

interopLab

Bloombase Cryptographic Module FIPS 140-2 Non-Proprietary Security Policy

Version 0.96

June 2, 2016

BLOOMBASE®

Document No. Bloombase Cryptographic Module - FIPS140-2 - Security Policy - 0.96

Table of Contents

Table of Contents 3

Introduction 6
Overview 6
Purpose 7
References 7
Document Organization 7

Bloombase Cryptographic Module 8
Cryptographic Module Specification 8
Security Level 10
Module Ports and Interfaces 11
Logical Interface 11
Physical Interface 11
Roles, Services, and Authentication 12
Identification and Authentication Policy 12
Access Control Policy and Services 13
FIPS Approved Services 13
Non-FIPS Approved Services 14
Cryptographic Algorithms 15
FIPS Approved Algorithms 15
Non-FIPS Algorithms 16
Cryptographic Key Management 16
Key Entry 16
Key Storage 17
Key Access 17
Key Protection and Zeroization 18
Operational Environment 18
Self-Tests 19
Power-up Self-tests 19
Conditional Self-tests 19
Setup and Installation 20
EMI/EMC 20
Physical Security Policy 20
Design Assurance 20
Mitigation of Other Attacks 20

Glossary and Definitions 21

References 24

Contacting Bloombase 25
Support and Service 25
Feedback 25

Introduction

Overview

This non-proprietary Cryptographic Module Security Policy for the Bloombase Cryptographic Module describes how the Bloombase Cryptographic Module meets the Level 1 security requirements of FIPS 140-2. It contains a specification of the rules under which the cryptographic module must operate. These security rules were derived from the requirements of the FIPS 140-2.

Validation testing for Bloombase Cryptographic Module was performed on BloombaseOS security hardened operating system running Java Runtime Environment (JRE).

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 Security Requirements for Cryptographic Modules) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST Web site at http://csrc.nist.gov/cryptval/.

Purpose

There are several major reasons for defining the security policy that is followed by the Bloombase Cryptographic Module:

- It is required for FIPS 140-2 validation.
- It allows individuals and organizations to determine whether the Bloombase Cryptographic Module, as implemented in a product, satisfies the stated security policy.
- It describes the capabilities, protection, and access rights provided by the cryptographic module, allowing individuals and organizations to determine whether it will meet their security requirements.

References

This document deals only with the operations and capabilities of the Bloombase Cryptographic Module in the technical terms of a FIPS 140-2 cryptographic module security policy.

More information is available on the Bloombase Cryptographic Module application from the following sources:

- Refer to http://www.bloombase.com/ for information on Bloombase products and services as well as answers to technical or sales related questions.
- The Bloombase Knowledgebase website contains detailed technical knowledge of our products.

Document Organization

This document explains the Bloombase Cryptographic Module FIPS 140-2 relevant features and functionality. This document comprises the following sections:

- This section, "Introduction", provides an overview and introduction to the Security Policy.
- "Bloombase Cryptographic Module" describes how Bloombase Cryptographic Module meets FIPS 140-2 requirements.
- "Glossary and Definitions" lists the acronyms and definitions used in this document.
- "References" contains information references that provide helpful background information.

Bloombase Cryptographic Module

Cryptographic Module Specification

This section defines the cryptographic module that is being submitted for validation to FIPS 140-2, level 1.

The Bloombase Cryptographic Module, software version 8.0, is defined as a multi-chip standalone cryptographic module according to FIPS 140-2.

The module consists of the following generic components:

- A commercially available general-purpose hardware computing platform as shown in below figure.
- A commercially available operating system that runs on the above platform.
- A software component, the Bloombase Cryptographic Module that runs on the above platform and operating system. This component is custom designed and written by Bloombase in the 'Java' and 'C' computer languages and is identical, at the source code level, for all identified hardware platforms and operating systems. An application programming interface (API) is defined as the interface to the cryptographic module.

