WAMI (West African Monetary Institute)
Request for proposals – WAMZ Payments System

Document C1
Functional specification for Real Time Gross Settlement System (RTGS)

Sending date :	**3rd of August 2009**
Closing date :	**12th of October 2009**

Date: To be defined

Version: 1.0

Reference: C2. Functional Specifications - RTGS - English version 090730
Confidential

REVISION HISTORY

Version	Date	Author	Description of actions
0.1	15/04/09	To be completed	To be completed
0.2	27/05/09	Logica	Full Review
1.0	03/08/09	Logica	Last draft after review in workshop with WAMi & the Central Banks

VALIDATION

Version	WAMI Sign-Off	LMC Sign-Off
2.0		

COMMUNICATION (FOR VALIDATION)

Name	Date	Validation

WAMI

Table of Contents

1 Introduction

1.1 Objectives of the document

The West African Monetary Institute (WAMI) plans to implement real-time gross settlement systems for high-value funds transfers in The Gambia, Sierra Leone and Guinea Central Banks.

This document contains the specification requirements of these new systems as they will be implemented at go live time. The questionnaire include a list of requirements that MUST or SHOULD or MAY be fulfilled by the proposed solution for further evolution of these systems. They are designed to allow suppliers to submit formal proposals as part of the procurement process.

The contents of this document are as follows:

Section 1: Introduction

Information and guidance. Objectives, current payment systems and scope of the new system.

Section 2: Scope of the Supply

Itemized list of deliverables

Section 3: RTGS General architecture

Section 4: RTGS Functional Requirements

Descriptions of the functional requirements of the proposed solution.

Section 5: RTGS Security specifications

Section 6: RTGS Technical Specifications

Section 7: RTGS Operational Specifications

Section 8: Services

Methodology approach and description of the requested services to be delivered

Section 9 Questionnaire

List of questions as to the proposed solution to be answered by the bidder.

1.2 Business objectives and scope of the system

The West African Monetary Institute (WAMI) is in charge of harmonizing the Payment Systems of the West African Monetary Zone (WAMZ).

The Institute is therefore seeking to put up the Payment Systems in Gambia, Guinea and Sierra Leone to the same level as the two other Member States of the WAMZ, namely, Ghana and Nigeria.

The overall objectives of the Payment System's harmonization are:

- Eliminate, as far as possible, risks from payments, clearing and settlement systems;

- Speed up the exchange and settlement of funds and securities to levels that will effectively eliminate float;

- Improve convenience, services and security for users;

- Bring efficiency to government receipts and payments;

1.2.1 Objectives

The WAMI plans to implement a system for real time settlement of interbank and central bank payments. The new systems will be implemented in each of the three countries' Central Bank (Gambia, Guinea, Sierra Leone), However for the purpose of the document, these will be referred to as the "Central Bank" (CB)

The new system will have the following objectives:

- Reducing settlement risk to the Central Bank and to participants in the payment system by providing real-time gross settlement capability across current accounts at the CB

- Developing a real-time delivery versus payment system to serve as an infrastructure for the government securities market to reduce settlement risks;

- Improving efficiency and service to participants;

- Allowing the integration of future services;

- Conforming to international best practices as set out by the Bank for International Settlements (BIS) and related agencies.

1.2.2 Scope for the System

The scope includes the implementation of a Real Time Gross Settlement System for high value inter-bank payments. Participants will be able to initiate electronic funds transfers to and from their settlement accounts directly.

At the same time, the WAMI will implement a Scripless Securities Settlement System (SSSS) for the transfer and settlement of the CB Certificates of Deposit, Government Bonds, etc. and an ACP/ ACH system (Automatic Cheque Processing/ Automatic Clearing House) in order to automate the activities of the clearing house and to reduce the timeframe of cheque processing

The RTGS system will provide these main services:

- Transfers of funds

- Balance and movement inquiries for settlement accounts

- Intraday liquidity facility via REPO transactions, etc

- Inquiries regarding the position of transfer instructions in the queue mechanism for settlement accounts, including queue management/manipulation instructions such as reordering and cancelling

- Messaging services

- Reporting facilities

- A high level of security for all transactions

- Provision to enable cross border transactions with other regional and international RTGS systems in the future

- Capable to support other currencies in the future.

2 Scope of the supply

2.1 Three turnkey systems

The supplier is expected to deliver three similar turnkey systems installed in Central Bank premises and including participant platforms for each of the commercial banks and financial institutions eligible to participate in the RTGS systems.

2.2 Hardware

2.2.1 Central system servers

See the relevant section in the Technical requirements section of the Term of Reference.

Should the supplier determine that additional servers or machines are necessary to support requirements specific to the RTGS (Websphere MQSeries, PKI, Directory etc.), he is invited to mention explicitly the nature, the specification, the configuration and the numbers of such additional equipment.

2.2.2 Central Banks workstations

The supplier is requested to deliver all necessary workstations for the central bank to run all pieces of software and allow easy organization and smooth system administration and operations.

This is including:

- Administration of system's permanent settings and parameters (participant details and parameters, accounts, user rights, business day calendar and schedule etc…)

- System operation and supervision (system monitoring, participant connection through the private network, business day schedule monitoring, accounts balances, settled orders, rejected orders, queues, gridlock resolution, on-demand statistics and reports etc…)

The supplier will determine the exact number of workstations he thinks adequate to enable the central bank performing normal system's operations and administration activities during the business day and provided that some spare resources remain available to perform non recurrent activities and so that any failure of one or more workstation do not significantly impact operations and supervision activities.

The supplier is expected to justify his proposal and to detail how the different activities are to be organized by the central bank and how roles and responsibilities are to be split between the staff of the payment system department making use of the different pieces of software.

A similar set of workstations is requested for the hot back up site. A third set of workstations may be requested, as an option, for the equipment of the cold back-up site.

In addition to workstations, the supplier has to provide two printers for the use of the Payment Systems Unit of the central bank on both the Main site and the back-up site.

2.2.3 Participant platforms

The supplier is expected to supply for each participant the following hardware components specific to the RTGS participant platforms:

- at least two PC-based workstation one for the use of the participant's operator for payment order creation and one for the use of the participant's treasurer for payment order's validation and submission to the core system

- one machine dedicated to hosting of the local participant's database where payment orders are to be stored (prepared but not yet validated orders, orders sent to the core system, messages received from the core system, permanent data of the system, etc…); the supplier is invited to detail the technical specification of such a machine and how it fits with the general technical requirements.

The number of participant platforms (including the platform for the central bank) that are to be supplied is as follows:

- The Gambia: fifteen (15) participant platforms with an option to increase the number of ordered platforms; final decision will be taken at the time of contract final negotiation,

- Sierra Leone: twenty three (23) participant platforms with an option to increase the number of ordered platforms, final decision will be taken at the time of contract final negotiation,

- Guinea: seventeen (17) participant platforms with an option to increase the number of ordered platforms, final decision will be taken at he time of contract final negotiation.

2.2.4 Security tokens

The supplier is requested to supply the central banks with security tokens for the use of central banks' staffs and participant's staffs (including deputy staff for each position in the targeted organization). There should be a provision for token storing tests certificates for each type of roles, for production certificates for each type of roles and for some spare tokens as well.

The supplier will detail in his offer how he has estimated the number of supplied tokens.

2.3 Software

2.3.1 General purpose and infrastructure software licenses

The supplier has to provide the three central banks with:

- all necessary operating systems software components (for the requested environments, servers, back-ends, front-ends, interfaces, adapters and participant platforms equipment and any additional machine the supplier considers necessary) and including all modules and necessary options,

- Database Management System full licenses for the requested number of users and processing units of all environments of all central banks,

- message oriented middleware (MOM) full licenses for all environments and central banks as the supplier's solution need it,

- Websphere MQSeries software license necessary to implement the interface with the three central banks SWIFT terminals (main and back-up),

- any other software licenses that the supplier considers necessary to customize, to compile, to install, to test, to operate, to administrate, to secure, to analyze, to diagnostic the system so that the central bank will have a full ownership of and control over their turn-key solution.

2.3.2 Application software

The supplier must provide a unique license covering the use of the software package by all three central banks and an unlimited number of participants in the three countries. It must cover the concurrent running of all four different environments in each country (production, hot back up, cold back-up and test).

The suppler is expected to deliver the runtime version of the customized software to be installed in each country on all core system environments.

He has also to provide an unlimited number of copies of all participants' application software components and of central banks' workplace application software components.

He will include in his proposal the detailed full list of software components he considers necessary for the systems to meet the requirements.

2.3.3 Software escrow

To ensure the central bank that, in case of disappearance of the software editor or in case of its inability to deliver the support and maintenance service, the permanence of the solution is preserved, the supplier is requested to escrow the source code of the application software at his expenses by a jointly accepted

Escrow Service Provider. As an option, escrow by the central banks themselves will be considered. In this case the supplier will provide the draft of the escrow agreement he expects to close with the central banks.

The Escrowed material will include:

- the source code of the customized software, (last version of the application software in operation and all updates and correctives that might not be yet in production),

- all software tools necessary to customize, to compile, to test, to install, to configure etc. the application software,

- all necessary documentation and guides (design, analysis etc.).

2.3.4 Security software

The supplier will provide licenses for all environments of all three central banks and all participants of:

- The PKI software solution allowing the generation of private and public keys and the issuance of X509 v3 certificates, their import in security tokens and periodic issuance of revocation lists. These keys and certificates are intended to be used for:

  o Authentication of users and/or software components;

  o Digital signature of messages/transactions;

  o Encryption of transaction details exchanged over the private network;

  o Establishment of SSL sessions for Web enquiries and transactions;

- The directory software (LDAP or Active Directory) for certificates and revocation lists publication;

- All necessary security software modules to interface application software components with tokens and to provide the requested security functions.

2.3.5 Maintenance and support

All of the above software will be covered by a maintenance and support contract with the software editor including the delivery of errors and bugs correction patches and the delivery of new software versions for the period starting with the initial delivery until the end of the warranty period of the turn-key systems.

