BISCOM The Leader in Enterprise Document Delivery

Biscom Cryptographic Library Version 1.0 Security Policy

FIPS 140-2 Level 1 Validation

February 25, 2013

Version 1.08

Table of Contents

List of Tables

List of Figures

1 Introduction

This document is the Security Policy for the Biscom Cryptographic Library Version 1.0. This Security Policy specifies the security rules under which the module shall operate to meet the requirements of FIPS 140-2 Level 1. It describes how the module functions to meet the FIPS requirements, and the actions that operators must take to maintain the security of the module.

This Security Policy describes the features and design of the Biscom Cryptographic Library using the terminology contained in the FIPS 140-2 specification. *FIPS 140-2, Security Requirements for Cryptographic Modules* specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. The NIST Cryptographic Module Validation Program (CMVP) validates cryptographic modules to FIPS 140-2 and other cryptography-based standards. Validated modules are accepted by the Federal agencies of both the USA and Canada for the protection of sensitive or designated information.

The FIPS 140-2 standard and information on the CMVP can be found at http://csrc.nist.gov/cryptval.

This Security Policy contains only non-proprietary information. This document may be freely reproduced and distributed whole and intact. All other documentation submitted for FIPS 140-2 conformance testing and validation is “Biscom - Proprietary” and is releasable only under appropriate non-disclosure agreements.

The Biscom Cryptographic Library (the cryptographic module) meets the overall requirements applicable to Level 1 security for FIPS 140-2 as shown in Table 1.

Table 1: Cryptographic Module Security Requirements.

Security Requirements Section	***Level***
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles and Services and Authentication	1
Finite State Machine Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A
Cryptographic Module Security Policy	1

1.1 Document Version History

Version	Date	Comments	Name
1.00	6/6/11	Initial Snapshot	Ward Rosenberry
1.01	6/14/11	Draft 1	Ward Rosenberry
1.02	6/21/11	Draft 2	Ward Rosenberry
1.03	9/21/11	Submission Draft	Ward Rosenberry
1.04	3/21/12	Addressing tester observations	Ward Rosenberry
1.05	5/4/12	Addressing 2md round tester comments	Ward Rosenberry
1.06	12/11/12	Addressing CMVP comments	Ward Rosenberry
1.07	1/12/2013	Addressing CMVP comments	Ward Rosenberry
1.08	2/25/13	Addressing CMVP comments	Ward Rosenberry

1.2 Acronyms and Abbreviations

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CSP	Critical Security Parameter
FIPS	Federal Information Processing Standard
GPC	General Purpose Computer
HMAC	Keyed-Hashing for Message Authentication
KAT	Known Answer Test
NIST	National Institute of Standards and Technology
OS	Operating System
PUB	Publication
RAM	Random Access Memory
RNG	Random Number Generator
SHA	Secure Hash Algorithm

2 Biscom Cryptographic Library

2.1 Functional Overview

The Biscom Cryptographic Library (the *cryptographic module* or the *module*) provides cryptographic security functions as Java APIs for application developers to integrate cryptographic services into Biscom applications or systems. The module is distributed only as an integrated subcomponent of the Biscom Delivery Server (BDS).

The Biscom Cryptographic Library provides security functions for encryption, decryption, random number generation, hashing, getting the status of the integrity test, and running the self-tests. The library is used by the application

2.2 Module Description

The Biscom Cryptographic Library is provided as a jar file running on a Java Virtual Machine (JVM) that, in turn, runs on both Windows and Linux operating systems. In FIPS 140-2 terminology, the Biscom Cryptographic Library is a multi-chip standalone cryptographic module.