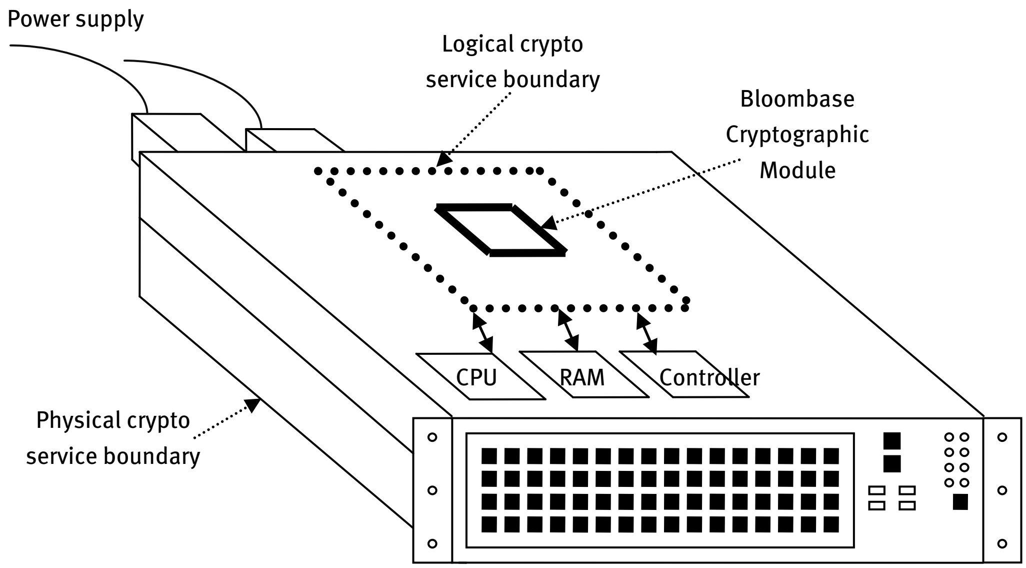

Figure 1 – Components of the Bloombase Cryptographic Module

The cryptographic module consists of executable object code which is intended for use in a commercially available operating system. The cryptographic module provides a set of APIs that allow Bloombase information security products to integrate the cryptographic module security features into the products where information security functions are required.