2.4 Services

As detailed in the services section

3 WAMZ RTGS General Architecture

3.1 RTGS Main Characteristics

The targeted RTGS system to be delivered is designed in accordance with international standards.

3.1.1 Roles of the central banks

The central bank is playing four different roles in the system:

- Manager of the system,

- System administration and supervision,

- System operation,

- Participant.

3.1.2 Participants

The entities eligible for RTGS participation are::

- The Central Bank

- Commercials Banks and eligible Financial Institutions

- Public Treasuries / General Accountants

- Clearing Houses (direct credit/debit, cheques etc.)

- Card switch operators (where existing)

- Stock exchanges and depositaries.

3.1.3 Participation modes

There will be a provision in the system to support four types of participation:

3.1.3.1 Direct Participants:

A Direct Participant holds its own settlement account in the RTGS and has its own technical access to the RTGS. The whole liquidity of the participant is therefore under its own responsibility.

3.1.3.2   *Indirect Participant*

An Indirect Participant holds its own settlement account in the RTGS System but does not have technical access to the System. The technical interfacing is under the responsibility of a Direct Participant under the cover of an indirect participation contract.

3.1.3.3   *Sub-Participant*

A Sub-Participant has no RTGS settlement account. Its liquidity is managed under the technical and financial responsibility of the Direct Participant with whom a sub-participation contract has been concluded.

3.1.3.4   *Technical Participant*

A Technical Participant does not hold any account in RTGS system. It has its own technical access to RTGS to place certain type of orders at pre-defined periods of time within RTGS business days (For instance SSS, ACP/ACH, Card switch systems…)

3.1.4   Accounts

3.1.4.1   *Settlement accounts and Sub- accounts*

RTGS participants will have one main settlement account in the RTGS system. This will be the Settlement Account over which all payments are settled.

All the settlements affecting participant accounts must be exclusively processed in the RTGS.

For the processing of fiduciary operations (deposits/ withdrawals) and specifically in the case of withdrawal operations, participants will hold one sub-account. Liquidity must be reserved (blocked) in advance on this sub-account prior to withdrawals of cash at central bank cashier's desk.

Moreover, it must be possible to open sub-accounts of the main settlement account of a direct participant for each of its sub-participants.

3.1.4.2   *Limits*

The proposed system must provide a facility for an overdraft limit on settlement accounts. At system go live, this debit cap will not be activated (debit cap nil except for the central bank settlement account which has an unlimited overdraft). The debit cap must be adjustable for each participant.

There will be no minimum limit on the value of transfer instructions to be processed in the system; the Central Bank wishes, however, to retain the option to impose such a limit for any transfer orders submitted

to the system in the future. The maximum amount value supported in the system should meet the SWIFT standards, which are 14 digits before the decimal point.

3.1.4.3 RTGS and General Ledger

To each settlement account opened in RTGS, Central Bank General Ledger hold a corresponding current account. This current account opened in the Central Bank books is the legal reference between the participants and the Central Bank.

On day 1, RTGS settlement accounts will be initialized with the actual balance of current accounts held in G/L.

During the RTGS business day, no transaction can be passed on G/L current account which cannot be updated. All payment transactions affecting the current account of participants must be made through RTGS.

At the end of the RTGS business day, updated balances and details of credit and debit transactions settled in RTGS are passed to G/L through the core banking application of the central bank for processing on current account and reconciliation.

On the next business day, RTGS upload from the G/L the updated current account balances.

Before RTGS settlement's opening, there will be a comparison between the uploaded participants' current account balances in G/L (business Day D) and the balance of settlement account recorded in the RTGS at closing in business day D-1.

Therefore, the RTGS system must allow authorized users to correct existing gaps in the settlement account without re-impacting the participants account balances. (In order to avoid duplicating accounting data)

3.1.5 Currency

All payments must be processed in the local Central Bank currency.

However, in order to provision the introduction of the ECO, the future unique currency of the WAMZ region, the system must be able to support multi-currency. The currency code should be provided in the message content of the payment instruction.

3.1.6 Value date

The system must accept exclusively current value date transfer instructions for processing. Current value date transfer instructions that fail to be settled by the end of the day will be cancelled.

However the system must provide as future requirement the possibility to accept future value-dated orders and to roll-over transactions unsettled by the need of the business day).

3.1.7 Settlement main rules

The RTGS System is a funds transfer system for use by participant banks in which payment orders are processed one by one in real time. The system provides for immediate settlement of all payments provided that there are enough funds or overdraft facilities for participants. The Central Bank acts as the settlement agent.

All transactions settled through the system are final and irrevocable. There will be no provision in the system for the reverse or cancellation of settled transfer instructions.

3.1.8 Languages

All deliverables, project documentation, software and technical documentation, guides, training courses and supports, screens and reports generated by the system must be in English (systems, software and documents delivered in Sierra Leone and The Gambia) and French (system, software and documents delivered in Guinea).

3.1.9 Multi-country capability

There should be a capability for the proposed system to enable a participant in the RTGS of one country to place a payment order to the benefit of a participant in the RTGS of another country of the WAMZ. This capability will not be activated in the initial implementation of the RTGS.

3.2 General Architecture

The RTGS system connects all participant bank platforms and the central system at the Central Bank. Two separate telecom infrastructure for transporting instructions, notification messages and enquiries are envisaged: the use of the Swift network and the use of a private interbank network. An option could consist at system go live in using Swift as the main network and the private network to be built as the back-up.

WAMZ's RTGS ARCHITECTURE
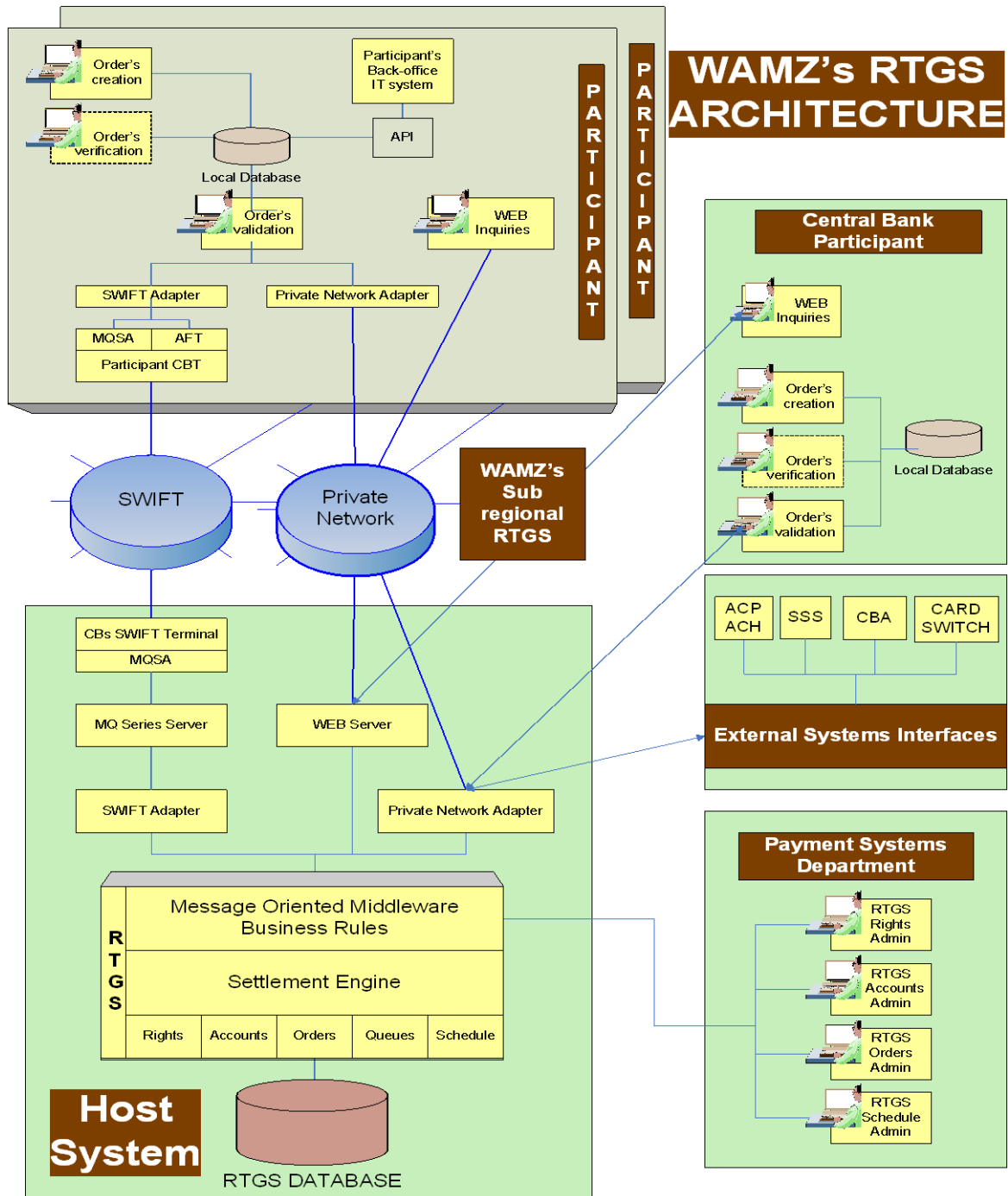
All links between entities in the above scheme allow exchange of messages and information flows in both ways.

3.3 RTGS Main Components

3.3.1 Central system

There must be a provision for four different RTGS environments: one main production environment, one hot back-up system, one cold back-up system and one test system for participant integration and software qualification. All environments are to be located at the Central Bank in three different sites.

3.3.1.1 Roles:

The Central systems must allow:

- Secured exchanges and controls of messages and transactions between participants platforms and core system

- Management of participants and user rights

- Monitoring of the business day operations

- Secured settlement of transactions submitted by participants according to parameterized business rules

- Secured management of settlement accounts and liquidity according to parameterized business rules

- Management of queues, priorities and FIFO rules, gridlock resolution mechanisms

- Appropriate periodical reporting (daily, weekly, monthly, on-demand)

- Secure archiving and auditing of all transactions

- Accurate invoicing of RTGS services to the participant

- Interface with external systems (ACP/ACH, SSS, other net systems, CB Core banking applications etc.)

