SWIFTNet Connectivity

Service Bureau

General Information for Service Bureau

This document provides an overview of how to establish and use a SWIFT Service Bureau.

12 October 2006

Legal Notices

Copyright

Confidentiality

Disclaimer

Translations

Trademarks

Preface

About this document

This document provides an overview of how to establish and use a SWIFT Service Bureau.

This document provides details of the following:

- how to apply the control framework
- the rules and guidelines governing the operation of a Service Bureau

Intended audience

The intended audience includes the following:

- Service Bureaux that want to set up a connection to SWIFTNet
- Users or customers that want to use a Service Bureau to connect to SWIFTNet

Further information

For more information about SWIFT services and products, including Service Bureau applications, do the following:

- For general information about SWIFT services and products, contact your regional SWIFT office (for details, see www.swift.com).
- For specific enquiries regarding Service Bureau applications and status, contact the SWIFT Board Secretariat, at brd.sec.generic@swift.com

Using this document

This document includes hyperlinks to online information. To use them, you need an Internet connection and Acrobat Reader level 4.0 or higher. You can download Acrobat Reader from www.adobe.com.

Acrobat Reader displays web pages and forms within the reader. If you have the full Adobe Acrobat licence, you can use conversion settings to change the way web pages are displayed. For more information about this functionality, see the Help provided with Adobe Acrobat.

Table of Contents

1 Introduction

1.1 What is a SWIFT Service Bureau?

Definition

A Service Bureau is a non-SWIFT User organisation that provides Users with services regarding the day-to-day operation of their SWIFT connection. For example, hosting or operating SWIFT connectivity components, logging on, or managing all sessions or security for SWIFT Users. To avoid any doubt, organisations that only install or maintain interfaces need not register as a Service Bureau.

Therefore, a Service Bureau is entitled to operate various connectivity components (such as a connection to the SWIFT network or interface software) for the benefit of or, as the case may be, on behalf of the Users for their prime or backup connection, or both.

A Service Bureau, however, is not entitled to use any of the following:

- SWIFT messaging services in its own name or for its own benefit
- security features allocated to Users

A Service Bureau is entitled to access and use these on behalf of Users only, except when performing a test in an isolated test-bed environment.

Categories

There are two types of Service Bureau, as follows:

- A Service Bureau Majority Owned and Controlled by Users

  An organisation majority owned (directly or indirectly) and controlled by Users may operate as a Service Bureau within the scope of the *SWIFT Service Bureau Policy*.

- A Service Bureau Not Majority Owned and Controlled by Users

  For an organisation that is not majority owned or controlled by Users, National Member Group advice is first required from the country where the organisation has its operations. Subsequently the request for registration must be submitted to the SWIFT Board of Directors for approval. For more details of this process, see the *SWIFT Service Bureau Policy*.

1.2 Service Bureaux and SWIFT services and products

Overview

Any Service Bureau can order the SWIFT services and products necessary to support and operate the connection of its users to the relevant SWIFT service.

Service Bureaux can connect to the Integration Test Bed (ITB).

No Service Bureau is allowed to send and receive data using SWIFT messaging services for its own account.

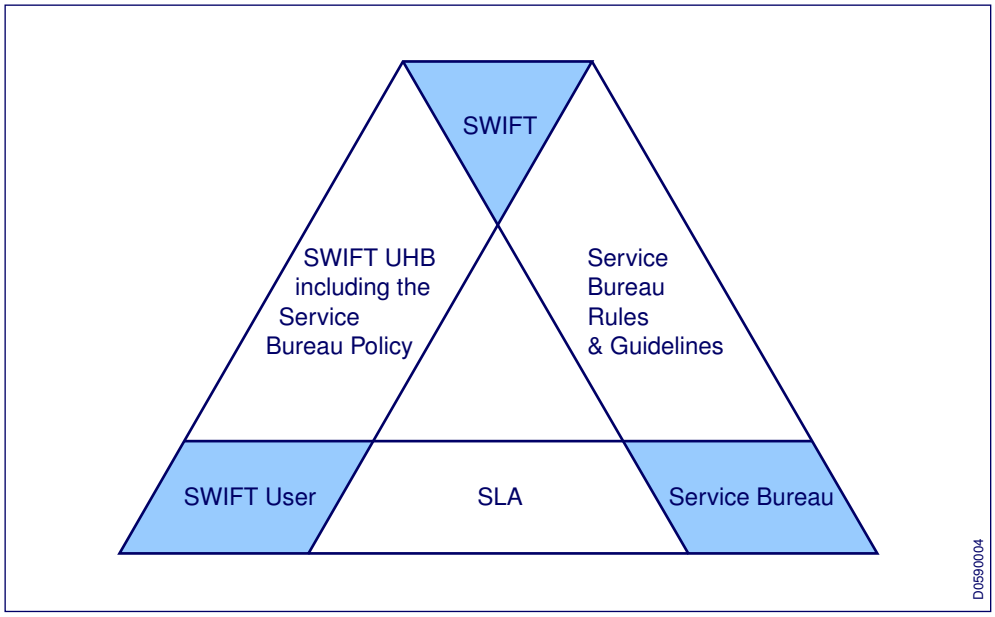
Each Service Bureau is a SWIFT customer, because it can acquire SWIFT products. It is not a SWIFT User, however, because it cannot exchange data with another entity on the SWIFT production network.

