FIPS 140-2 Non-Proprietary Security Policy

BigFix Cryptographic Module 1.0
Level 2 Validation

Document Version: 1.0.6
Last Updated: 17 December 2008

BigFix, Inc.
1460 64th St., Suite 200
Emeryville, CA 94608
www.bigfix.com

Table Of Contents

1 INTRODUCTION

1.1 Purpose

This document describes the non-proprietary FIPS 140-2 Security Policy for the BigFix Cryptographic Module 1.0. This document describes how the BigFix Cryptographic Module 1.0 meets all the requirements as specified in the FIPS 140-2 Level 2 requirements. This Security Policy forms a part of the submission package to the validating lab.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2) specifies the security requirements for a cryptographic module protecting sensitive information. Based on four security levels for cryptographic modules this standard identifies requirements in eleven sections. For more information about the standard download the file at this URL: http://csrc.nist.gov/cryptval/.

1.2 References

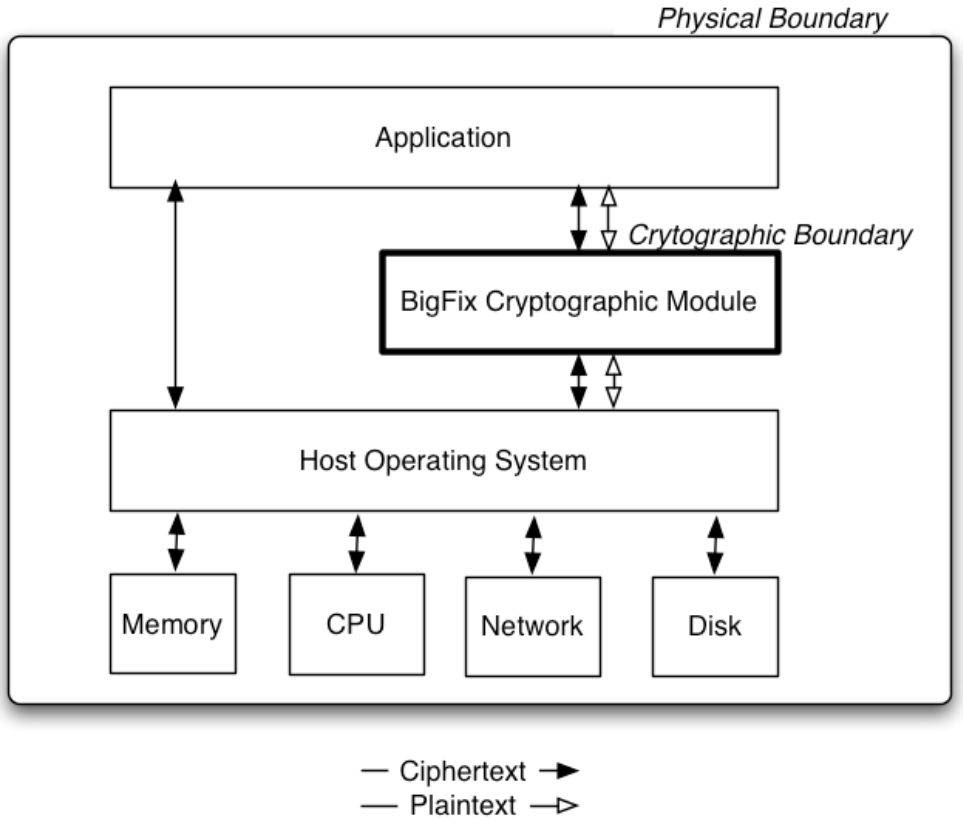
This Security Policy describes how this module complies with the eleven sections of the FIPS 140-2 Standard:

- For more information on the FIPS 140-2 standard and validation program please refer to the NIST website at http://csrc.nist.gov/groups/STM/index.html.
- For more information about BigFix solutions please visit http://www.bigfix.com

All operating systems used to test the module have been certified against the Controlled Access Protection Profile (CAPP), version 1.d, Protection Profile NoPP006, 8 October, 1999.