The Biscom Cryptographic Library provides the following cryptographic services:

- Encryption and decryption of data
- Generation of hash values
- Generation of random numbers
- Execution of self test and conditional test

The module was tested for validation with FIPS 140-2 using Windows 2008 R2 (SP1) with Sun JRE 6.0 running on a Dell Optiplex 790, however compliance of the module is maintained in accordance with Implementation Guidance G.5 on platforms for which the JAR file remains unchanged. These platforms include (but are not limited to):

- Windows 2003 Server with Sun JRE 5.0 and above
- Windows 2008 Server with Sun JRE 5.0 and above
- Redhat Enterprise Linux 5 with Sun JRE 5.0 and above
- Ubuntu 10.04 LTS with Sun JRE 5.0 and above

The physical boundary includes the additional general-purpose computing platforms on which the operating systems are supported.

The platform is configured in single user mode (multiple concurrent operators are not allowed).

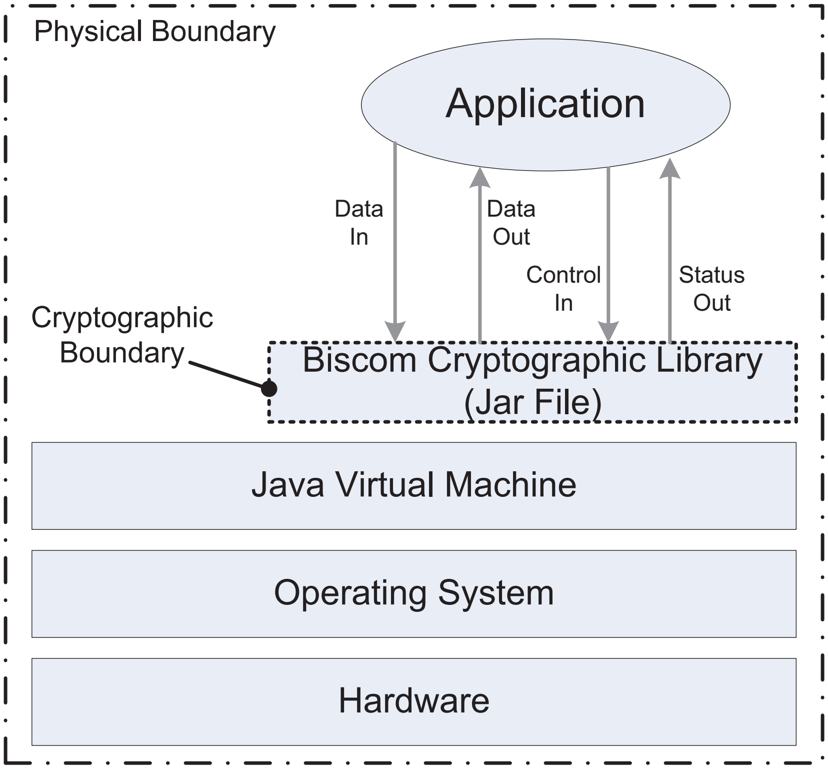
The module does not have a bypass or maintenance mode.

Biscom distributes the module only as an integrated component of an application that ensures it is only accessed in a manner consistent with this document.

2.2.1 Module Block Diagram

Figure 1 shows a module block diagram of the cryptographic module that illustrates the physical and cryptographic boundaries of the module.

Figure 1: Cryptographic Library Module Block Diagram



The cryptographic boundary of the cryptographic module defines the jar file providing the Cryptographic Library. The physical boundary of the cryptographic module is the enclosure of the physical computer on which the cryptographic modules resides and executes. The power input is provided with the hardware.

2.3 Module Ports and Interfaces

The logical interfaces to the Cryptographic Library are the Java classes accessed using the instance() method from a consumer application.

The physical interfaces are the standard I/O ports on a general purpose computer for connecting external devices such as network adapters, monitors, and keyboards. These physical interfaces are outside the boundary of the cryptographic module and are not included in the validation.

The power interface consists of the power supply of the general purpose computer that provides power to run the application containing the cryptographic module.

Table 2 describes each logical interface.

Table 2: FIPS 140-2 Logical Interfaces.