Though not directly identifiable on the SWIFT production network, each Service Bureau is allocated a unique 8-character Partner Identifier Code (PIC). The syntax of the PIC resembles a Bank Identifier Code (BIC). PICs have a prefix of SBX and are used to identify each Service Bureau in SWIFT internal systems. For example, when ordering a product, or when acquiring ITB access.

1.3 Service Bureau Governance

Introduction

The following diagram shows the governance structure of each Service Bureau as it relates to SWIFT and SWIFT users:



The key policy documents are as follows:

- **SWIFT UHB**

  The *SWIFT User Handbook* (UHB), which includes the *SWIFT Service Bureau Policy*, governs the relationship between SWIFT and a SWIFT user that uses a Service Bureau.

- **Service Bureau Rules and Guidelines**

  The "Service Bureau Rules and Guidelines" on page 13 govern the relationship between SWIFT and each Service Bureau.

- **SLA**

  A Service Level Agreement (SLA), based on the "Service Bureau Rules and Guidelines" on page 13, governs the relationship between any Service Bureau and a SWIFT user.

2 Service Bureau Application and Control Processes

Introduction

SWIFT has defined a structure in which Service Bureaux and their customers can operate. The structure differentiates between majority-owned Service Bureaux and non-majority-owned Service Bureaux.

Majority-owned Service Bureaux are permitted to connect to SWIFT only after submitting a *Service Bureau Ownership Declaration*, which is available at www.swift.com.

A formal application and approval process is required for each non-majority-owned Service Bureau. It includes approval by the National Member Group (NMG) of the country in which the Service Bureau is to operate, and the ratification of the SWIFT Board of Directors.

Whether majority-owned or non-majority-owned, each Service Bureau is required to comply with the Service Bureau Policy (including the rules and guidelines that govern operations). It is also subject to the annual compliance process.

2.1 Service Bureau Majority Owned by User

Application and approval process

The following application and approval process applies to each majority-owned Service Bureau:

1. The Service Bureau requests the application and the supporting documentation at www.swift.com.
2. The Service Bureau completes the *Service Bureau Ownership Declaration*, identifying each owner of the Service Bureau and each SWIFT user.
3. The SWIFT Board Secretariat provides a notification of the request to the National Member Group or SWIFT User Group in the country in which the Service Bureau operates.
4. The SWIFT Board Secretariat requests ratification from the SWIFT Board and then notifies the Service Bureau of the Board's decision.

2.2 Service Bureau Not Majority Owned by User

Application and approval process

The following application and approval process applies to each non-majority-owned Service Bureau:

1. The Service Bureau requests the application and the supporting documentation at www.swift.com.
2. The Service Bureau completes the *Service Bureau Compliance Declaration*, identifying each SWIFT user, and then sends it to the SWIFT Board Secretariat.
3. The SWIFT Board Secretariat submits the request to the National Member Group or the local SWIFT User Group for approval.
4. The National Member Group or the SWIFT User Group returns its approval to the SWIFT Board Secretariat.

5. The SWIFT Board Secretariat requests ratification from the SWIFT Board and then notifies the Service Bureau of the Board's decision.

2.3 Annual Control and Compliance Procedure

Introduction

In addition to the application and approval process, a yearly control and compliance procedure applies to all Service Bureaux:

1. The SWIFT Board Secretariat requests the following:
   - ownership status
   - a list of users
2. Each non-majority-owned Service Bureau must also submit the following information:
   - confirmation of compliance, together with supporting documentation, written in English
   - a list of users

Important Any change to the information requested by this procedure must be communicated to the SWIFT Board Secretariat at brd.sec.generic@swift.com.

