Sigaba Gateway

FIPS 140-1 Non-Proprietary Security Policy

Level 1 Validation

October 2001
Multi-chip standalone

© Copyright 2001 Proofpoint. Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Table of Contents

TABLE OF CONTENTS **2**

1 INTRODUCTION **3**

1.1 PURPOSE 3
1.2 TERMINOLOGY 3
1.3 DOCUMENT ORGANIZATION 3

2 THE SIGABA GATEWAY **3**

2.1 CRYPTOGRAPHIC MODULE 4
2.2 MODULE INTERFACES 5
2.3 ROLES AND SERVICES 5
2.3.1 Crypto Officer Services *5*
2.3.2 Local Crypto Officer Services *6*
2.3.3 User Services *6*
2.4 PHYSICAL SECURITY 6
2.5 SOFTWARE AND OPERATING SYSTEM SECURITY 6
2.6 CRYPTOGRAPHIC KEY MANAGEMENT 7
2.6.1 Key Generation *7*
2.6.2 Key Storage *7*
2.6.3 Key Zeroization *7*
2.7 CRYPTOGRAPHIC ALGORITHMS 7
2.8 SELF-TESTS 7

3 SECURE OPERATION OF THE SIGABA GATEWAY **8**

4 ACRONYM LIST **8**

1 Introduction

1.1 Purpose

This is a non-proprietary cryptographic module security policy for Proofpoint, Inc's Sigaba Gateway. This security policy describes how the Sigaba Gateway meets the security requirements of FIPS 140-1, and how to operate the Sigaba Gateway in a FIPS 140-1 compliant manner. This policy was prepared as part of the Level 1 FIPS 140-1 validation of the Sigaba Gateway version 3.0.

FIPS 140-1 (Federal Information Processing Standards Publication 140-1 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-1 standard and validation program is available on the NIST website at http://www.nist.gov/cmvp.

1.2 Terminology

Throughout this document the Sigaba Gateway is also referred to as the gateway or the module.

1.3 Document Organization

The Security Policy document is one part of the complete FIPS 140-1 Submission Package. In addition to this document, the complete Submission Package contains:

- Vendor evidence
- Finite state machine
- Source code
- Other supporting documentation

The first section of this document provides an overview and introduction to the Security Policy. Section 2 describes the module, and how it meets FIPS 140-1 requirements.

Corsec Security, Inc. produced this Security Policy and other Certification Submission Documentation under contract to Sigaba Corporation. With the exception of this Non-Proprietary Security Policy, the FIPS 140-1 Certification Submission Documentation is Proofpoint, Inc. proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Proofpoint, Inc.

2 The Sigaba Gateway

In the digital world of today, information systems and their contents are among the most valuable assets that organizations own. Every year organizations spend significant amounts of money to protect data from unauthorized access. Yet everyday, with a click of a button, users email valuable corporate information outside of the firewall and onto untrusted networks.

The vulnerability of email sent across the Internet has become increasingly apparent with the advent of electronic commerce, mobile computing and continuing reports of third party surveillance. This widespread use of the Internet has brought a more populous and sophisticated community of attackers.

Employees usually want to comply with information security policies; however, most existing software tools are difficult to use and often limit with whom the message sender can communicate. For these reasons, many enterprises are now searching for an easy-to-use, end-to-end security solution.

The Sigaba Gateway is a policy-driven email gateway that enables organizations to easily and transparently implement email security. The Sigaba Gateway seamlessly integrates with existing email infrastructures, thereby allowing any current email handling processes such as virus scanning, content filtering and anti-spamming to remain intact. Organizations that deploy the Sigaba Gateway can securely communicate with anyone. Email recipients may be other Sigaba Gateway-enabled enterprises, individual end-users who have the Sigaba email plug-ins, or any party using an HTML-enabled email client. The following diagram shows the role of the Sigaba Gateway in the context of an enterprise.