- Interface with Central Banks G/L through the Core Banking Application

3.3.2 Participants platforms

3.3.2.1 Roles:

The participants' platforms must allow:

- Preparation, control, validation, securing and routing of messages sent to RTGS,

- Optionally reception of messages prepared by participant IT system

- Reception, edition, display and optionally rerouting to IT system of messages received from RTGS

- Reception, editing, printing of reports generated by RTGS

- Monitoring of participant position in RTGS through a secured Web type application

- Production of participant statistics

- Secured storage and archiving of all messages and transactions

- Audit

3.3.2.2 *Architecture:*

The supplier is required to propose three different components for the participants:

1. A dedicated stand alone participant platform allowing the participant to create, control, validate and send payment orders to the core RTGS and to receive messages and notification from it either through the Swift network or through the interbank private network in project. A 4-eyes principle must be implemented for payment orders preparation, controls and validation.

   As a result two different workplaces are requested for these activities, one for the creation and optionally verification of the payment orders and one for the validation and sending to the core RTGS of these payment orders. This later workplace is expected to be placed under the responsibility of the commercial bank's treasurer who manages the bank liquidity and takes the decision to present the payment orders to the settlement.

   All payment orders at any stage should be securely stored in the participant repository. All messages and notifications received from the core should also be stored securely in that database.

   The supplier will detail the proposed architecture of his solution, how it supports the required 4-eyes principle process and how message preparation/verification and validation workflow can be set up and secured.

   The supplier will provide the necessary software adapters allowing exchanging payment messages with the core system either through the Swift network or through the private interbank network in construction.

When the private network is used for transfer of payment instruction, there should be no security downgrade. This means that the proposed solution must include the necessary security mechanisms and software to provide user authentication, message multiple digital signature and data encryption with the same strong level of security as offered by Swift.

Whichever is the network in use, the participant should be able to use Swift messages to request information from the core system (account balance, status of payment orders, queues etc…). The supplier will detail how this requirement is met by its proposed solution.

2. A Web browser based enquiry solution giving access to the full participant information as it is available in the core RTGS. This solution is expected to be used with a connection to the core through the private network.

   The security of the proposed solution should not be weaker than provided through the dedicated platform using Swift messages to reach the same goal (user authentication, encryption of date etc…).

3. In addition to the above components, the supplier is required to provide all necessary APIs and software components allowing the participant to adapt, to integrate and to use its core banking software solution to manage its RTGS participation. Two alternatives are envisaged:

- The core banking system is customized and used only for the preparation of payment orders and their storage in the stand alone participant platform database so that they are made available for validation and sending to the core RTGS by the treasurer through the use of its participant platform workstation,

- A full Straight Through Processing (STP) solution for complete integration of the participant functions in the core banking system of the participant and interconnection through both Swift and the private network. Such a solution must include the integration of the RTGS security mechanisms within the core banking system.

   The supplier is requested to provide a detailed explanation on how the proposed software enables the participant to realize each of the above alternative schemes.

3.3.3 Networks

3.3.3.1 Communication and Payment Network

For each participant, the default communication and payment network will be the SWIFT network for payment orders messages and the private network for Web enquiries (settlement account inquiries, queue inquiries and payment orders inquiries etc.).

The proposed solution will also allow the use of Swift FIN messages for performing all type of inquiries through the Swift network in case of failure of the private network.

Similarly, each participant must be able to use the Private Network for sending and receiving payment orders messages in case of unavailability of the Swift infrastructure. The proposed solution must include all necessary security mechanism to ensure the central banks that the transactions performed over the private network will at least benefits of the level of security provided by the SWIFT network.

The type of network in use must be a parameter associated individually to each participant and it must be possible for the central bank to change the value of this parameter in real-time for any participant at any time during the RTGS business day without having to interrupt operations and without any kind of impact on the other participants.

The proposed solution must allow interconnection of the core RTGS with the Central Bank Swift Access Alliance terminal through an MQSA interface. On participant side, the interconnection of the stand alone platform with the participant Swift Access Alliance terminal should be using either an AFT or an MQSA interface.

3.3.3.2 *S.W.I.F.T. V-Shape Message*

For the initial implementation, the central bank has made the decision to use the Swift V-Shape topology.

Therefore, the proposed system must be able to support the following S.W.I.F.T. payment messages flow using that V-Shape topology:

The message flow as indicated below is:

(1). Payer Bank sends a payment instruction message via SWIFT to RTGS.

RTGS receives the message and check it before settlement.

(2). the settlement engine of RTGS checks the Payer Bank has sufficient funds to make the payment. If sufficient funds are available, RTGS will settle the instruction and forward the payment message to the Payee Bank with confirmation of settlement.

Otherwise, the instruction will be moved to the queue in RTGS with an optional notification of queuing sent to the Payer Bank.

(3). RTGS sends a notification message to the Payer Bank to advise the settlement result of the payment instruction.
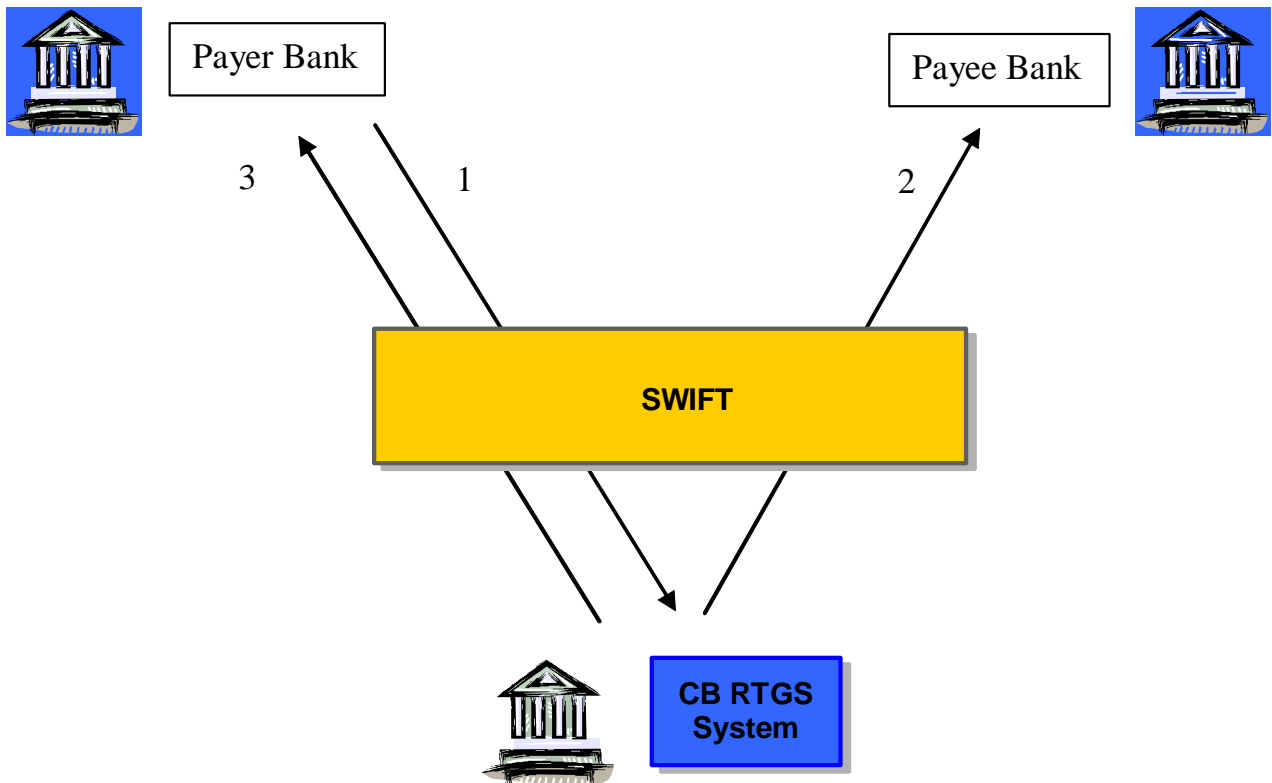
Y-Copy SWIFT messages are considered as optional but the system must provide an option to handle this type of messages.

3.3.4 Interfaces

According to the functionalities and facilities described above, the RTGS core system must be able to interface with the following external components:

- The Core banking application or the General Ledger of the central banks to upload the opening balances of participants' settlement accounts at the beginning of a day, and to download the operations details and closing balances at the end of the day.;

- The ACH (Automated Clearing House) / ACP (Automated Checks Processing) system for the settlement of the net results of the clearing of low value payments;

- Other net systems: for the settlement of the net results of the clearing of card transactions or the clearing of securities transactions;

- SSS: for the support of the settlement of all type of operations relating to securities including DvP processing, intraday liquidity facility (ILF) processing and net settlement as the case may be;

- The central bank Core Banking Applications for the settlement of central bank operations originated in the core banking applications (as the needs may appear at the time of elaboration of the detailed functional specification),

- The Swift Alliance Access terminals of the central banks and their back-up; it is expected that the supplier's solution includes adapters to the MQSA interface in accordance with SWIFT specification and the MQSeries middleware.

As to the participant's platform, it is expected that the supplier's solution comes with the interfaces to Swift Alliance Access terminal with both MQSA and AFT interface.

Should the supplier's solution include additional interface as a standard feature, the supplier is invited to detail them.

The supplier will provide a detailed functional and technical description of each of the proposed interfaces.

4 WAMZ RTGS Functional Specifications

4.1 General Specifications

4.1.1 Business day schedule

Each RTGS business day is to be divided into successive periods dedicated to the processing of specific operations. The business day schedule is parameterized and placed under the relevant central bank staff responsibility.

It is expected that the schedule is prepared in advance and then loaded into the system at start of the day. Central bank staff must have the possibility to make changes in the business day schedule during the business day (changes in period start and end time, cancellation of a period, insertion of an extra period, rearrangement of period orders etc…).

The RTGS should notify participants of the beginning of each period of the current business day.

4.1.2 Messages formats

The message formats should be based on the latest SWIFT common message standards.