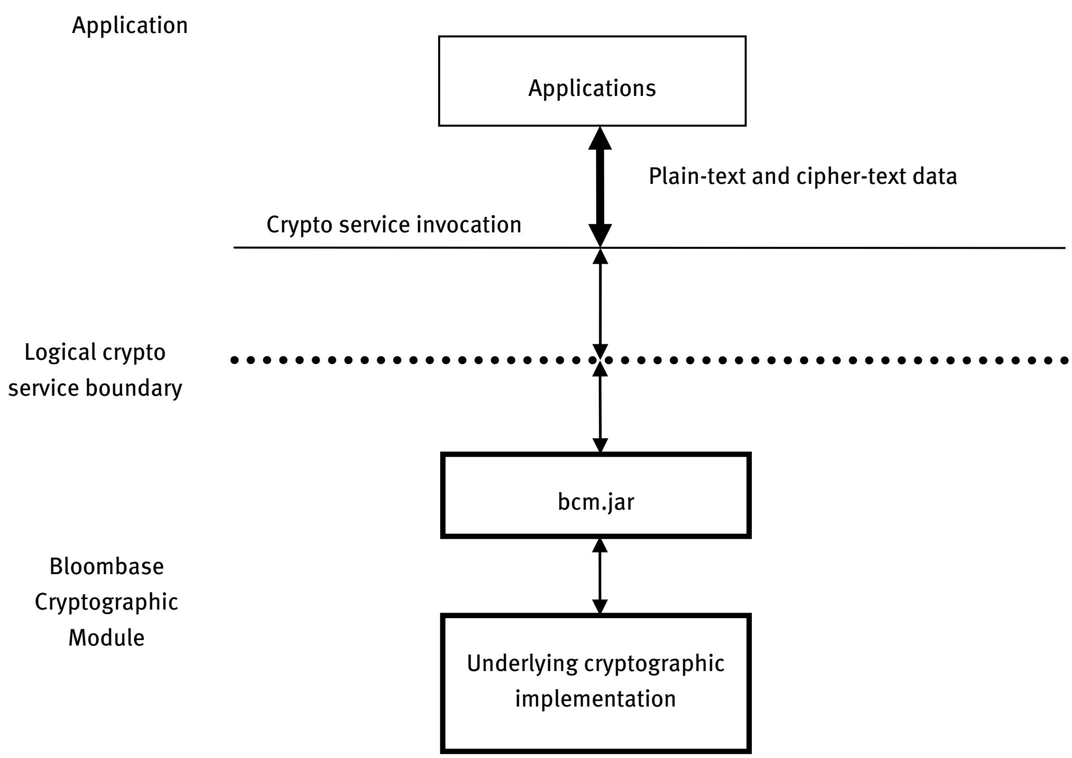

Figure 2 – The Bloombase Cryptographic Module Block Diagram

Security Level

The Bloombase Cryptographic Module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

The following table summarizes module security level specification:

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

Table 1 –Security Level of Security Requirements

Module Ports and Interfaces

The Bloombase Cryptographic Module is considered according to the requirements of FIPS 140-2 to be a multi-chip standalone module.

Logical Interface

FIPS 140-2 Interface	Description
Data Input Interface	Input parameters of module function calls
Data Output Interface	Output parameters and return values of module function calls
Control Input Interface	Module control function calls
Status Output Interface	Return values from module function calls and output messages to console
Power Interface	Initialization functions

Table 2 – Logical Interfaces

Physical Interface

FIPS 140-2 Interface	Description
Data Input Interface	Ethernet/Network Port
Data Output Interface	Ethernet/Network Port
Control Input Interface	Keyboard and Mouse
Status Output Interface	Monitor
Power Interface	Power Interface

Table 3 – Physical Interfaces

Roles, Services, and Authentication

Bloombase Cryptographic Module meets all FIPS 140-2 Level 1 requirements for roles and services, implementing both a User (User) role and Cryptographic Officer (CO) role. Since the module is validated at security level 1, it does not provide an authentication mechanism.

Identification and Authentication Policy

The following table summarizes roles and required identification and authentication

Role	Type of Authentication	Authentication Data
User	None	N/A
Cryptographic Officer	None	N/A

Table 4 – Roles and Required Identification and Authentication

The following table summarizes strengths of authentication mechanisms

Authentication Mechanism	Strength of Mechanism
None	N/A

Table 5 – Strengths of Authentication Mechanisms

The following table describes the services accessible by the two roles

Role	Services
User	The User can perform general security functions, as described in the Bloombase Cryptographic Module User Guide. The User can also call specific FIPS 140-2 module functions and method invocation calls as defined in the User Guide.
Cryptographic Officer	The Cryptographic Officer has access to a superset of the services that are available to the User. The Cryptographic Officer role can also invoke the full set of self-tests inside the module.

Table 6 – Roles and their Accessible Services

Access Control Policy and Services

Bloombase Cryptographic Module supports two roles: User and Cryptographic Officer. The types of services and cryptographic key access corresponding to the supported roles are described in the table below. The roles are implicitly assumed by the operator, based on the services executed.

FIPS Approved Services

Service	Roles	Cryptographic Keys	Accessibility
Symmetric encryption/decryption	• User • Cryptographic Officer	• Symmetric key • AES	• Read • Write • Execute
Key transport	• User • Cryptographic Officer	• Asymmetric private key • RSA	• Read • Write • Execute
Digital signing/verification	• User • Cryptographic Officer	• Asymmetric private key • RSA	• Read • Write • Execute
Keyed hash (HMAC) (Key size >= 112 bits)	• User • Cryptographic Officer	• HMAC SHA-1 key • HMAC-SHA-1	• Read • Write • Execute
Message digest (SHS)	• User • Cryptographic Officer	• N/A	• Read • Write • Execute
Show status	• User • Cryptographic Officer	• N/A	• Execute

Service	Roles	Cryptographic Keys	Accessibility
Module initialization	• User • Cryptographic Officer	• N/A	• Execute
Self test	• Cryptographic Officer	• N/A	• Execute
Zeroize	• User • Cryptographic Officer	• Symmetric key • Asymmetric key • HMAC-SHA-1 key	• Execute

Table 7 – FIPS Approved Services

Non-FIPS Approved Services

These non-FIPS approved services cannot be used in the FIPS mode of operation. Keys generated by these non-FIPS approved services cannot be used in the FIPS mode of operation.