2 PRODUCT DESCRIPTION

The BigFix Cryptographic Module 1.0 is a software library that runs on a wide variety of computing platforms and performs encryption, hashing, and random number generation functions. The cryptographic boundary is defined as the BigFix Cryptographic Module itself: a binary software library for general purpose computers. The format of this library differs from system to system: on Windows this library is a Dynamic Link Library (.dll); on Mac OS X it is a Dynamic Library (.dylib); on Linux, AIX, HP-UX, and Solaris the file is a Shared Object library (.so). The block diagram for the module is as shown below with all the inter-connections between the components of the module.



Block Diagram note: The BigFix Cryptographic Module accepts data input, and control input; the module returns data output and status output.

The module implements AES, Triple-DES, RSA (signing/verification), DSA, HMAC-SHA, and SHA algorithms in the approved mode. FIPS 140-2 allows the use of RSA for key wrapping, which is implemented in the module. Diffie-Hellman is non-Approved at this time as it only provides functions that implement Diffie-Hellman primitives. The Diffie-Hellman shared secret, as implemented in the module, provides between 80 and 219 bits of encryption strength. The Diffie-Hellman implementation is not capable of key agreement.

The product meets the overall requirements applicable to Level 2 security for FIPS 140-2, with Roles, Services and Authentication meeting the Level 3 requirements. The module relies on the Operating System to provide authentication of operators. The Operating System is responsible for clearing any previous authentications when the computer is powered down and has the capability to protect the authentication data. For purposes of FIPS 140-2, the module is considered to be a multi-chip standalone product.

Security Requirements Section	Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services and Authentication	3
Finite State Machine Model	2
Physical Security	N/A
Operational Environment	2
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A
Cryptographic Module Security Policy	2
Overall Level of Certification	2

Table 1: Module Compliance

2.1 Platform Support

The BigFix Cryptographic Module 1.0 supports twelve (12) different Operating Systems. The following table lists the Operating Systems and hardware that was used for testing the module. Each of the systems listed in the table are CCEVS approved configurations.

Operating System	Hardware
AIX 5.2	IBM P610, Power3-II 333 MHz CPU
http://www.commoncriteriaportal.org/files/epfiles/0194a.pdf	
HP-UX 11.11	HP C3000 (which is part of the HP 9000 Server or HP Integrity family), 64-bit PA-8500 400 MHz CPU
http://www.commoncriteriaportal.org/files/epfiles/CRP176.pdf	
SuSE Linux Enterprise Server v9	IBM eServer 325 Dual AMD Opteron 2.0 GHz CPU
http://www.commoncriteriaportal.org/files/epfiles/0256a.pdf	
Mac OS X 10.3.6	Apple iMac G4, PowerPC G4 1.0 GHz CPU
http://www.niap-ccevs.org/cc-scheme/st/vid4012/	
Red Hat Enterprise Linux 4 Update 2 Advanced Server	HP XW4100 Pentium 4 3.0 GHz CPU
http://www.niap-ccevs.org/cc-scheme/st/vid10133/	
Red Hat Enterprise Linux 4 Update 2 Advanced Server 64-bit	HP ProLiant DL145 G2 AMD 64 Opteron 2.0 GHz CPU
http://www.niap-ccevs.org/cc-scheme/st/vid10133/	
Solaris 9 SPARC	Sun Blade 150, Ultrasparc IIe 650 MHz CPU
http://www.commoncriteriaportal.org/files/epfiles/Solaris 9 CR.pdf	
Solaris 10 SPARC	Sun Blade 150, Ultrasparc IIe 650 MHz CPU
http://www.commoncriteriaportal.org/files/epfiles/solaris10R1106-cert-e.pdf	
Solaris 10 x86	Dell Precision 650, Dual Xeon 3.0 GHz CPU
http://www.commoncriteriaportal.org/files/epfiles/solaris10R1106-cert-e.pdf	
Windows 2000 Pro SP3	Dell Optiplex GX400, Pentium 4 CPU
http://www.niap-ccevs.org/cc-scheme/st/vid4002/	
Windows 2003 Enterprise Edition SP1	Dell Optiplex GX270, Pentium 4 CPU

http://www.niap-ccevs.org/cc-scheme/st/vid9506/	
Windows XP Pro SP2	Dell Optiplex GX270, Pentium 4 CPU
` http://www.niap-ccevs.org/cc-scheme/st/vid9506/	

Table 2: Platform Support

3 MODULE PORTS AND INTERFACES

The BigFix Cryptographic Module provides the following logical interfaces through the module's API: data input, data output, control input, and status output. The physical ports and interfaces are those of the general purpose computer on which the module is installed.

