South African Reserve Bank

National Payment System Department

Position Paper-

Interbank Settlement Network Security Architecture

Position Paper number 02/2008
Date Issued: 2008-05-15

Table of contents

1. Introduction

This document describes the security architecture that applies to the interbank settlement network and should be viewed in the context of the publication: *Interbank Settlement Network*, (Position Paper number: 02/2008), which describes the architectural design of the interbank settlement network component of the interbank settlement system.

Information Paper NPS03 issued by this Office is hereby withdrawn and replaced by Position Paper number: 02/2008.

2. Principles of the SARB-Link Security Architecture

The current SWIFT SARB-Link security architecture is shown in figure 1 of this document while the SAMSec (SAMOS Security) SARB-Link security architecture is shown in figure 2 of this document.

2.1. SWIFT[1] message carrier security

Each participant is responsible for security within its own environment, including the preparation of instructions before their submission to the SWIFT message carrier service.

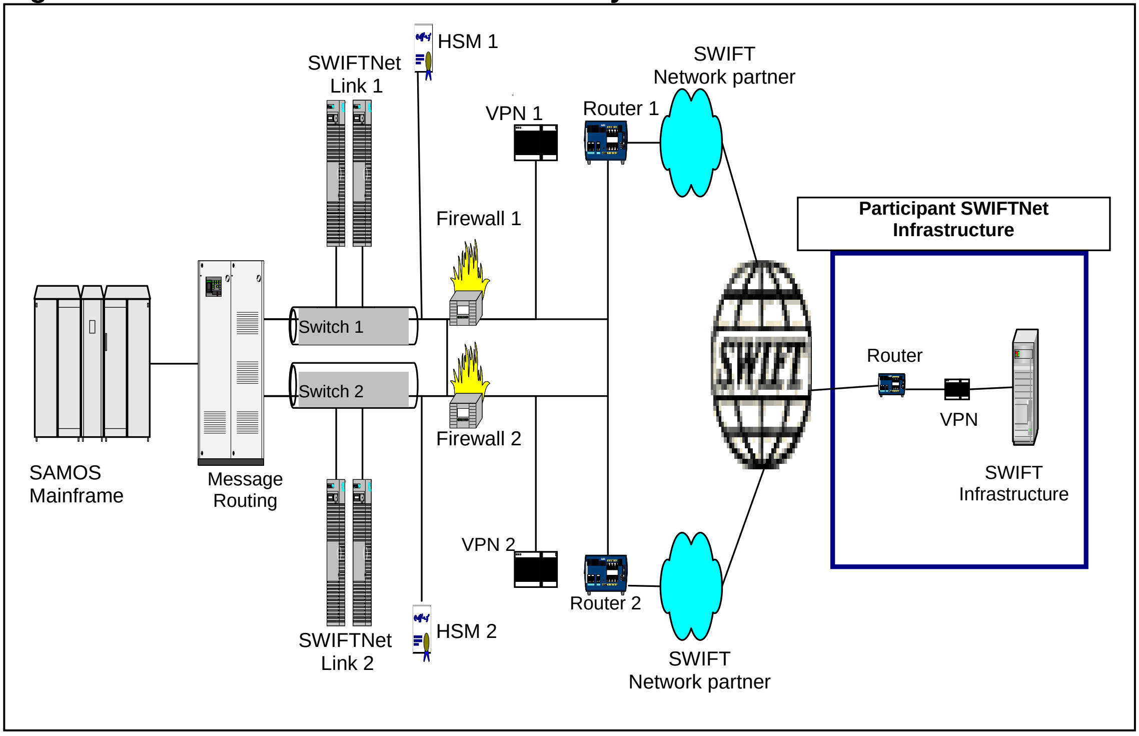
SWIFT has recently implemented a new security solution based on a Public Key Infrastructure (PKI). This security solution makes use of Hardware Security Module (HSM) devices to host participant private keys and is based on best practise regarding security implementations.

SARB-Link SWIFT network security devices which consist of the following can be seen in figure 1:

- Firewalls
- VPN (Virtual Private Network) Devices
- Hardware Security Modules (HSM’s).

[1] SWIFT : Society for Worldwide Interbank Financial Telecommunication

Figure 1: SARBLink SWFIT Network Security Architecture



The standard SWIFT authentication and encryption security measures integrated within the SWIFT service are utilised between SARB-Link and the SWIFT connectivity points making use of the secure network provided by SWIFT network partner. SARB-Link delivers all relevant messages to the SWIFT service based on the routing rules configured on the routing application. SARB-Link assumes no responsibility for the security, protection and delivery of these messages once delivered to the SWIFT service.

2.2. SAMSec message network security

Each participant is responsible for security within its own environment, including the preparation of instructions before their delivery to the SARB via the MQSeries communications Application Programming Interface (API).

The MQSeries based security solution ensures that all messages transmitted by SARB-Link through the direct connection are encrypted before transmission. SARB-Link is responsible for the security, protection and secure delivery of messages through the direct connection, from the participant to the SARB-Link network connection at the SARB as well as messages routed from SAMOS through SARB-Link to the participant.