Service	Roles	Cryptographic Keys	Accessibility
Asymmetric key generation	• User • Cryptographic Officer	• RSA • Asymmetric private key	• Read • Write • Execute
Symmetric key generation	• User • Cryptographic Officer	• Symmetric key • AES	• Read • Write • Execute
Keyed hash (HMAC) (Key size < 112 bits)	• User • Cryptographic Officer	• HMAC SHA-1 key • HMAC-SHA-1	• Read • Write • Execute

Service	Roles	Cryptographic Keys	Accessibility
Random number generation	• User • Cryptographic Officer	• AES	• Read • Write • Execute

Table 8 – Non-FIPS Approved Services

Cryptographic Algorithms

FIPS Approved Algorithms

The following is a list of validated FIPS Approved algorithms that can be used by the operator of the Bloombase Cryptographic Module:

FIPS Approved Algorithm	Validation Certificate Number	Usage
AES (ECB/CBC/CFB8, 128/192/256)	1041	Encryption and decryption
RSA PKCS#1 sig/verify (modulus sizes 2048/3072/4096 and SHA-1/SHA-256/SHA-384/SHA-512)	496	Digital signing and verification
SHA-1/SHA-256/SHA-384/SHA-512 (Byte-only)	991	Hash generation
HMAC-SHA-1[1]/HMAC-SHA-256/HMAC-SHA-384/HMAC-SHA-512	583	Message authentication code

Table 9 – FIPS Approved Cryptographic Algorithms

1 HMAC with key size < 112 bits are only allowed for legacy signature verification

Non-FIPS Algorithms

The Bloombase Cryptographic Module provides non-FIPS approved algorithms, which are not allowed to be used in FIPS Mode, as follows

Algorithm
PRNG (ANSI X9.31, AES 128/192/256)
RSA X9.31 KeyGen (modulus sizes 1024/1536/2048/3072/4096)
RSA PKCS#1 sig/verify (modulus sizes 1024/1536)
HMAC-SHA-1 (key size < 112 bits)

Table 10 – Non-FIPS Approved Cryptographic Algorithms

Cryptographic Key Management

Cryptographic key management is concerned with generating and storing keys, managing access to keys, protecting keys during use, and zeroizing keys when they are no longer required.

Key Entry

Key or CSP	Description
AES	Input by the calling application and never exits the module.
RSA	Input by the calling application and never exits the module.
HMAC-SHA	Input by the calling application and never exits the module.
HMAC-SHA-1 integrity key	Generated at module build time.

Table 11 – Descriptions of Cryptographic Key Entries

Key Storage

Key or CSP	Description
AES	Volatile memory while in use.
RSA	Volatile memory while in use.
HMAC-SHA	Input by the calling application and never exits the module.
HMAC-SHA-1 integrity key	Stored in plaintext in module binary.

Table 12 – Descriptions of Cryptographic Key Storage

Key Access

Key or CSP	Description
AES	Used by the calling application. An authorized operator of the module has access to all key data created during the Bloombase Cryptographic Module operation.
RSA	Used by the calling application. An authorized operator of the module has access to all key data created during the Bloombase Cryptographic Module operation.
HMAC-SHA	Used by the calling application. An authorized operator of the module has access to all key data created during the Bloombase Cryptographic Module operation.
HMAC-SHA-1 integrity key	No operator has access to this key.