For transfer instructions, at a minimum, the system must support SWIFT MT103, MT202, MT203, MT900, MT910, MT940, MT950, MT971, MT999 and MTn98/96. Supplier should advise if there are other SWIFT message types supported in their proposed system.

Each payment settled/rejected must generate a notification to the concerned parties (payee/payer bank).

Each payment queuing should generate a notification to the issuing bank. However the issuance of that notification should be placed under the control of parameters (participant and operation type).

The system must also incorporate a process for securing the messages sent through a non-S.W.I.F.T. interface (multiple digital signatures and encryption).

Each message must include a unique operation number to avoid duplication of message processing. This operation number is left to the responsibility of the message issuing participant.

The system must include a message flow control mechanism designed in such a way that in case of operation disruption, there will be no risk of message duplication or loss after operations resume. This mechanism must be strong enough to support operations restart using a different message exchange network (SWIFT/Private) and/or restart from one of the back-up environment.

4.1.3 Types of operation

The system should provide the possibility for instruction to include types of operation code, identifying the different types of operation. This code should be used when necessary by the central system to process the instruction in a relevant manner. This same type of operation code will be passed with credit/debit details to the General Ledger for accounting purpose.

The supplier may advise if other mechanism is supported to achieve the same results.

4.1.4 Payment orders controls and processing
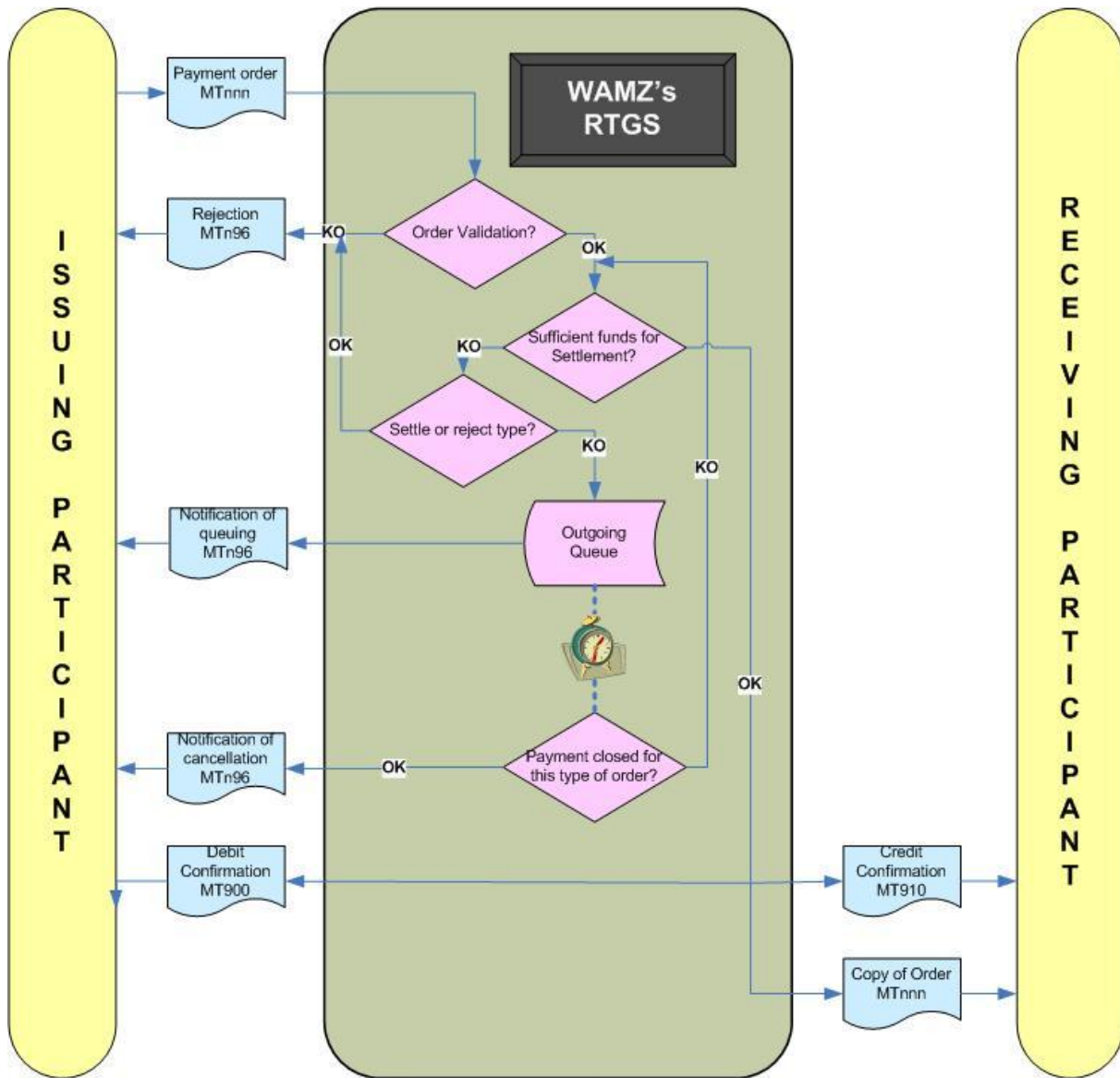
PAYMENT ORDER PROCESSING: GENERIC MESSAGES WORKFLOW

When the system is opened for payment, instructions sent by participants are accepted.

The central system must then check the digital signatures of the payment order.

Order's syntax and the rights of the participant's user to present the selected type of payment order during the current business day period are then checked.

The initial implementation of RTGS is not authorizing presentation of orders for future value dates. However, the proposed solution should provide support of such functionality.

Therefore payment orders with value date different from the current value dates are rejected.

Should any of these controls fail, the payment order must be rejected.

After performing these controls, the central system must check if there are sufficient funds in the settlement account to execute the transaction.

If there are not sufficient funds on the account, the central system will either reject the transaction or send it to a "queue".

The system must allow defining, for each kind of transaction, if they can be queued or if they are to be rejected in case of funds insufficiency.

4.1.5 Queues

The queuing mechanism is the mechanism that keeps instructions received from participants for execution depending on whether there are sufficient funds in the account. The queues will be centrally located at the Central Bank in the RTGS Host Computer.

4.1.5.1 Queue discipline - Priority level

Each type of transaction must be given a degree of priority in the queuing mechanism. The level of priority of a particular instruction is to be chosen within the class of levels associated to the type of operation of that particular instruction.

Operations executed by the Central Bank will be given the highest priority classes, together with the multilateral funds transfers (MFT) orders coming from Net Systems.

Participants will have the possibility to assign different level of priority to their orders; however all of them will be of lower priority than central bank orders and net systems orders. Assigning priorities at payment source is important if banks are to sell timeliness of delivery as a product feature.

Transactions belonging to the same level of priority will be processed according to the FIFO principle.

A new payment order submitted to the system cannot be settled, even when there are sufficient funds to do it, when a payment order with a higher priority is waiting in the queue.

4.1.5.2 *Revocability of queued transfers*

Any queued transfer instruction can be cancelled by the central bank as long as it has not been carried out by an actual settlement in the RTGS system.

Unsettled transactions should remain in the queue until they are either cancelled by participants or revoked automatically at the end of the day.

4.1.5.3 *Queue management by RTGS participant*

The initial implementation of RTGS will not authorize participants to cancel their queued outgoing transfers; this will only be placed under the Central Bank's responsibility.

This functionality must however be placed under the control of system parameters so that in the future the central bank can decide to authorize one, several or all participants to cancel their outgoing queued payment orders.

Participants will be allowed to reorder queued instructions by either moving a transfer to the front of the queue or to the back of the queue. All queue manipulations will generate notification messages back to the sending participant.

They will also have the possibility to change the level of priority of an instruction within the class of levels authorized for the type of operation.

4.1.5.4 *Queue management by the Central Bank*

As part of the responsibilities for the smooth running of RTGS and resolving problems, the authorized Central Bank personnel must have the possibility to both cancel and reorder transfer instructions for all participants (including the Central Bank). All queue manipulations will generate notification messages back to the participant.

4.1.5.5 *Transparency of queued transfers*

Participants can examine their queued outgoing transfers. They cannot examine incoming transfers being sent to them that are held in other banks' outgoing queues. The Central Bank should be able to look at all the queues to facilitate its role as system problem-solver and regulator.

4.1.5.6 *Operating Hours*

The queues will thus start as soon as the system begins to accept transfer instructions.

There will be an adjustable cut-off time when all fund transfers instructions still remaining in the queue will be stopped from processing. After the cut-off time, the system will flush (cancel) all outstanding fund transfer instructions remaining in queues.

4.1.6 Gridlock resolution

A gridlock problem occurs when a batch of transfer instructions cannot be executed due to insufficient funds in the settlement accounts.

As soon as a Gridlock problem occurs, an alert must be sent to the relevant Central Bank administrator. The alerts must be configurable according to number of payments in queue(s)/amount of payment in queue(s), elapse time since last settlement criteria.

The system must provide the possibility to either launch automatically or manually gridlock resolution mechanisms.

The gridlock resolution mechanisms must be possible in accordance to different resolution techniques (By-pass FIFO/ Simulated net balances). The supplier should advise of other gridlock resolution mechanisms permitted by its proposed solution.

The system must also allow simulating the effects of the different resolution modes with optimization of number/amount of settled orders.

There should be an option in the system to automatically perform gridlock resolution before flushing out all outstanding instructions remaining in queues at cut-off time.

4.2 Operations settled in RTGS

4.2.1 Participants operations

4.2.1.1 *Payments issued on their own behalf*

These are Interbank Funds Transfer, i.e. one-sided payments (single credit/debit transfer instructions) made by one bank to another bank on its own behalf. In addition to facilitating funds transfers between participant banks, the system should be able to handle interbank transactions between accounts within participant banks as well as transactions between the Central Bank and participants.

Each payment should be settled individually for the gross amount across settlement accounts at that time if there are sufficient funds in the paying bank's account, otherwise it should be queued. Each settlement should result in:

- A debit to the paying bank's account; and

- A corresponding credit to the receiving bank's account.

The system should immediately send confirmation of successful settlement to the paying bank and the receiving bank without any delay.