The security architecture will apply to the MQ Series-based user interfaces, for all messages exchanged between participants and the South African Reserve Bank (SARB) using this proprietary interface.

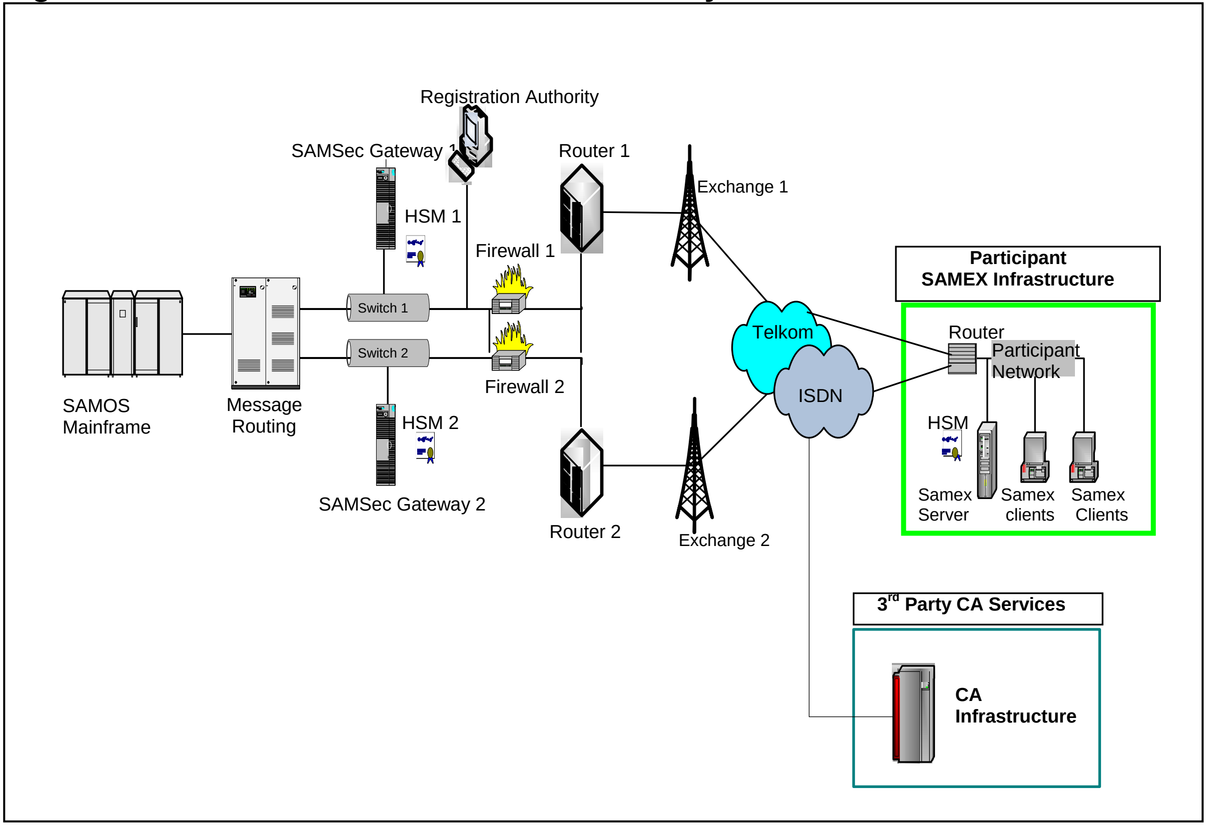
The security implemented on this network is based on the RSA public/private key pairs of 2048 bits in length, and uses encryption protocols and algorithms based on international standards. The Reserve Bank fulfils the role of Certification Authority and manages the certification process in terms of a Certification Practice Statement (CPS). A Trusted Infrastructure Provider has been appointed as the party tasked with providing the infrastructure necessary for the issuing, revocation and management of certificates and public/private keys.

The security system provides the following:

- Authentication of participants.
- Encryption of all messages, in order to ensure confidentiality between sender and receiver.
- Digital signing of all messages, in order to ensure the authenticity and integrity of each message.
- Automated electronic distribution of digital identification certificates to all participants.
- Management of keys over the full life cycle, from issuance to expiry or revocation.

The security is implemented using Hardware Security Modules (HSM). Each bank is required to acquire one HSM for each SAMEX server.
Hybrid security solutions cannot be accepted since they would negate the key management and monitoring functions. Therefore, conformity with the prescribed security requirements is a prerequisite for any participant connecting directly to SARB-Link, for both the Standard user interface and the Information Exchange user interface.

Figure 2: SARB-Link SAMSec Network Security Architecture



2.3. Security implemented in the SAMOS environment

Since the SARB-Link network and SAMOS processors are located next to one another in a secure environment and are connected through a direct physical link, no encryption of messages has been implemented between SARB-Link and SAMOS.

Should this direct connectivity however be changed in the future, an appropriate security solution will be implemented.

Through its normal, auditable security standards, the SARB will ensure the security of messages in the SAMOS application