Logical Interface	Description
Data input	Data input consists of ciphertext and plaintext data entering the cryptographic module as input to the java classes from the application using the module. Data is input from end users via the application using the module for the purpose of encryption or decryption.
Data output	Data output consists of ciphertext and plaintext data exiting the cryptographic module and returned to the calling application from the Java classes. Data is output to end users via the application using the module.
Control input	Control input enters the module via parameters passed as input to the Java classes from the application using the module. Control input consists of calls to the java classes. The control input is provided by the end users or crypto officers using application features or services.
Status output	Status output consists of exceptions and status returned from calls to the java classes. This data is output to crypto officers via log file events maintained by the calling application.

3 Security Functions

The Cryptographic Library implements the approved security functions described in Table 3.

Table 3: Module Approved Security Functions.

Approved Security Function	Certificate
Symmetric Key Encryption (and Decryption)	
AES (FIPS PUB 197) ECB Mode E/D 128, 192, 256	2029
Random Number Generation	
RNG (ANSI X9.31, Appendix A.2.4) AES 128key	1062
Hashing	
SHA (FIPS PUB 180-2) SHA-256	1778
MAC	
HMAC SHA-256 (FIPS PUB 198) (Key Size Ranges Tested: KS=BS) SHS Val#1778	1231

4 FIPS Approved Mode of Operation

The module’s approved mode of operation is restricted to performing only FIPS-approved cryptographic algorithms and security functions. The module automatically enters FIPS approved mode on power up as soon as it successfully completes the power-on self test.

The module does not have a non-approved mode.

5 Cryptographic Keys and CSPs

The module uses the following cryptographic keys and CSPs:

Table 4: Cryptographic Keys and CSPs

CSP	Description	Size	Origin	Storage	Output	Zeroization
seedInput	Entropy bits used to derive the RNG seed key. The caller is responsible for specifying an appropriate entropy source.	128 bits	Generated outside the module.	Not stored	N/A	Zeroized after use.
Seed Key	The initial input to the RNG to derive a random number.	128 bits	DRNG	Not stored	N/A	Zeroized after use.
RNG State Variables (I, temp, R)	RNG intermediate values	128 bits	DRNG	Not stored	N/A	Zeroized after use.
cryptkey	Used internally by the AES function within the Random Number Generator	256 bits	Generated outside the module.	Temporary, in volatile RAM.	N/A	Zeroized on power-off or reboot.
HMAC key	A persistent key stored outside of the cryptographic module that is used for the software integrity test	256 bits	Generated outside the module.	Stored outside the module.	N/A	Not Zeroized.
AES e/d keys	Ephemeral AES keys for use in encryption and decryption operations.	128, 192, or 256 bits	Generated outside the module.	Temporary, in volatile RAM.	N/A	Zeroized on power-off or reboot.

Key management functions of key generation, key establishment, key storage, key destruction) is the responsibility of the application using the Biscom Cryptographic Library.

AES encryption and decryption keys are entered into the library in plaintext form, using parameters of the appropriate Java classes. All local copies of key data in the module reside in internally allocated volatile memory. These ephemeral keys are only in library-controlled memory for the duration of the execution of the function. Once the function execution completes, the memory containing the keys is zeroized and released. The underlying operating system is responsible for protecting the memory and process space of the library from unauthorized access.

See section 7, Access Control for more information about how keys are accessed.

6 Roles, Services, and Authentication

6.1 *Roles and Services*

The module supports a Crypto Officer role and a User role.

The Crypto Officer and User roles are implicitly assumed by the entity accessing services implemented by the module. The Crypto Officer role is implicitly entered when installing or deinstalling the module or using the RNG function to generate keys. The Crypto Officer and User may be different people or they may be the same person performing role-specific module operations. Table 5 describes the roles and services.

Table 5: Roles and Services

Role	Services
Crypto Officer	Installation/deinstallation of the cryptographic module onto the computer system. All services provided by the Cryptographic Library.
User	Data encryption and decryption services provided by the Cryptographic Library.

6.2 *Authentication*

The module does not support operator identification or authentication mechanisms. These functions are outside the scope of the module.

Only a single user in a specific role may access the module services at any given time.