4.2.1.2   *Payments issued on behalf of customers*

These are Third Party Funds Transfer, i.e. one-sided payments (single credit transfer instructions) made by a bank on behalf of its customers. The system should be designed to support bank customer to bank customer payments upon request.

Each payment should be settled individually for the gross amount across settlement accounts at that time if there are sufficient funds in the paying bank's account, otherwise it should be queued. Each settlement should result in:

- A debit to the paying bank's account; and

- A corresponding credit to the receiving bank's account in favour of its customer.

The system should send confirmation of successful settlement to the paying bank and the receiving bank.

4.2.1.3   *Payment issued on behalf of sub-participants*

These are payment instructions processed by a Direct Participant on behalf of a Sub- Participant.

Depending on which side of the transaction the Sub-participant stands, each settlement should result in:

- A debit to the Sub-participant sub- account; and

- A corresponding credit to the receiving bank's account.

Or

- A debit to the paying bank's account; and

- A corresponding credit to the Sub-Participant' Sub- account

4.2.2 Central bank operations

Transactions initiated by the Central Bank arise from cash operations (deposits and withdrawals), intraday liquidity facilities, money market payments, mandatory reserves adjustments, foreign exchange trades, government securities trades, payment by government agencies, loans provided by the Central Bank, repayment of loans to the Central Bank, payments of fees, penalties and others.

4.2.2.1   *Payment orders issued on its own behalf*

These are the same as the participant issued transfers on their own behalf. They may, for instance, relate to payment of suppliers invoices, of staff salaries and benefits etc…

4.2.2.2   *Debit orders*

These are one-sided payments (single debit transfer instructions) initiated by the Central Bank. This type of payment is required to support specifically designated debit transfers initiated by the Central Bank.

Each payment should be settled individually for the gross amount across the participant's settlement account at that time if there are sufficient funds in the paying bank's account, otherwise it will be queued. Each settlement will result in:

- ▪ a debit to the paying bank's account; and
- ▪ a credit to the Central Bank's account.

The system should send confirmation of successful settlement to the paying bank and the Central Bank.

4.2.2.3   *Cash withdrawals / Deposits*

These are fiduciary operations made by participants at the cahier's desk of the central bank. This includes both the cashier department at the head office and at the central bank branches wherever they exist.

For withdrawal operations settlement purpose, subaccounts will be opened to each participant settlement account. Participants are requested to beforehand reserve funds on the subaccount. This liquidity transferred from the main account to the subaccount is not available for any other purpose. When the employee of the commercial bank arrives at the cashier desk to withdraw cash, the requested amount of cash is debited from the subaccount of the participant using a special instruction (settled or reject mode). , The maximum amount withdrawn must not exceed the available funds on the dedicated sub-account.

Cash deposits are credited immediately to the settlement account of the participant. Adjustment may be processed later after the cash amount has been verified by the central bank.

These operations are initiated in the new Core Banking Application (CBA) to kick off before the RTGS in the central bank departments.

- Cash deposits are initially processed in the CBA so that the cashier's balance is updated. CBA prepares the payment order which credit the participant account and debit the central bank account. The CBA receives the confirmation of settlement from the RTGS and updates the cashier's balance.

- Cash withdrawals:

  - The treasurer processes the necessary funds reservations in advance in the RTGS. Each reservation transfers funds from the main account to the subaccounts for withdrawal in a defined entity of the central bank (head office or branch). Each confirmation of settlement of reservation orders sent back to the commercial bank treasurer contains the authorization code which will be requested by the central bank cashier at the time of physical withdrawal.

  - The employee of the commercial banks presents to the central bank cashier a withdrawal slip with the list of requested denominations and the authorization code. The cashier enters in CBA a transaction containing the requested amount of cash and the authorization code. CBA generates a payment instruction for RTGS which debit the subaccount of the participant and credit the central bank account. The RTGS core system verifies the validity of the authorization code and the availability of the requested fund. If funds are sufficient on the subaccount, the payment order is settled and the confirmation of settlement is sent to both the participant treasurer and the CBA. CBA notifies the cashier that the funds can be delivered to the commercial banks and updates the cashier's balance.

4.2.2.4   *Intraday Liquidity Facilities*

In order to accommodate intraday liquidity needs in the RTGS system, the Central Bank will be providing an Intraday Liquidity Facility (ILF) against collateral to participants under the following principles:

The ILF funds available to each eligible participant are determined by the amount of collateral it chooses to put for this purpose on their ILF securities sub-account in the Securities Settlement System. Only eligible securities will be accepted for ILF purpose. Central Bank will determine the list of eligible securities.

It is envisaged that central banks will not charge any interest for ILF loans.

At the beginning of each business day, the SSS will look at securities available on the ILF sub-account of each participant and process REPO transactions. The securities will be earmarked and SSS will generate in parallel RTGS instructions in order to provide the intraday liquidity to the participants by crediting automatically their RTGS account and debiting the central bank account.

At any time during the business day, participants have the possibility to transfer securities from their main securities account in SSS to their ILF sub-account. SSS will then process automatically the REPO

transaction and provide the corresponding liquidity by crediting the participant account and debiting the central bank.

RTGS participant will receive notification of each credit.

At the end of the business day, SSS will automatically process buy-back transactions corresponding to each REPO transactions processed within the business day. They results in debit orders posted to the RTGS debiting the settlement account of the participant and crediting the central bank account. A specific period should be defined in the business day schedule for this purpose.

On reception of the notification of settlement sent by the RTGS, SSS will free the securities on the ILF sub-account.

If there are not sufficient funds on the RTGS settlement account of the participant, the order is to be rejected and SSS notified of such situation. The ILF will then be transformed in Overnight facility at penalty rate.

At the beginning of the next business day, SSS will post to the RTGS debit orders corresponding to the payment of the interests with the highest priority level and buy-back transactions will be processed again at the end the day.

There might be a possibility that central bank decides not to grant the overnight loan and to take the ownership of the collateral.

4.2.2.5 *Money Market / Open market operations*

Standard central bank operations including:

- Open Market Operations/ tender processes
- Standing facilities (deposit, loans)

These are one-sided payments (single debit/ credit transfer instructions) initiated by the Central Bank. This type of payment is required to support specifically designated debit/ credit transfers initiated by the Central Bank.

Each payment should be settled individually for the gross amount across the participant's settlement account at that time if there are sufficient funds in the paying bank's account, otherwise it will be queued. Each settlement will result in:

- A debit/credit to the paying bank's account; and
- A credit/debit to the Central Bank's account.

The system should send confirmation of successful settlement to the paying bank and the Central Bank.

4.2.2.6   *Legal mandatory reserves*

There are to be two different schemes implemented in the regard of legal mandatory reserves:

• These reserves are managed through specific accounts managed in the G/L but not in the RTGS. As a consequence, periodic adjustment of the mandatory reserves will results in the central bank relevant department preparing and posting in the RTGS the single sided debit/credit orders that are moving the liquidity from the settlement account of the participant to the settlement account of the central bank; the counterparty will be accounted in the G/L between the central bank account mirroring the central bank settlement account to the legal mandatory reserve accounts of banks.

• The liquidity of the legal mandatory reserves is integrated in the settlement account of the bank so that it is made available for settlement purpose. In this case the average balance of the settlement account over the period must remain at least equal to the requested amount of reserves. It is expected that the RTGS system will be able to calculate periodically the average balance of the settlement account of each participant and help central bank staff to determine whether or not each participant has met its requested level of mandatory reserves. In case one participant has not met the target, penalties are applied by the central bank under the form of a debit order placed in the RTGS.

4.2.2.7   *Foreign Exchange operations*

These are foreign currency exchange operations either between the central bank and a commercial bank or between commercial banks.

The RTGS processes only the leg in central bank money of FOREX operations. The leg in foreign currency is processed with the correspondent bank through usually the use of Swift messages sent to them.

After the negotiation as taken place between the interested parties, the foreign currency buyer is to initiate an instruction in the RTGS transferring the counterparty in central money of the FOREX operations in currency. This will be a simple interbank transfer crediting the foreign currency seller's account and debiting the foreign currency buyer's account.

This instruction may be queued.

Parties are notified of the settlement of the national currency leg of the operation. Then the foreign currency seller will initiate OUT of the RTGS, the transfer of foreign currency through SWIFT.

However, the proposed solution should provide functionalities to support settlement accounts in foreign currency in addition to the settlement accounts in local currency. When this option will be activated, it will

be requested that both legs the FX operations are settled in the RTGS. The supplier will detail how its solution supports a Payment versus Payment settlement process.

4.2.3 Government operations

There will be two possibilities opened to the ministry of Finance of the governments:

- Either they are not participating in the new payment systems as direct participant and will remain "client" of the central bank. In this particular case, their operations will be mixed together with the operations of the other clients of the central bank and of the central bank itself. No specific requirements results then on RTGS since all operations go through the CBA.

- Or the ministry of finance becomes a direct participant of the RTGS. In this particular case, there might be a need to open one or several accounts for this participant to manage its liquidity. This will not encompass the management of the special accounts usually opened in the books of the central bank. These settlement accounts which could be placed under the responsibility of different users of the ministry will be used to centralize the liquidity of the government and make it quicker and easier the payment of the suppliers and salaries, the collection of taxes and the financing operations through the issuance of government bonds and bills. Such a situation may require the government to integrate its IT system together with the RTGS for more efficiency.

The supplier will find additional insights of the respective situation of each country in the inception reports in appendix. At the time of the production of the detailed specification, the supplier is expected to provide assistance to the central banks to analyze the impact on the RTGS of government participation.

4.2.4 DvP operations

It is expected that a real-time DvP facility will be implemented initially for any obligations of the Government, the Central Bank and other public-sector entities in dematerialized, scriptless form.

At present there is no stock market for private-sector corporate securities, though the intention is to establish one in due course. The architecture should take account of this in 2 respects. Firstly, the output from the stock exchange would form part of the net settlement process similar to the process described in the following section. Secondly, the gross settlement on a DvP basis of large stock transactions in the stock market will require a link to be established between the stock exchange and the RTGS system, via the equities central depositary.