Audit

To support the yearly compliance process, SWIFT reserves the right to submit Service Bureaux to physical audits. SWIFT sends notification of such an audit a maximum of three months in advance. The Service Bureau bears the cost of the audit, including all reasonable travel and related expenses.

SWIFT personnel, or agents approved and authorised by SWIFT, conduct the audits.

The results of the audit are published in a report, which is communicated to the Service Bureau. A copy of the report is also sent to the relevant NMG.

SWIFT reserves the right to communicate the results to the Service Bureau's users.

3 Service Bureau Configurations and Ordering

Introduction

Different Service Bureau configurations are possible.

If your needs meet any of the following criteria, please use one of the specific ordering profiles available at www.swift.com:

- You are interested in establishing a SWIFT-registered Service Bureau.
- You are a new SWIFT User wanting to connect through a Service Bureau.

Otherwise, or for more information, please contact your local SWIFT office or SWIFT Business Partner.

4 Service Bureau Rules and Guidelines

Introduction

The purpose of the Rules and Guidelines is to define the commitments of Service Bureaux towards SWIFT customers, expressed as mandatory rules. They also include good industry practices through the optional guidelines describing recommended extensions of the rules.

It is the responsibility of each Service Bureau and its customers to agree on the terms and conditions of the service to be provided by each Service Bureau. These Rules and Guidelines are designed to help both the Service Bureau and its customers to define appropriate conditions on the quality and security of SWIFT connectivity.

SWIFT strongly recommends that these Rules and Guidelines constitute an integral part of the Service Bureau arrangements with its customers.

The Rules and Guidelines cover the following are categorised as follows:

- **Availability**

  The SWIFT services to which Service Bureau customers subscribe are accessible and usable when needed.

- **Access control**

  Customer data is protected against unauthorised physical and logical access.

- **Integrity**

  Procedures guarantee the completeness and integrity of all data processing by SWIFT.

  Procedures ensure the integrity of all SWIFT services.

- **Change management**

  Procedures ensure all required changes are implemented completely, accurately and timely.

4.1 Availability

Mandatory rules

Rule	Description
Service Level Agreement	Upon request of the customer, the Service Bureau must sign a Service Level Agreement defining measurable availability objectives (such as hours of service, response times, escalation-report times), and associated reporting.
Compliance to SWIFT service availability requirements	The Service Bureau must ensure that each customer can comply with availability requirements applicable to all SWIFT services to which the customer subscribes. These availability requirements are described in the relevant service documentation (typically the policies and service descriptions in the *SWIFT User Handbook*). Adequate reporting on service availability must be available upon customer request. For instance, if the customer subscribes to the FIN service, the Service Bureau must ensure that "Users must take all necessary steps to receive all messages addressed to them and queued during local working hours before the applicable cut-off time" as expressed in the *SWIFT User Handbook*, FIN Policy, Terminal Policy.

Rule	Description
Reliable operations	The Service Bureau must put in place operational procedures to cover disruptions. In particular: • The Service Bureau must implement measures to face foreseeable incidents on the prime infrastructure, including but not limited to air conditioning, fire suppression measures and uninterruptible power supplies (UPSs). • A fallback solution designed to take over a normal level of operations is in place and regularly tested. • Timeframes for the activation of the fallback solution are specified. • Formal monitoring and operational procedures are in place to allow timely activation of the fallback solution, if needed. • In case of a major incident - that is, an incident that prevents a customer from meeting its requirements regarding a SWIFT service - the Service Bureau proactively notifies the customer.
Business Continuity	The Service Bureau must inform the customers of whether a Business Continuity plan, describing disaster-recovery procedures, exists. If such a plan exists, the Service Bureau must communicate to customers any information required to ensure proper execution of that plan.

Optional guidelines

Guideline	Description
Disaster recovery infrastructure	SWIFT recommends that the Service Bureau ensures that its fallback solution remains unaffected by unforeseen incidents on the prime infrastructure. This may involve for instance a disaster recovery site located in a different building.

4.2 Access Control

Mandatory rules

Rule	Description
Authorised personnel	Upon request, the Service Bureau must maintain and communicate to the customer a list of the Service Bureau personnel authorised to operate the infrastructure on behalf of the customer.
Physical security	Physical access to the Service Bureau SWIFT infrastructure, including FIN ICCs, must be restricted to authorised Service Bureau personnel or, when absolutely required, other parties accompanied by authorised personnel. The names of these parties must be communicated upon request to the customers as soon as practicable.