6.3 Services

The module supports services that are available to operators in the Crypto Officer or User role. All of the services provided by the module are described in the *Biscom Cryptographic Library 1.0 Javadoc API Reference.* Table 6 shows the cryptographic services available to the various roles.

Table 6: Authorized Services

Service	***Java Class***	***Crypto Officer***	***User***
Installation Deinstallation	N/A	●	
Data encryption using AES-ECB	AESCipher	●	●
Data decryption using AES-ECB	AESCipher	●	●
SHA Hashing	SHA256MessageDigest	●	
Random Number Generation	RandomGenerator	●	
Software Integrity Test	HmacSHA256	●	
Run self test	CryptoServices getInstance Restart the calling application	●	
Show status	CryptoServices.getInstance().isValid() and CryptoServices.getInstance().showStatus()	●	
Get version	CryptoServices.getNameAndVersion() and CryptoServices.getVersion()	●	
Zeroize module keys	CryptoServices.zeroize()	●	

7 Access Control

Table 7 shows services that use or affect cryptographic keys or CSPs. For each service, the key or CSP is indicated along with the type of access.

Table 7: Access Control

Key or CSP	***Service***	***Access Control***
AES Symmetric Key	Run self test	R,E *
	Data encryption and decryption	E, Z *
	Zeroize	Z
HMAC Key	Integrity Test	R, E *
Cryptkey	Generate random number	R, E *
	Zeroize	Z
Seed Key	Generate random number	R, E *
	Zeroize	Z

* E, Z, and R indicate the type of access as follows:

Type of Access	**Description**
R	The item is **read** or referenced by the service.
Z	The item is **zeriozed** by the service.
E	The item is **executed** by the service. (The item is used as part of a cryptographic service.)

8 Physical Security

The Biscom Cryptographic Library is a software cryptographic module and does not enforce any physical security as it has no direct physical embodiment.

The module is software that is intended to run on standard computer that conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital devices, Class A. The module was tested on a standard computer having a FCC DoC (Declaration of Conformity) meeting these requirements.

9 Self Tests

The module performs power-on self tests (POST) to verify the integrity and correct operational functioning of the cryptographic module. If the system fails a self test, it reports status indicating which failure occurred and transitions to an error state, blocking all data output via the data output interface and preventing use of any cryptographic keys, CSPs, cryptographic algorithms, and security functions.

While the module is performing any power on self test, the module design and implementation prevents it from entering a state where data output via the data output interface is possible. Table 8 describes the self-tests.

Table 8: Self Tests

Self Test	***Description***
Mandatory power-up tests performed at power-up and on demand:	
Cryptographic Algorithm Known Answer Tests	Each cryptographic algorithm (AES ECB, RNG), performed by the module, is tested using a “known answer” test to verify the operation of the function.
Software Integrity Test	The module computes an HMAC SHA-256 hash of the software binary files to verify its integrity.
Critical Function tests performed at power-up:	
None.	No security-relevant critical function tests are performed.
Conditional tests performed, as needed, during operation:	
RNG Continuous Tests	RNG continuous tests are performed to check for duplicate contiguous random numbers which may indicate the RNG is stuck.

The known answer tests (KAT) function by encrypting (or hashing) a string for which the calculated output is known and stored within the cryptographic module. An encryption or hashing test passes when the freshly calculated output matches the expected (stored) value. A test fails when the calculated output does not match the expected value. The test then decrypts the ciphertext string. A decryption test passes when the freshly calculated output matches the plaintext value. A test fails when the calculated output does not match the plaintext value.

10 Mitigation of Attacks

The cryptographic module is not designed to mitigate specific attacks.

11 Design Assurance

Configuration Management – Source code, associated documentation, and other module files are managed using the CVS (Concurrent Version System) configuration management system. Each modification automatically applies a unique version identifier.