At the time of the initial implementation, the system must be able to interface to SSS and support real-time "Delivery versus Payment" (DvP) orders for transfer of government securities. This enables simultaneous settlement of both the payment and the securities part of a transaction.

The RTGS system and SSS must communicate with each other by using messages in standard S.W.I.F.T. format to process DvP of a securities transfer transaction.

The process of securities transfer should take place as follows:

- both buyer and seller of securities input orders into the SSS.

- SSS performs matching and keep the orders for settlement at defined dates.

- on the value date for settlement, the SSS checks availability of securities on the seller's account and earmarks them so that they are not anymore available for any other transaction. Simultaneously, SSS automatically generates a payment order to the RTGS debiting the settlement account of the buyer and crediting the settlement account of the seller of the value of the cash leg of the securities operation.

- RTGS determine if funds are available. If they are available, settlement of payment take place and notification of payment of cash leg of the securities operation is sent to SSS.

- On reception of the notification, SSS processes the transfer of securities from the seller's account to the buyer's account and notifies them. The operation is then completed.

- If liquidity is not available, the payment is queued in RTGS and wait for settlement. When liquidity is available, RTGS settle the order and notifies SSS.

- At the end of the business day, the payment order remaining in the queue will be automatically rejected by RTGS. SSS is notified of the rejection for lack of funds and free the securities on the seller's account. The securities transaction is then rejected.

4.2.5 Settlement of results of Net Systems

These are Multilateral Funds Transfer (MFT) Transactions ie multiple debit and credit transfer instructions allowing the RTGS to settle the clearing positions generated from other external systems.

The instruction should contain only the value of the credit to or debit from each institution in the batch. All other payment details should be cleared between participants outside the RTGS system.

The results of the settlement should be:

- Debit the paying banks' accounts;

- Credit the receiving banks' accounts;

- Confirmation sent to the relevant banks.

MFT transactions will be used to perform settlement of the following payment instructions in the Central Bank:

- cheques after clearing in the ACP/ACH system

- Net direct credit and debit transactions in the ACH system

- Card operations switches (when and where existing)

- Net results of securities transactions in stock exchanges.

As described above, MFT will be given a high level of priority in the queuing mechanism. Nevertheless, during the business day, those operations won't be processed in the same period.

All debits and credits must be processed at the same time. It is expected the MFT instruction to be an MT971 Swift message.

If one (or more) participant does not cover its debiting position, the instruction is queued. Due to its very high level of priority it is blocking the settlement of all other payment orders that may arrive in the system later. At the same time alerts are automatically generated to the failing participant(s), to the RTGS administrator and to the net system administrator. The alert shows the amount of missing funds.

The participant has a limited time to cover its position (up to the end of the dedicated period). He may make use of any of the financing mechanisms that are available (interbank loan, additional ILF, cash deposit etc…).

As soon as the necessary liquidity is made available, the system must settle the queued MFT instruction.

If at the end of the dedicated period the failing participant(s) has not covered its position, the MFT instruction is rejected. Rejection message includes information about failing participant so that the net system may unwire the clearing process.

4.2.6 Messaging facilities

This function is one of the services of RTGS to allow communications between participants and between the participant and the Central Bank during service hours. The Central Bank should be able to send general messages to one receiver or an unlimited number of receivers, including all participants in the system. Each participant should be able to send messages as well.

4.2.7 Inquiries

Inquiries mechanisms are twofold:

- A browser-based application connecting participant to the core system through the private network allows participants to perform the full set of inquiries

- In case of failure of the private network, inquiries should be possible using the treasurer workstation in the participant platform and swift messages through Swift.

4.2.7.1   *Account Balance and Movement Inquiry*

To assist participants in managing their accounts more effectively, the system allows them to gain access to information concerning their settlement accounts at the Central Bank at any time during the service hours of the RTGS system. This includes both settlement accounts' balance and movement inquiry.

The system must provide a full account inquiry capability to all participants for any specific transactions or all transactions in real-time as followings:

4.2.7.2   *Payment Inquiry*

Each account owner should be able to view outgoing, but not incoming queues at any time during the day, rejected and settled payments.

4.3 Systems management

4.3.1 RTGS administration

4.3.1.1   *Administration organization*

The IT Department of the central banks will be responsible of the administration of all technical equipments:

- servers (power on and off machines, control of the hardware, administration of the operating systems administration of the database, of the middleware and of any general use software)

- Setting and administration of all telecommunication networks (LAN, MAN, WAN and active equipments)

IT Department staff is also responsible of database maintenance activities like replication to the back-up sites and back-up operations.

As to the RTGS software, their role is limited to starting the RTGS application software.

The Payment system Unit of the central banks (to be created in some central banks) will be responsible of the administration and the operation of the RTGS.

The payment System Unit managers are responsible for creating and defining rights to system administrators and system operators.

- RTGS Administrators

RTGS Administrators create participant and user profiles and define access rights to users in the Central Bank and participants, who access the RTGS system.

They also create master information data for the system e.g. operating hours, system parameters, holiday table, etc.

- RTGS Operators

They launch the business day operations, monitor the business day schedule progress, supervise the participant connections to the system (private network), manages and traces outstanding messages in queues, oversee the liquidity fluidity, ensure that the participants undertake the necessary financial operations to cover their position, decides to launch the gridlock resolution mechanisms when appropriate, launch the end of day operations and prints daily reports..

To do so the Payment Systems Unit administrators and operators must have at their disposal, client application software running on their workstations. The supplier is requested to describe how its standard solution is architectured and how the above roles and responsibilities will be supported.

The supplier is expected tom make recommendations to the central banks on the organisation to set up in Payment System Units, the optimized repartition of roles and responsibilities between their staff and which software tool should be at the disposal of each staff;

These recommendations should also take into consideration the back-up site.

4.3.1.2 *Permanent Data*

These consist in:

- Participants data and statuses

- Users

- Rights

- Accounts

- Creation / Changes & Updates

- Distribution of permanent data and updates

The supplier will explain how these permanent data are initialized / updated in the system, how their modification is placed under the "4 eyes principle" and how this permanent information is distributed to the participant so that they will always have the last update recorded in their local database.

4.3.1.3 RTGS Calendar and Business Day Schedule

The proposed solution should include the provision of tools to manage:

- Calendar edition, updates and distribution to participants

- Business Day Schedule edition (models)

- Business Day Schedule information broadcast to participants

- Business Day Schedule real-time changes at any time during the business day

The system must be able to create banking holidays as specified by the Central Bank.

- Participants should be informed of banking holidays by the system.

- The system shall prevent any transfer instruction from being entered for a value date which is a banking holiday.

The expected typical Business Day Schedule envisaged is as follows:

7:00 – 7:30	Start of Day: servers control and start up, DBMS launch, network readiness control, application start (IT Department), initialization of business day schedule (Payment System Department)
7:30 – 7:45	Account balances reconciliation with G/L figures
7:45 – 8:00	Central bank operations period: adjustment of account balances, money market operations, CB advances, repayments, interests payments, legal reserves operations, ILF allocation (SSS and CBA application need to be ready) etc.
8:00 – 13:00:	Participants and Central Bank operations period: system is open to participant banks for all types of operations
13:00 – 14:00:	Net systems settlement periods; other types of operations remain open to settlement

14:00 – 17:00	Participants and CB operations remain opened
17:00:	System is closed; participants' orders are rejected; web monitoring remains active for participants' inquiries.
17:00 – 17:15:	System automatically tries to settle as much as possible of the payment orders staying in queues by activating gridlock resolution mechanisms and then automatically tries to refund all ILF granted during the business day (interaction with SSS); if some participant funds are insufficient to allow refund, ILF is transformed in overnight at penalty rate
17:15 – 17:30:	Automatic generation of reports which are sent to participants (MT940 & MT950); CBs reports & statistics are generated, stored (files) & printed. Accounting entries (if not transferred on-line throughout the business day) and final account balances are transferred to the Core Banking Application for reconciliation in the G/L
17:30 – 18:00	RTGS end of operations: operators launch the archiving process. At the end of this last activity, RTGS administrator (Payment Systems Department) informs IT department's administrator that application can be stopped and back-up and other technical maintenance activities can be carried out.

4.3.2 RTGS Operations and Monitoring

4.3.2.1 *RTGS system Start of Day Operations*

- RTGS Starting

As said in section 4.3.1.1 above, IT Department is responsible every morning of the system launch at technical level.

As soon as the IT department has launched the application software, responsibility of operations is handed over to the Payment System Unit RTGS operators.

The RTGS Operator will input the business date for processing which might be different from the operating system date. The software must validate the business date and reconfirm with the RTGS Operator.

- Interface Systems Connection

The interfacing systems include the CBA, SSSS, ACH and other central bank applications. The RTGS operator is responsible to check the connection of these systems with the RTGS in cooperation the operators of the respective systems.

The solution must provide facilities to check the correct connection and diagnostic any possible connection problem.

4.3.2.2   Business Day Schedule Launch

The RTGS operator set the business day schedule of the day.

The system must allow user to adjust the business operating hours for each of the above events (cf 4.3.1.3)

The adjustment by the Central Bank will take place at any time in response to appropriate banking practice in a changing business environment.

4.3.2.3   Settlement accounts balances reconciliation with G/L

RTGS will upload the opening balance of participants' settlement account from the GL System..

Reconciliation with the closing account balances of the previous RTGS Business day is processed automatically and the system should alert the operator of any discrepancies. Accounts department will be informed of that situation and make the necessary inquiries and research to find out the reason of the gap.

The system will anyway start with the RTGS balances of the previous day.

4.3.2.4   Central bank operations

This includes the SSS system which is due to automatically inject the Intraday liquidity facilities in accordance with the collateral lodged by the SSSS participants on their ILF sub-account in SSSS.

When ILF operations are all settled, the RTGS operator will start RTGS operations for all the Central Bank users to login.

This will allow the different departments to present to the settlement the central bank operations of the day.

4.3.2.5   Online Opening

The RTGS Operator will open online operations to allow participant logging in, to receive business day schedule and opening operation information. After participants are successfully online, the system will receive transfer messages and enquiry messages from the participants.