Rule	Description
Network configuration	The Service Bureau must ensure that the network access configuration, up to the customer's premises, complies with all mandatory configuration specification in the *SWIFTNet Network Access Control Guide*.
Logical access	Logical access to the Service Bureau SWIFT interface and underlying operating system must be restricted to authorised Service Bureau or customer personnel referred to in the `Authorised Personnel' rule.
Cryptographic keys	Access to the private PKI keys or bilateral keys must be restricted to Security Officers designated by the customer only. If the Security Officers designated by the customer are Service Bureau personnel, then: • Any disabling, revoking, creation and usage of the private PKI keys and certificates and changes in the user profile defined in the context of Role Based Access Control (RBAC) by the Service Bureau must be performed according to strict procedures agreed between the Service Bureau and the customer, restricted to authorised Service Bureau personnel, recorded in an audit trail, and reported upon request to the customer. • Modification, initiation, and termination of BKE arrangements or other cryptographic secrets by the Service Bureau must be performed according to strict procedures agreed between the Service Bureau and the customer, restricted to authorised Service Bureau personnel, recorded in an audit trail, and reported upon request to the customer.
User data	Access to and modification of a customer's data (such as traffic, message, and configuration data) stored locally (including any backup storage) or during transport on a network must be restricted the customer and to the authorised Service Bureau personnel covered in the Authorised Personnel rule.

Optional guidelines

Guideline	Description
Service Bureau to customer communications	SWIFT strongly recommends that the traffic between the Service Bureau and the customers be authenticated, protected against modification and possibly encrypted.
Segregation of duties in Service Bureau	Depending on the size of the Service Bureau, different groups of Service Bureau Personnel can fulfil different role profiles. Security definitions at application and operating system level must reflect the segregation of duties.

4.3 Integrity

Mandatory rules

Rule	Description
Reports and error alerts	When the customer outsources the monitoring of the SWIFT messaging to the Service Bureau, the Service Bureau must agree with the customer on the processes to handle alerts in case of error and reports on data processing received from SWIFT. Typical examples of alerts / reports would be ACK / NAK messages, non delivery reports, PDE and PDM.

4.4 Change Management

Mandatory rules

Rule	Description
Change management process	The Service Bureau must agree with the customer on the procedures to initiate, approve, plan, track, and implement changes to the SWIFT connectivity infrastructure, including but not limited to mandatory upgrades and migration.
Software upgrades	The Service Bureau must implement Standards releases at least three months before Standards-release change-over, to allow the customers to test in Test and Training mode. The Service Bureau must implement promptly any security patch.

4.5 Governance

Mandatory rules

Rule	Description
Arrangements between Service Bureaux and customers	If the customer requests it, the Service Bureau must explicitly include the present Rules and Guidelines in a binding agreement between the Service Bureau and the customer. The agreement must include liability clauses in case of non-compliance.
SWIFT documentation	It is the responsibility of each Service Bureau to verify that it accesses the latest available version of the Service Documentation made available by SWIFT (whether in paper or electronic format) and to obtain the latest available information relating to the provision and use of the SWIFT services and products by consulting www.swift.com on a regular basis and subscribing to the *SWIFT User Handbook*.
Confirmation statement	The Service Bureau must provide the SWIFT Board secretariat with a yearly confirmation statement regarding its compliance with all mandatory rules described in this document, together with supporting documentation, written in English.

Rule	Description
Audits	The Service Bureau must agree promptly to provide SWIFT with: • written evidence of information reasonably requested by SWIFT relating to the compliance with the present Rules and Guidelines, • access (in person or otherwise) to all relevant locations, so SWIFT can audit the compliance with the present Rules and Guidelines and any written evidence provided pursuant to the foregoing, provided always that SWIFT must at all times comply with the customer's reasonable security policies. The Service Bureau must also make available any facilities, information, assistance, and other services that SWIFT reasonably requires in this regard. SWIFT must charge any such audit to the Service Bureau at the current SWIFT audit rate. The Service Bureau acknowledges and agrees that SWIFT reserves the right to distribute the audit report to the Service Bureau customers upon request.