Table 13 – Descriptions of Cryptographic Key Access

Key Protection and Zeroization

Key or CSP	Description
AES	Never exits the module. When the module is uninstalled or by rebooting power cycle, the key will be zeroized.
RSA	Never exits the module. When the module is uninstalled or by rebooting power cycle, the key will be zeroized.
HMAC-SHA	Used by the calling application. An authorized operator of the module has access to all key data created during the Bloombase Cryptographic Module operation.
HMAC-SHA-1 integrity key	Zeroized by uninstalling the module.

Table 14 – Descriptions of Cryptographic Key Protection and Zeroization

Operational Environment

The operating environment for the Cryptographic Module is a "modifiable operational environment".

When the Cryptographic Module is operated in FIPS approved mode, the environment is restricted to a single operator mode of operation (i.e., concurrent operators are explicitly excluded).

The Cryptographic module prevents access by other processes to private and secret keys, and intermediate key generation values during the time the Cryptographic Module is executing or in operation; using address space separation mechanisms of the operational environment. Processes that are spawned by the Cryptographic Module are owned solely by the Cryptographic Module and are not owned by any other external processes/operators. Non-cryptographic processes shall not interrupt the Cryptographic Module during execution.

The Bloombase Cryptographic Module is installed in a form that protects the software and executable code from unauthorized disclosure and modification.

Each software components of the module implements an approved message authentication code, used to verify the integrity of the software component during the power-up self-test.

While loaded in the memory, the target OS will protect all unauthorized access to the Cryptographic Module's address memory and process space.

Self-Tests

To prevent any secure data from being released, it is important to test the cryptographic components of a security module to ensure all components are functioning properly. To confirm correct functionality, the Bloombase Cryptographic Module performs the following self-tests.

Power-up Self-tests

Test	Description
Software integrity check	Verifying the integrity of the software binaries of the module with HMAC SHA-1. The integrity check on all three binaries is carried out by bcm.jar.
AES Encryption KAT	Verifying the correct operation of the AES algorithm implementation
AES Decryption KAT	Verifying the correct operation of the AES algorithm implementation
RSA	Sign and verify test with 2048-bit key
SHA	SHA-1
HMAC	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512

Table 15 – Descriptions of Power-up Self-tests

Conditional Self-tests

Test	Description
RSA	Sign/Verify test with 2048-bit key
Non-approved PRNG	Continuous PRNG test

Table 16 – Descriptions of Conditional Self-tests

The power-up self-tests are automatically invoked on module power-up and status output is logged to the system console.

A failure in any self-test causes an exception to be thrown and an error message logged to the system console, causing the module to transition to an error state.

All data output via the data output interface is inhibited both during self-tests and while in the error state.

Setup and Installation

The module comes pre-installed on the target platform and requires no set-up, as it only executes in the FIPS-approved mode of operation. The module is deemed to be operating in FIPS mode when the power-up self-tests have passed and one of the FIPS approved services (from above) is being utilized. Otherwise, it is considered a non-approved usage of the module.

EMI/EMC

The hardware computing platforms under testing comply with the limits for a Class B digital device pursuant to Part 15 of the Federal Communications Commission (FCC) Rules.

Physical Security Policy

Since the Bloombase Cryptographic Module is implemented solely in software, the physical security section of FIPS 140-2 is not applicable.

Design Assurance

Bloombase maintains all versioning for all source code and associated documentation through CVS versioning handling system.

Mitigation of Other Attacks

The Bloombase Cryptographic Module does not employ security mechanisms to mitigate specific attacks.

Glossary and Definitions

The following table lists the glossaries and definitions used throughout this document

Term	Definition
AES	Advanced Encryption Standard. A fast block cipher with a 128-bit block, and keys of lengths 128, 192, and 256 bits. Replaces DES as the US symmetric encryption standard.
API	Application Programming Interface.
CBC	Cipher Block Chaining. A mode of encryption in which each ciphertext depends upon all previous ciphertexts. Changing the Initialization Vector (IV) alters the ciphertext produced by successive encryptions of an identical plaintext.
CFB	Cipher Feedback. A mode of encryption that produces a stream of ciphertext bits rather than a succession of blocks. In other respects, it has similar properties to the CBC mode of operation.
DES	Data Encryption Standard. A symmetric encryption algorithm with a 56-bit key. See also Triple DES.