When the Swift network is used to connect participants, online opening results in the acceptance of messages from the central bank's Swift terminal and in the generation of messages to the participants about business day schedule and start of operation.

4.3.2.6   *Participant monitoring*

Messages received from participants are to be monitored in order to trace the status or to solve problems. It should be possible to configure the monitor screen into several windows showing at least::

- the status and details of incoming messages.

- the status and details of outgoing messages.

- the records according to specified conditions e.g. by institution, value date etc.

The system must have the capacity to suspend operations (debit and/or credit) of participants during the business day. In such case the pending payment orders of a suspended participants must be kept on a separate queue until either the end of the business day (when they are rejected) or the un-suspension of the participant (then they are submitted again to the settlement engine).

4.3.2.7   *Payments messages monitoring*

The system must allow monitoring the following payment messages:

- Messages received

- Messages rejected

- Messages queued

- Messages settled

- Messages flows by operation

4.3.2.8   *Accounts monitoring*

The system must allow monitoring of the following account information::

- participant owner of the account

- General Ledger code

- Account status

- Minimum legal reserve balance

- total current balance

- Available current balance

- Subaccounts and reserves denomination and balances

4.3.2.9   Queues monitoring/ Gridlock Resolution

The system must provide queue status, management trace and control commands for transactions in queues which are waiting for execution:

The system must include provision for the RTGS operator to

- Monitor the queues

- Cancel payment orders blocking a queue

- Monitor debit and credit transactions

- Receive alerts relating to lack of funds to settle multilateral net balances of net systems (ACH, Card switch etc.)

- Set Gridlock detection parameters (general and per participant)

- Emulate gridlock resolution performance (bypass FIFO and Net balances) and optimize efficiency (number and amounts of settled orders)

- Activate gridlock resolution mechanism (choice of bypass FIFO or net balances)

4.3.2.10   Participant default processing

Participant default processing requires the RTGS operator:

- to coordinate with the operators of the external systems connected to RTGS

- to report to the payment Systems Unit manager

- to activate the crisis cell meeting

Until a decision (temporary or definitive) is taken by the central bank authorities, he might have the possibility to monitor the transaction of the failing participant or to suspend partially or totally this participant.

The supplier will assist the central banks in defining the detailed procedure of management of such a situation and in creating the crisis cell.

4.3.2.11 *Net systems processing*

The business day schedule includes at least one period dedicated to the settlement of multilateral net balances of a net system. If several net systems need to be settled in the RTGS, several periods will be managed in the schedule.

The system will automatically send messages to the participants to inform them of the beginning of this period. The net system sends the payment instruction to the RTGS.

The RTGS tries to settle the order. It is an "All or None" type of order which means that all debited participants must cover their position to get the order settled. Should any debited participant fail to cover its debiting position, the order will be queued and alerts will be send to:

• The RTGS operator

• The ACH operator

• The failing participant(s)

The message of alert will show explicitly the missing funds of each failing participant(s).

The participants must find the missing liquidity before the end of the period. They can get extra liquidity:

• By transferring additional securities from their SSSS main account to the ILF sub-account which will result in additional ILF automatically granted by the SSSS

• By entering in a REPO interbank transaction with another participant bank. The cash leg of such a transaction will be settled in the RTGS only if the transfer of liquidity does NOT prevent the lending participant to still cover its position in the net system.

• By making a cash deposit at the central bank

• Or by any other type of operation authorised in the country like FOREX operations which could result in crediting its settlement account in local currency.

Normal business practices require the participant to manage their liquidity needs sufficiently in advance so these operations can take place before the special period starts. It is expected that the participants will be informed in advance of their net position in the net system by the net system so that they can undertake in time any appropriate action to cover their positions.

However, when one participant is unable to cover its net debiting position in a net system, at the end of the period dedicated to the settlement of the payment order of this net system, the instruction is rejected.

The operator of the net system is automatically notified by the RTGS.

The RTGS operator start the process detailed in the section above.

When the net system has recalculated the net positions after exclusion of the failing participant, the RTGS operator needs to adjust the business day schedule. He will integrate in the current schedule a new period dedicated for the settlement of the net system. The net system needs to present to the settlement the newly calculated payment instruction.

4.3.2.12 *End of Day Processing*

- Notice to participants prior to the end of RTGS service

The System will send a warning notice to participants when the online operations are about to be closed. However, participants are still allowed to send messages during the warning period of time before the system online period is closed.

- Online Closing

The system stops receiving messages from participants.

- System Closing

The system will check what messages remain in the queue. For unsettled payment messages, the system first tries to perform gridlock resolution so that as few orders as possible remain unsettled. All orders remaining unsettled are rejected. Participants are notified with these rejections so that they are informed that the new orders will have to be prepared on the next business day.

When all standing orders are rejected, a message is sent to the SSSS to trigger the generation of the reverse REPO operations. This will result in SSSS sending payment orders to RTGS for ILF redeeming.

These orders should be of the "Settle or Reject" type so that either the liquidity is available and the transaction is completed or there is a lack of funds and the orders is immediately rejected.

SSSS will then receive notification of the rejection and transform the intraday transaction in Overnight transaction.

- Participant reports

The system will send report messages to all participants and notice all workstations to logout from the RTGS at the closing time. The report messages should adopt the format of SWIFT MT940 and MT950 message types.

- Central bank reports

The RTGS operator will launch the generation of the central bank daily reports and statistics. Reports are in paper form or electronic files.

Reports should print the lists of transfer messages, incoming and outgoing messages, and settlement transactions from or to all participants including the Central Bank.

4.3.2.13 *Reports and Statistics*

- Reports for system administrator

The system must be able to provide the following reports for system administrator:

- Daily payment participant report (including the precise time at which each transaction was input to the system, and the time that it was settled)

- Daily incoming / outgoing transactions report (ditto)

- Daily rejected transactions per participant

- Changes to system queue with respect to priorities, cancellation etc.

- Report on ILF facilities received/redeemed by each participant

- Detailed billing reports

- Queued transactions

- Maximum time in queue for each participant

- Journal log

- Operations log

The reports should also include volumes and values in each of several value bands for each participant and for the system as a whole.

The report data should be available for time periods within each day and for total daily/weekly, etc. traffic. The administrators need to be able to look at a run of figures showing where and when the pressure on liquidity or capacity occurs, so that they can fine-tune the ILF or other aspects of the system.

The system must be designed to capture and prepare reports summarising activity by different transaction types passing through the system, including the following:

- Daily / Monthly / Quarterly / Yearly Payment Transactions

- Daily / Monthly / Quarterly / Yearly Transaction Billing report

- Daily Posting Documents

- Summary of Monthly Transaction Volume by Participants

- Payment Transaction Confirmation

- General Messaging Report

Report/Extracted data must be able to be created:

- In electronic file format (Microsoft Office format for example)

- On hard copy;

- Others i.e. CD ROM

- Reports for Participants

The system must be able to provide the following reports for participants:

- Daily incoming transactions list

- Summary of daily outgoing transactions listed by status

- Daily incoming transfer summary report

- Daily outgoing transfer summary report

- Summary of monthly transactions

- Settled transaction list

- Unsettled transaction list

- Changes to system queue with respect of priorities, cancellation etc.

- Payment transaction confirmation or statement

- System / error log

The participant platform software must be capable of extracting information from the local database containing all relevant details for each participant, so those participants can generate their own reports.

4.3.2.14 *Archiving*

The system must provide a function to backup data from the database on a daily, weekly and monthly basis.

4.3.2.15 *Auditing*

The system will provide an audit trail for all instructions.

All information of previous business days which has not yet been removed from the database should remain accessible by the RTGS operators and by the participants, during the business day, in the same way than the current business day information.

Therefore, the Central Bank and the participants should be provided with an on-line access to a minimum of one year of transactions processed in the system.

4.3.2.16 _Billing_

The system must be capable of capturing and calculating fees charged to participants, based on:

- Participant Fee

The system must provide flexibility for the Central Bank:

- To modify monthly participation fees from time to time;

- To define different fees for different participants.

- Transaction Fee

The transaction fee is based on:

- Number of payment transfer transactions

- Time of day when a payment transfer instruction is received from

- Transaction type

Provision should also be made for the Central Bank to adjust fees per transaction from time to time as transaction volume increases.

5 WAMZ RTGS Security Specifications

5.1 Security overview

5.1.1 Security objectives

As it handles large value payments, RTGS is the most exposed payment system to fraudulent attempts. As such, it requires the highest level of security, including:

- authentication of users (subjects and objects),

- digital signatures of all payment instructions ensuring integrity of information, non repudiation of transactions and trackability,

- confidentiality of information through the encryption of data.

5.1.2 Public key infrastructure (PKI)

The implementation of a Public Key Infrastructure is therefore required in order to meet these overall objectives. This PKI will allow:

- the generation of the root key(s)

- the configuration of certificate profiles

- the generation of digital signature and encryption keys

- the issuance of user certificates

- the import of user certificates into security tokens (USB type)

- the revocation of user certificates

- the renewal of user certificates

- the publication of the user certificate in an LDAP directory (or active directory)

- the publication of revocation lists in the directory

5.1.3 Policies

In order to reach these security objectives and to ensure effective and efficient use of the security technology, the central banks will have to elaborate or update the existing security documentation, procedures and practices.

In this respect, the supplier is expected to assist the central bank and to provide them with the necessary advices and recommendations to put together the following security documents and to implement the relevant practices:

- Central bank security policy

- RTGS certificates policy and profile

- RTGS certificate issuance practices

- RTGS certificate revocation list issuance practices

5.2 Authentication

Authentication is the process that verifies a user's identity. This can be done in many different ways and at different strengths. The central bank has chosen for security reasons to make the requirement that all authentications of users to the system shall be strong.

Strong authentication refers to two-factor authentication, something the user knows (for instance, a PIN code) and something the user has (for instance, an access device or hardware certificate).

It has been determined that the central bank look positively on a system that supports both authentication with an access device and some form of hardware certificate (USB tokens, smart cards, etc.). Regardless of which method is used, it is important that the administration of users and identities can be integrated with the central banks' directory.

