivation.
- i. A “Service Bureau” must annually confirm in writing that it is in compliance with all criteria and conditions specified in the “Service Bureau”x Policy.

4. Specific Rights and Obligations

Considering the above definitions, principles, responsibilities and requirements, the following distinctions shall apply:

4.1 “Service Bureau”x not majority owned and controlled by Users

For “Service Bureau”x not meeting the ownership criteria specified above, National Member Group approval is first required from every country where the “Service Bureau” plans to provide the service, as determined by the country code of the BIC of the User(s) receiving the service.

In addition, the “Service Bureau” application for connection to S.W.I.F.T. shall be submitted to the S.W.I.F.T. Board of Directors for their approval.

Approval by the National Member Group as well as by the S.W.I.F.T. Board of Directors shall be based upon the provision by the “Service Bureau” of genuine services to Users and its adherence to the following additional conditions:

The “Service Bureau” must agree to be audited by S.W.I.F.T. on an annual basis at their own expense to ensure compliance with all criteria and conditions specified in the “Service Bureau” Policy and Service Level Agreement. This Service Level Agreement shall be made available to the S.W.I.F.T. Security Auditors upon request.

4.2 "Service Bureau"x for Disaster Recovery Facilities

Independent of ownership, "Service Bureau"x are permitted to have access to S.W.I.F.T. solely for disaster recovery purposes. A specific agreement between a "Service Bureau" and its User(s) must govern activation of this connection which has to remain under the operational control of S.W.I.F.T.

4.3 Other facilities

Approved "Service Bureau"x will have access to the S.W.I.F.T. products and/or services necessary to ensure the connection of their User(s) to the S.W.I.F.T. network according to this "Service Bureau" Policy.

Admitted "Service Bureau" will thus have the right to:

- a) acquire - on behalf of their User(s) - S.W.I.F.T. products and/or services necessary for the connection to the S.W.I.F.T. network;
- b) call - on behalf of their User(s) - the S.W.I.F.T. Customer Support Centre for support related issues;
- c) use S.W.I.F.T. Vendor Testbed facilities.

"SERVICE BUREAU" POLICY

1. Definition and General Principles

A "Service Bureau" for the purpose of this Policy is a non-S.W.I.F.T. organisation that provides facilities management and/or data processing services to one or more S.W.I.F.T. Users including operation of a S.W.I.F.T. interface for prime connection to the network and/or for disaster recovery.

A "Service Bureau" may only act on behalf of Users to use S.W.I.F.T. products and services.

A "Service Bureau" may not send or receive messages through the S.W.I.F.T. network for its own account and accordingly is not entitled to a S.W.I.F.T. address.

A "Service Bureau" connection should not diminish the security either of S.W.I.F.T.'s or of a User's systems.

2. Users Responsibilities

A User choosing to be connected via a "Service Bureau" is responsible for:

- a) Ensuring that the security features to access the S.W.I.F.T. system remain under its control so as to restrict access to authorised Users;
- b) Controlling how access to S.W.I.F.T. is managed by the "Service Bureau";
- c) Ensuring that the "Service Bureau" does not act in a way contrary to that User's obligations and responsibilities towards S.W.I.F.T. and other Users;
- d) Ensuring that the same level of security standards for message confidentiality, integrity and systems availability applicable to it as a S.W.I.F.T. User is maintained by the "Service Bureau" to minimise the potential impact of an operational failure of the "Service Bureau";
- e) Ensuring that the "Service Bureau" complies with all ownership, operational and security requirements;
- f) Ensuring that the "Service Bureau" complies with all User Handbook obligations incumbent upon Users;
- g) Defining the scope of its "Service Bureau"'s functions and obligations in an agreement with its "Service Bureau";
- h) Notification of any non-compliance with and breach of the conditions specified in this "Service Bureau" Policy.

Users accept full responsibility for messages sent or received in their name through a “Service Bureau” connection; they recognise that delivery of a message to a S.W.I.F.T. interface operated by their “Service Bureau” is deemed to equate to delivery of that message to them. Users also recognise that they are responsible for any message passing through a S.W.I.F.T. interface at their “Service Bureau” and which thereby purports to emanate from them.

Users connected through the same “Service Bureau” shall be jointly and severally liable in case of breach of any of their above obligations. They agree to indemnify S.W.I.F.T. for any claims for losses or damages resulting from failure to comply with this “Service Bureau” Policy.

Failure to adhere to all obligations mentioned in this Policy may result in revocation of the “Service Bureau” connection to the S.W.I.F.T. network and accordingly result in the User's deactivation.