Term	Definition
Diffie-Hellman	The Diffie-Hellman asymmetric key exchange algorithm. There are many variants, but typically two entities exchange some public information (for example, public keys or random values) and combines them with their own private keys to generate a shared session key. As private keys are not transmitted, eavesdroppers are not privy to all of the information that composes the session key.
DSA	Digital Signature Algorithm. An asymmetric algorithm for creating digital signatures.
ECB	Electronic Codebook. A mode of encryption that divides a message into blocks and encrypts each block separately.
ECC	Elliptic Curve Cryptography.
FIPS	Federal Information Processing Standards.
IV	Initialization Vector. Used as a seed value for an encryption operation.
KAT	Known answer test.
Key	A string of bits used in cryptography, allowing people to encrypt and decrypt data. Can be used to perform other mathematical operations as well. Given a cipher, a key determines the mapping of the plaintext to the ciphertext. The types of keys include distributed key, private key, public key, secret key, session key, shared key, subkey, symmetric key, and weak key.
MD5	A secure hash algorithm created by Ron Rivest. MD5 hashes an arbitrary-length input into a 16-byte digest.
NIST	National Institute of Standards and Technology. A division of the US Department of Commerce (formerly known as the NBS) which produces security and cryptography-related standards.
OFB	Output Feedback. A mode of encryption in which the cipher is decoupled from its ciphertext.
OS	Operating System.
PC	Personal Computer.
RC2	Block cipher developed by Ron Rivest as an alternative to the DES. It has a block size of 64 bits and a variable key size. It is a legacy cipher and RC5 should be used in preference.
RC4	Symmetric algorithm designed by Ron Rivest using variable length keys (usually 40-bit or 128-bit).
RC5	Block cipher designed by Ron Rivest. It is parameterizable in its word size, key length, and number of rounds. Typical use involves a block size of 64 bits, a key size of 128 bits, and either 16 or 20 iterations of its round function.
PRNG	Pseudo Random Number Generator.

Term	Definition
RSA	Public key (asymmetric) algorithm providing the ability to encrypt data and create and verify digital signatures. RSA stands for Rivest, Shamir, and Adleman, the developers of the RSA public key cryptosystem.
SHA	Secure Hash Algorithm. An algorithm that creates a unique hash value for each possible input. SHA takes an arbitrary input that is hashed into a 160-bit digest.
SHA-1	A revision to SHA to correct a weakness. It produces 160-bit digests. SHA-1 takes an arbitrary input that is hashed into a 20-byte digest.
SHA-2	The NIST-mandated successor to SHA-1, to complement the Advanced Encryption Standard. It is a family of hash algorithms (SHA-224, SHA-256, SHA-384 and SHA-512) that produce digests of 224, 256, 384 and 512 bits respectively.
Triple DES	A variant of DES that uses three 56-bit keys.

Table 17 – Glossary and Definitions

References

1. [FIPS-140-2] "Security Requirements for Cryptographic Modules" Version 2, May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

2. [FIPS-180-2] "Secure Hash Standard" Version 2, August 1, 2002. http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf

3. [FIPS-186-2] "Digital Signature Standard (DSS)" Version 2, January 27, 2000. http://csrc.nist.gov/publications/fips/fips186-2/fips186-2.pdf

4. [FIPS-197] "Advanced Encryption Standard (AES)" November 26, 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

5. [FIPS-46-3] "Data Encryption Standard" October 25, 1999. http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

Contacting Bloombase

The Bloombase Website contains latest news, security bulletins and information about our coming events

The Bloombase Knowledgebase website contains detailed technical knowledge of our products.

Support and Service

If you have any questions or extra information is required, please see Bloombase SupPortal.

Feedback

We welcome your feedback on our documentation. If you have further inquiries, please contact us at email certifications@bloombase.com.