Only specific payment systems department administrators will have the right to create new users. Apart from objects, users are individually and namely identified in the system (no generic users). When created, a new user has all his rights set to prevent him to undertake any action or transaction in the system. The next stage consists in assigning specific rights to this new user depending on his role in the system.

Only specific payment systems department administrators will have the right to set/change access rights and privileges. These administrators will have no rights to create new users. In accordance with the four eyes principle, there must be two different roles for rights assignment: one administrator will be authorized to set the rights where another administrator will only have the right to activate the right previously set/changed.

User strong authentication (tokens) is required for user access to RTGS software components and workstations (Central bank administration and operation workplaces and participants' workplaces).

5.3 Securing exchanges and transactions

5.3.1 Preparation of payment orders and digital signatures

All messages must be signed and encrypted using user tokens (keys generated by RTGS PKI) (digital signature in block 4). When different users are involved in the payment orders creation/verification/validation workflow, digital signatures must be applied at each stage and kept in a secured manner in the local database of the participant.

When the payment instruction is generated by the core banking system of the participant bank, it must be signed by the interface between the core banking and the RTGS platform before being stored for validation in the local database. The supplier is requested to provide the necessary APIs and software components to allow such on-the-fly digital signature. Such a digital signature can be produced using a generic user certificate associated to the core banking system. It is the responsibility of the core banking system to provide the necessary functionality to ensure trackability, integrity and non repudiation of the transaction. The central bank will be entitled to verify that the participant's core banking solution provides sufficient security services to meet RTGS security requirements. This will be part of the accreditation process of the integrated solution.

5.3.2 Communication of payment orders

When Swift network is used, Swift security mechanisms will be substituted to RTGS security mechanisms at participant Swift adapter level. However the participant's local database will keep trace of the signatures initially applied to the instruction. The payment orders will be transferred in clear and without digital signature between the central bank Swift Alliance Terminal and the RTGS core system MQSA adapter. For this reason and to ensure the highest possible security on this LAN segment, authentication between software components are strongly recommended.

When Private network is used, RTGS security mechanisms must be used end to end between participant platforms and central systems. This communication channel must be encrypted from the participant software platform to the core system front end. Encryption should be ensured using encryption keys of the signee.

5.3.3 Security operations at core system level

Central RTGS software must check digital signature and certificates validity is checked against revocation list in LDAP.

For Web monitoring, SSL authenticated session using user keys and tokens are required.

Transactions generated through a Web interface must allow the digital signature of the transaction in addition to SSL encryption of exchanges between workstation browser and core system.

Should the digital signature's verification fail or should the certificate's validity verification fail or should the rights associated to the signee be inappropriate, the payment order must be rejected.

5.3.4 Securing the interfaces between RTGS and external systems

The required security level on interfaces is:

- Interfaces between RTGS and external systems submitting payment orders (Core banking application of the central bank, Scriptless Securities Settlement System, other central bank applications etc…) should allow signature and encryption of messages/transactions.

- Interfaces between RTGS and CBA should support authentication using RTGS keys and certificates

- Interface between RTGS core system adapter and Swift terminal requires strong authentication.

6 WAMZ RTGS Technical Specifications

6.1 *Functional architecture*

Re. Technical specifications document

6.2 *Technical architecture*

Re. Technical specifications document

7 WAMZ RTGS Operational Specifications

7.1 Performances

The Core system response time (independently of networks response time) must be less than 2 sec in 99,5% of the cases, less than 5 sec in 99,9% of the cases

The System availability (independently of networks availability) must be 99,9%

Systems architecture should be designed under supplier's responsibility to ensure that no impact (data, message or transaction lost or duplicated) nor extra significant delays or slow-down is incurred on single system component failure.

Hot back-up and cold back-up impacts must be detailed by supplier

Back-up procedures must be delivered and tested by supplier

7.2 Volumes

Rough estimates of the volumes in each country in 2009 are in the range of 1 000 operations per day.

These estimates should be carefully considered as, at the moment, there is no final decision made by WAMI as to the maximum amount of payment instruments authorized to be presented to the future ACP/ACH.

The expected volumes to be supported in the future by systems without upgrades or changes must be 10 (ten) times estimated volumes of year 2009.

The expected volumes to be supported with minor upgrades (disk spaces, memory, network bandwidth, etc.) must be 20 (twenty) times estimated volumes of year 2009.

For storage volumes, the database and disk space should allow storage of at least 18 months of operations without impact on system performance and without need of upgrades.

8 Services

At the time of contract signature, the supplier is expected to deliver a detailed implementation project plan for each of the three national RTGS.

They are expected each to follow the approach detailed below:

8.1 Initial training

The very first activity to be delivered by the supplier consists in training the central banks and WAMI RTGS project teams. This initial training is aiming at providing the staff sufficient knowledge of the supplier's solution. It may include some demonstration of the standard version of the solution but it is not intended to be a full hands-on training. The scope includes both functional and technical aspects of the product.

There should be about 6 to 8 attendees to this training from each country including WAMI.

As a result of the training, the central bank staff must perfectly master the concept, the architecture and the available functionalities of the provider's standard solution so that they can participate efficiently in the detailed specifications design activities.

This training is expected to be delivered offshore in the supplier's premises.

8.2 Detailed system specifications

The production of the detailed specifications is placed under the responsibility of the supplier. The RTGS project team (central bank, WAMI and the consultants) will be assisting them in the production of the following specifications:

- Detailed functional specifications including for each type of operation a fully detailed workflow diagram of the requested exchanges and the detailed messages formats to be used.

- Detailed technical specifications

- Interface specifications with all external systems (ACP/ACH, SSS, Central Bank G/L, Central Bank Core banking etc…)

- Specification of API's made available to participants for integration of the RTGS with their own core banking.

8.3 Change management

The supplier is requested to assist the RTGS project team in the change management.

This includes, for each department/division of the central banks impacted by the implementation of the RTGS and the external systems sending payment orders to the RTGS, the production of the following documentation:

- An analysis of the new workflow of operation in accordance with the detailed functional specifications of the RTGS;

- The detailed operational procedures to be implemented by the central bank (including the definition of supporting documents)

These documents will need to be approved by the central bank step by step. The production of the formal documentation (internal instructions) will remain the responsibility of the central bank; however, the supplier will have to check that these documents are compliant with the reengineered procedures.

8.4 Solution customization

This is an in-house activity which must include unit testing in the provider's lab.

8.5 Installation

This phase is under the responsibility of the supplier who is required to handle all installations at central bank premises of:

- Main, hot back-up and test/cold back-up hardware (servers, workstations and all necessary interconnection and network equipment)

- All software (operating systems, database system, security software, middleware software, application software)

- All necessary settings.

- At least two participant platforms for testing purposes.

Supplier is expected to perform a site inspection before starting this phase.

When installation is completed, the supplier is expected to perform its own on-site tests.

8.6 Hands-on training

This training phase is intended for the central bank staff only: IT staff, RTGS administrator, operators and users. It is intended to be a full hands-on training with the customized version of the solution for an average of 10-12 attendees in each country.

The supplier is expected to deliver a fully detailed training plan including pre-requisites to be fulfilled by the central bank.

As a result of this training, the central bank staff must have acquired a fully detailed knowledge of system functioning, starting, administrating and operating including the participant platform and operations. Therefore they should be ready to perform acceptance testing.

8.7 Acceptance testing

The supplier is expected to deliver a global test plan detailing the suggested test approach and all necessary test cases with the relevant tests tools. The supplier will be assisted to do so by the central banks, WAMI and the consultants.

Acceptance tests will consists in:

- Functional tests covering testing of all types of operations, of central bank administration and operation software, of participant software components. Both private network and Swift network configuration will be covered.

- High availability testing including cluster tests and switching operation from main to back-up sites.

- Performance testing demonstrating the capability of the delivered system to meet the performance criteria

- Integration tests with the external systems (ACP/ACH, SSS, CBA, Core banking etc…)

8.8 Deployment

The supplier will deliver a detailed deployment plan and calendar for this activity. He will advise which assistance and support he may need from the central bank project team.

This phase is aiming at:

- installing at each participant premises the participant platform (hardware and all software),

- configuring the necessary network and software parameters and settings and

- ensuring that all data flows can go both through Swift and the private network as requested.

It is also encompassing the delivery of training to both participants users/trainers and IT staff. Training session must be hands-on training for a minimum of 4 attendees per participant (2 IT and 2 users/trainers). Session might be delivered jointly for different participants' staff in the central bank premises.

It is expected that central bank staff will participate and be progressively involved in the training session delivery to prepare them to assume better their future role of supporting the participants during the operations. Ideally the last session should be delivered by the central bank's staff with the assistance of the supplier's staff.

As a result of this training phase, participant IT staff should be able to install/update/configure and administrate their participant platform. Users should master the sufficient knowledge to be able to administrate their platform and to process all type of operations.

8.9 Pilot phases

The supplier is required to support the central bank team in designing in detail this twofold phase and running it. It needs an on-site permanent assistance.

- The first phase consists in requesting each participant to submit payment orders to the payment systems (all types of operations). The central bank staff is expected to operate the system by his own with the on-site assistance of the supplier's staff. Full business day should be rolled out progressively. This first phase will be considered as completed when central bank and all participants will have demonstrated their ability to process properly all necessary operations and supervision activities

- The second phase consists in a parallel run meaning that, during that phase, central bank and participants will be requested to process twice all of their real operations of the business day:

  - Using the currently existing paper process

  - Using he new RTGS process.

This last phase will last until the central bank and the participant have all reached the necessary level of readiness to go-live. It is expected that, during that phase, operations will be switched from the main site to the back-up site and then switched back so that the Business continuity plan will have been tested at least once with all participants and external systems connected to the RTGS.

8.10 System Go-live

Supplier's staffs are expected to fully check the system before go-live, to assist the central bank staff in preparing the go-live and in configuring and setting the systems.

8.11 On-site assistance

A three month on-site assistance is required to be delivered by the supplier at central bank premises.

During that period, administration and operations of the system will be the responsibility of the central bank but supplier's staffs will be available on-site during the operating hours and advising the central bank staffs.

9 Questionnaire