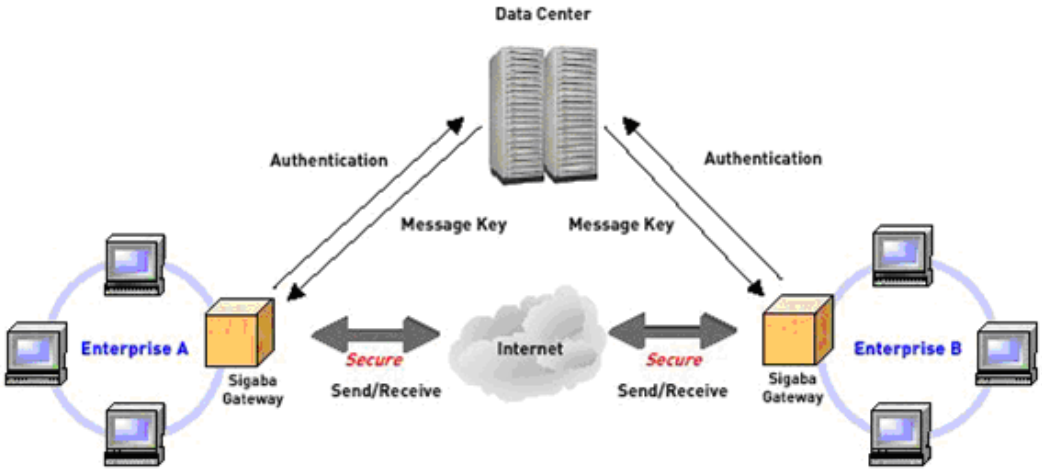

Figure 1 Sigaba Gateway

2.1 Cryptographic Module

The Sigaba Gateway is classified as a multi-chip standalone module for FIPS 140-1 purposes. As such, the module must be evaluated upon a particular operating system and computer platform. The cryptographic boundary thus includes the Sigaba Gateway running upon an IBM compatible Personal Computer (PC) running the Windows™ NT Operating System (OS) when configured in “single user” mode. The Sigaba Gateway running on this platform was validated as meeting all FIPS 140-1 level 1 security requirements, including physical security and operating system requirements.

2.2 Module Interfaces

The physical interfaces of the Sigaba Gateway consist of all the physical interfaces provided on a standard IBM-compatible PC, including a computer keyboard, mouse, screen, floppy drives, CDROM drives, speakers, microphone inputs, serial ports, parallel ports, and power plug. The logical interfaces of the Sigaba Gateway consist of a set of logical network interfaces and Application Programming Interfaces (APIs). The complete list of logical interfaces is as follows:

- Key server interface
- Authentication server interface
- Configuration manager interface
- Email (SMTP) interface
- Log files interface
- Service control manager interface
- Configuration/Policy file interface

The above interfaces are classified in terms of the FIPS 140-1 required logical interfaces as follows:

- Data input – data received via SMTP interface (for both inbound and outbound channels) and data received via communication with the key and authentication servers
- Data output – data output via SMTP interface (for both inbound and outbound channels) and data output via communication with the key and authentication servers
- Control input – data read from configuration files, data input via remote configuration sessions, commands entered via the service API accessed by the OS to start/stop the service
- Status output – data output to log files, status returned as part of ESRP and SMTP sessions

2.3 Roles and Services

The Sigaba Gateway supports three distinct roles: a Crypto Officer role, a Local Crypto Officer role and a User role. As described below, Crypto Officers manage and configure the Sigaba Gateway and Users exercise email services (i.e. sending and receiving secure electronic mail). Although not mandated by FIPS 140-1 at security level 1, the Crypto Officer role requires identity-based authentication.

2.3.1 Crypto Officer Services

Crypto Officers configure and manage the gateway via a remote administration interface. The port associated with remote administration of the module is configurable and is typically accessed via a Configuration Manager utility.

Crypto Officers may perform any action related to the configuration and management of the gateway including: configuring inbound and outbound email channels; defining

encryption/decryption policies; etc. Crypto Officers accessing the module via the remote administration interface must authenticate to the module using a username and password.

2.3.2 Local Crypto Officer Services

Local Crypto Officers configure and manage the gateway by manually editing configuration files or otherwise interacting with the host system. Local Crypto Officers may perform any action related to the configuration and management of the gateway including: starting/stopping the Sigaba Gateway; configuring inbound and outbound email channels; defining encryption/decryption policies; etc.

2.3.3 User Services

Users access gateway services in a transparent manner using SMTP. Depending on the topography of the network in which the gateway is deployed email messages may be sent to the gateway by individual users or by existing SMTP servers relaying messages for a group of users. Users do not need any special software to exercise the functionality provided by the gateway. The following diagram shows a typical deployment scenario with an SMTP server relaying traffic to the Sigaba Gateway.