Delivery and Operation – Delivery and first time operation are controlled. The Biscom Cryptographic Library is distributed only as an integrated component of other Biscom software products. A crypto officer obtains the software product containing the module by downloading it from a Biscom Delivery Server over a secure (SSL) channel. The crypto officer installs and configures the product containing the module for use.

Development – The module design follows a High Level Design specification that functionally defines the module, ports and interfaces and the purpose of each. Details are provided in the *Biscom Cryptographic Library 1.0 Javadoc API Reference*.

12 Guidance

This section provides guidance for crypto officers and users. A crypto officer obtains the software containing the cryptographic module from Biscom, and installs and configures the software for use. Users access the module encryption and decryption services by way of the application that contains the module.

The guidance assumes cryptographic officers are not malicious and they follow all instructions in the guidance.

12.1 Crypto Officer Guidance

12.1.1 Obtaining the Module

The crypto officer receives an email containing an HTTPS link to a Biscom Delivery Server containing the software product that includes the cryptographic module and downloads the software.

12.1.2 Installation

The crypto officer installs the software containing the library on one of the general-purpose operating systems supported by the Biscom Cryptographic Library. Section 2.2 describes the validated platforms and the compatible platforms on which the module may be installed. The crypto officer must follow the installation instructions provided with the software.

After the software is installed the encryption and decryption services must be enabled as described in the installation instructions for the software containing the module.

12.1.3 Single User Mode

When the crypto module is implemented in a server environment, the server application is the user of the cryptographic module. The server application makes the calls to the cryptographic module. Therefore, the server application is the single user of the cryptographic module, even when the server application is serving multiple clients. See section 6.1 of the *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*, updated March 03, 2011.

The module may be executed on a non-server environment, but for the purposes of this validation, the module was tested and may also be executed in a server environment.

12.1.4 Operating the Module

Routine cryptographic officer operations includes:

- Starting and stopping the module by starting the software application that contains the module.

- Using the random number generator to create encryption/decryption keys
- Destroying encryption and decryption keys
- Using the encryption and decryption services to test operation
- Running the power-on self test by restarting the software application.
- Viewing module event messages to determine the module version information, or whether a self-test has failed.

12.1.5 Troubleshooting the Module

If the module is throwing exceptions, the module is in an error state. In this error state, the module is non-functional and does not provide cryptographic services.

If the module is not throwing exceptions, the module has successfully completed its power-up self-tests and is fully functional. If the library is not throwing exceptions, it is running successfully.

If the module is returning exceptions on every call to the module's services, it is possible the cryptographic module has failed one of the power-on self tests or a conditional test. In this case, view the module event messages by calling CryptoServices.getInstance().getErrorList() to find any of the following module self test failure messages:

- AESCipher self test failed
- RandomGenerator self test failed
- HmacSHA256 self test failed (Software Integrity Test)
- RandomGenerator generated duplicate contiguous random numbers

If the most recent module self test message indicates a failure, restart the module by restarting the application. If a self test failure persists, contact Biscom support for assistance.

12.2 User Guidance

Users access the modules encryption and decryption services indirectly by using the software application features. No special instructions are needed for users.

13 References

The Security Policy references the following API reference document:

- *Biscom Cryptographic Library 1.0 Javadoc API Reference*

The following National Institute of Standards and Technology publications are available at URL http://csrc.nist.gov/groups/STM/cmvp/index.html:

- *FIPS PUB 140-2: Security Requirements for Cryptographic Modules*
- *FIPS 140-2 Annex A: Approved Security Functions*
- *FIPS 140-2 Annex B: Approved Protection Profiles*
- *FIPS 140-2 Annex C: Approved Random Number Generators*
- *FIPS 140-2 Annex D: Approved Key Establishment Techniques*
- *Derived Test Requirements (DTR) for FIPS PUB 140-2, Security Requirements for Cryptographic Modules* (a joint publication of the National Institute of Standards and Technology and Communications Security Establishment).
- *Advanced Encryption Standard (AES)*, Federal Information Processing Standards Publication 197
- *Secure Hash Standard (SHS)*, Federal Information Processing Standards Publication 180-3