4.6 Documentation to Support an Audit

Introduction

Each Service Bureau must maintain the following documentation to support audit activity:

- Contracts and agreements
  - the Contract or Non-Disclosure Agreement, or both, between the Service Bureau and its SWIFT users
  - at least one example of a Service Level Agreement (SLA) between each Service Bureau and its users
  - all SLA-reporting information, as provided to the users
- Problem Management
  - an incident procedure with escalation timers between the Service Bureau and its users
  - all operational monitoring procedures that describe the reporting escalation path and actions to be taken in case of a message-processing problem
- Change management
  - details of the change management process
- Hardware and network configuration
  - a hardware and network configuration map, to include details of backup sites and encryption devices
- Environmental controls (specific to the computer room)
  - details of physical security controls
  - details of fire detection and suppression systems
  - details of cooling systems
  - details of power systems (generators, batteries, UPSs)

- Disaster and contingency management
  - a business continuity plan for the Service Bureau
  - contingency procedures for the IT systems and network
  - a contingency plan to support customers if both main and fallback systems simultaneously fail
- Security management
  - SWIFT application user profiles
  - operating system accounts profiles
  - operating system file permission and ownership
  - procedures that describe the user authorisation steps and Service Bureau controls for the management of user secrets and controls, to authenticate the Service Bureau users and to protect transmitted data against modification (integrity checksum/encryption)
  - (for SWIFTNet FIN) a list of User Security Officer (USOF), USER and User Key Management Officer (UKMO) ICC cards managed by the Service Bureau Procedure (or procedures) on ICC cards (USOF, USER, and UKMO) and related card readers (BCR, SCR)
  - System administration
    - identification of the latest releases
    - a list of applied patches

5 Service Bureau Service Level Agreement Guidelines

Introduction

This chapter provides guidelines that form a framework for each Service Bureau when defining Service Level Agreements (SLAs) with its users. The guidelines help Service Bureaux consider and implement various aspects of the *SWIFT Service Bureau Policy* when they create an SLA.

The guidelines provided are generic in nature, because the specifics of each SLA can vary according to the services provided and the Service Bureau involved.

5.1 SLA Principles

Introduction

SLAs are part of contractual agreements between Service Bureaux and their clients that specify the quality and quantity of the service provided by each Service Bureau during a stipulated time period. They also document the responsibilities and expectations of each party.

In other words, an SLA *document* aligns the parties on particular service delivery issues. The SLA *activities* specified are the result of service delivery processes and organisational behaviour. SLAs must, therefore, state objectives that can be *measured* and *monitored*, to ensure they are maintained to agreed levels.

5.2 SLA Sample Framework

Introduction

Each Service Bureau SLA must contain at least a specific section for each of the following topics:

- Scope of service
- Roles and responsibilities
- Service specification
- Service offerings
- Service availability
- Service reporting
- Disaster recovery
- Charges and invoicing
- Legal information.

Details of the information that must be specified for each section follow:

Scope of service

Specifies the overall objective of the agreement.

Roles and responsibilities

Details the roles of the Service Bureau and the SWIFT user. For example, the responsibility for security remains with the SWIFT user, while the Service Bureau performs the security changes (see "Service Bureau Rules and Guidelines" on page 13).

Service specification

In general, the Service Bureau provides connectivity to the SWIFT network and system operations on the interfaces. Services can also include:

Service area	Description
Systems Operations	Access to, and operation of, a data-processing environment for the (Business) applications, including the backup and recovery of those applications.
Backups	Regular application backups.
Recovery	The problem management process covers all hardware and software problems. Data recovery, when required, must be completed in accordance with corporate *Business Continuity Planning* standards.
Infrastructure	Provides connectivity to local and wide-area communication networks.
First Level Application Support	Provides operational support of current application software, such as troubleshooting and correction of processing-related problems.
Consulting	Provides expertise to consult on capacity and infrastructure needs.
Desktop Support	Provides for standard desktop software applications, including the installation and support of workstation hardware and software required to perform the job. Also provides local and remote access to electronic mail and groupware applications.

Service offerings

Details which activities the Service Bureau must provide. For example, for the FIN application a Service Bureau can provide the following:

- Message-queue monitoring (sending or receiving)
- Message-gap analysis (ISN/OSN check)
- Check undelivered-message report (MT082)
- Reconciliation of message Delivery Notification
- Check duplicates, and so on.

Service availability

Defines an availability objective. Generally expresses, as a percentage, the availability of the interfaces or of the client terminal.

Service reporting

Specifies how SLA objectives are met. Regular meetings must be set up to review performance report against SLA objectives.

Disaster recovery

Defines the objectives for disaster recovery and contingency plans.

Charges and invoicing

Defines the cost of using the service and how it must be invoiced. Can also state penalties for not fulfilling an objective of the SLA.

Legal information

Includes nondisclosure clauses and disclosure-agreement clause for SWIFT auditors. The document must be written in English, or a translation must be available.