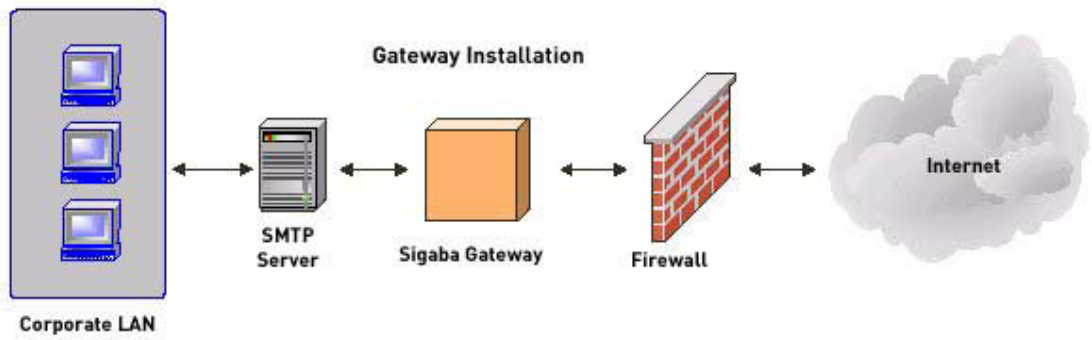

Figure 2 Typical deployment scenario

2.4 Physical Security

The module was tested against FIPS 140-1 requirements on a standard Intel platform Personal Computer (PC) that meets all FIPS 140-1 level 1 physical requirements. This platform provides production grade equipment, industry-standard passivation, and a strong enclosure.

Although the Sigaba Gateway consists entirely of software, the FIPS 140-1 evaluated platform is a standard PC which has been tested for and meets applicable Federal Communication Commission (FCC) Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for business use as defined in Subpart B of FCC Part 15.

2.5 Software and Operating System Security

The Sigaba Gateway is a software module evaluated for use with the Microsoft Windows NT 4 operating system but will operate under Windows 2000, Linux, Solaris and other

UNIX variants. The module consists of a variety of files, including executables, dynamic link libraries, JAR files and configuration files. As explained below, a cryptographic mechanism is used within the module to ensure that the code has not been accidentally or ineptly modified from its evaluated configuration.

2.6 Cryptographic Key Management

The Sigaba Gateway securely administers both cryptographic keys and other critical security parameters such as passwords. This includes a Sigaba Data Center password, an administrator password, ephemeral session keys and message keys. The Gateway stores and transmits passwords in encrypted form. All session keys are ephemeral and are discarded immediately after use. Message keys are electronically distributed in encrypted form. Like session keys, message keys are also discarded after use (although they are stored by the Key Server for later retrieval).

2.6.1 Key Generation

The module does not generate any asymmetric keys. Symmetric key material generated as part of the ESRP protocol relies on a FIPS 186-2 compliant pseudo-random number generator.

2.6.2 Key Storage

The module does not store secret or private key material. Passwords are stored encrypted in configuration files.

2.6.3 Key Zeroization

All ephemeral key data resides in internally allocated data structures that are zeroized by the Java Virtual Machine's (JVM) garbage collector.

2.7 Cryptographic Algorithms

The Sigaba Gateway provides support for the following FIPS approved algorithms:

- Digital Signature Standard (DSS) – FIPS 186-2
- Triple DES – FIPS PUB 46-3
- Secure Hashing Algorithm (SHA-1) – FIPS 180-1

Additionally, support is provided for the following non-FIPS-approved algorithms:

- Advanced Encryption Standard (AES) – Draft FIPS
- Message Digest 5 (MD5) – RFC 1321
- SHA-1 HMAC (Keyed-Hashing for Message Authentication) – RFC 2104

Note: For added security MD5 is used to hash the CO's password during CO authentication. With the exception of MD5, only FIPS-approved algorithms may be used when operating the gateway in a FIPS 140-1 compliant manner.

2.8 Self-Tests

The Sigaba Gateway performs a number of startup and conditional self-tests to ensure proper operation (see Table 1 for a list of all self-tests performed by the module). If the

module fails a self-test it will enter an error state and inhibit all cryptographic functions and data output. Self tests include integrity checks over each binary component at load time, cryptographic algorithm known answer tests (KATs), a bypass test, and other critical startup tests. Additionally, a continuous random number generator tests monitors output from the module's FIPS-approved random number generator, as required by FIPS 140-1.

Test	Type
Bypass test	Conditional Self-Test
Continuous random number generator test	Conditional Self-Test
DSA KAT	Power-up Self-Test
HMAC KAT	Power-up Self-Test
Module integrity check	Power-up Self-Test
SHA-1 KAT	Power-up Self-Test
Triple DES KAT	Power-up Self-Test

Table 1 – Summary of FIPS required self-tests

3 Secure Operation of the Sigaba Gateway

When placed in "FIPS Mode", version 3.0 of the Sigaba Gateway meets all the level 1 requirements for FIPS 140-1. To place the Sigaba Gateway in "FIPS Mode," follow the instructions below.

1. Launch the Configuration Manger
2. Select the Encryption tab
3. Select the "FIPS Gateway Mode" radio button and press the "Apply" button
4. Restart the Sigaba Gateway Service

4 Acronym List

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
DSS	Digital Signature Standard
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESRP	Extended Secure Remote Password
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
HMAC	Hash Message Authentication Code
JAR	Java ARchive
KAT	Known Answer Test
NIST	National Institute of Standards and Technology
OS	Operating System
PC	Personal Computer
SHA1	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
Triple DES	Triple Data Encryption Standard