3. “Service Bureau” General Operational and Security Requirements

- a. A “Service Bureau” may only act on behalf of their User(s) in establishing a connection to S.W.I.F.T. and may not send or receive messages through the S.W.I.F.T. network for their own account.
- b. A “Service Bureau” may not allow non-S.W.I.F.T. Users to connect to or otherwise use a S.W.I.F.T. interface.
- c. A “Service Bureau” may not disclose any information related to S.W.I.F.T. operations, including but not limited to the contents of messages passing through the S.W.I.F.T. system, S.W.I.F.T. technical documentation, S.W.I.F.T. security tokens and S.W.I.F.T. network information, without the prior written consent of S.W.I.F.T. and the User(s) to whom they provide services.
- d. The interface used by a “Service Bureau” to access the S.W.I.F.T. network must be qualified and capable of supporting all features of the respective S.W.I.F.T. service.
- e. All S.W.I.F.T. FIN messages sent from one S.W.I.F.T. User to another S.W.I.F.T. User through a “Service Bureau” must be transmitted over the S.W.I.F.T. network.
- f. A “Service Bureau” may not sub-contract any of their obligations specified in this “Service Bureau” Policy to any third party without prior written consent of their User(s) and S.W.I.F.T.
- g. A “Service Bureau” must sign Service Level Agreements with all S.W.I.F.T. Users to whom they provide services. The Service Level Agreement between the “Service Bureau” and its Users must include the conditions specified herein. In addition, it must contain security arrangements, operations and availability requirements, back-up facilities and disaster recovery mechanisms, based upon the “Service Bureau” Rules and Guidelines document provided by S.W.I.F.T.

h. A “Service Bureau” must acknowledge that failure to adhere to all obligations mentioned in this Policy may result in revocation of the “Service Bureau” connection to the S.W.I.F.T. network and accordingly result in the User’s deactivation.

i. A “Service Bureau” must annually confirm in writing that it is in compliance with all criteria and conditions specified in the “Service Bureau”x Policy.

4. Specific Rights and Obligations

Considering the above definitions, principles, responsibilities and requirements, the following distinctions shall apply:

4.1. “Service Bureau”x majority owned and controlled by Users

“Service Bureau”x majority owned (directly or indirectly) and controlled by S.W.I.F.T. Users are permitted by right to connect to S.W.I.F.T.

Prior to the connection, and annually thereafter, the User(s) controlling the “Service Bureau” shall provide S.W.I.F.T. with a certificate confirming the ownership situation.

The User(s) controlling the “Service Bureau” must immediately inform S.W.I.F.T. when its ownership situation changes. Should this mean that the “Service Bureau” is no longer eligible under the above provision, then the conditions listed in 4.2 hereunder shall apply. The “Service Bureau”’s User(s) must ensure compliance with the conditions listed in 4.2. within 90 days from effect of the ownership changes.

4.2. “Service Bureau”x not majority owned and controlled by Users

For “Service Bureau”x not meeting the ownership criteria specified above, National Member Group approval is first required from every country where the “Service Bureau” plans to provide the service, as determined by the country code of the BIC of the User(s) receiving the service.

In addition, the “Service Bureau” application for connection to S.W.I.F.T. shall be submitted to the S.W.I.F.T. Board of Directors for their approval.

Approval by the National Member Group as well as by the S.W.I.F.T. Board of Directors shall be based upon the provision by the “Service Bureau” of genuine services to Users and its adherence to the following additional conditions:

The “Service Bureau” must agree to be audited by S.W.I.F.T. on an annual basis at their own expense to ensure compliance with all criteria and conditions specified in the “Service Bureau” Policy and Service Level Agreement. This Service Level Agreement shall be made available to the S.W.I.F.T. Security Auditors upon request.

4.3. "Service Bureau"x for Disaster Recovery Facilities

Independent of ownership, "Service Bureau"x are permitted to have access to S.W.I.F.T. solely for disaster recovery purposes. A specific agreement between a "Service Bureau" and its User(s) must govern activation of this connection which has to remain under the operational control of S.W.I.F.T.

4.4. Other facilities

Approved "Service Bureau"x will have access to the S.W.I.F.T. products and/or services necessary to ensure the connection of their User(s) to the S.W.I.F.T. network according to this "Service Bureau" Policy.

Admitted "Service Bureau" will thus have the right to:

- a) acquire - on behalf of their User(s) - S.W.I.F.T. products and/or services necessary for the connection to the S.W.I.F.T. network;
- b) call - on behalf of their User(s) - the S.W.I.F.T. Customer Support Centre for support related issues;
- c) use S.W.I.F.T. Vendor Testbed facilities.