FIPS Interface	Physical Port	Module Interface
Data Input	Ethernet ports	API input parameters
Data Output	Ethernet ports	API output parameters
Control Input	Keyboard, Serial port, Ethernet port	API function calls
Status Output	Keyboard, Serial port, Ethernet ports	API return codes
Power Input	PCI Compact Power Connector	N/A

Table 3: Module Ports and Interfaces

The BigFix Cryptographic Module isolates and distinguishes the paths for data input, data output, control input, and status input. Additionally, if the module enters the Error State all data output is inhibited over the data output interface.

4 ROLES, SERVICES AND AUTHENTICATION

The BigFix Cryptographic Module supports a Crypto Officer and a User role. Authentication for these roles is provided by the host operating system. The Module runs on various host operating systems each of which has a mechanism that requires the role be properly authenticated prior to the operator accessing cryptographic module functions. Each host operating system distinguishes between an administrator (or "super user") role and that of a non-privileged user. The module relies on this operating system authentication to distinguish between the different classes of operator.

The Crypto Officer and User roles are implicitly assumed by the entity accessing services implemented by the module. The Crypto Officer can install and initialize the module. The Crypto Officer role is implicitly entered when installing the module or performing system administration functions on the host operating system.

The module does not support a maintenance role.

4.1 Identification and Authentication

The authentication mechanism is provided by the host operating system. Proper operation of the module requires that the host operating system be configured to enforce a password length of at least 8 (eight) characters.

Assuming that no password lockout settings were configured, that no delay is configured between password attempts, and that an attacker could attempt 100 password entries per minute, then the probability that a random attempt will succeed is still less than one in 2 x 10 to the power of 12. Therefore,

the module is sufficiently protected against this type of attack for each of the Operating Systems on which it was tested.

Role	*Type of Authentication*	*Authentication Data*
User	Logon	Password
Crypto Officer	Logon	Password

Table 4: Authentication Type Table

4.2 Roles and Services

The BigFix Cryptographic Module 1.0 supports the services listed in the following table. The table groups the authorized services by the operator roles and identifies the Cryptographic Keys and CSPs associated with the services. The modes of access are also identified per the explanation.

R - The item is **read** or referenced by the service.
W - The item is **written** or updated by the service.
E - The item is **executed** by the service. (The item is used as part of a cryptographic function.)

The two tables below show the services available for each role:

Role	*Authorized Services*	*Cryptographic Keys and CSPs*	*Access Type*
CO	Symmetric Encryption/Decryption	AES	R, W, E
CO	Symmetric Encryption/Decryption	Triple-DES	R, W, E
CO	Message Digest	SHS (SHA-1 SHA-224, SHA-256, SHA-384, and SHA-512)	R, W, E
CO	Message Authentication	HMAC (HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512)	R, W, E
CO	Key Establishment	RSA	R, W, E
CO	Show Status	N/A	E
CO	Self Test	N/A	E
CO	Random Number Generation	Seed Key, Seed, AES	R, W, E
CO	Module Initialization	N/A	R, E
CO	Key Generation	RSA, DSA, AES, Triple-DES	R, W, E
CO	Digital Signature	RSA, DSA	R, W, E
CO	Shared Secret Generation	Diffie-Hellman Shared Secret	R, W, E
CO	Key Zeroization	AES, Triple-DES, HMAC-SHA, RSA, Seed Key	E
CO	Installation	N/A	E

Table 5: Cryptographic Officer – Roles and Services

Role	*Authorized Services*	*Cryptographic Keys and CSPs*	*Access Type*
User	Symmetric Encryption/Decryption	AES	R, W, E
User	Symmetric Encryption/Decryption	Triple-DES	R, W, E
User	Message Digest	SHS (SHA-1 SHA-224, SHA-256, SHA-384, and SHA-512)	R, W, E
User	Message Authentication	HMAC (HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512)	R, W, E
User	Key Establishment	RSA	R, W, E
User	Show Status	N/A	E
User	Self Test	N/A	E
User	Random Number Generation	Seed Key, Seed, AES	R, W, E
User	Key Generation	RSA, DSA, AES, Triple-DES	R, W, E
User	Digital Signature	RSA, DSA	R, W, E
User	Shared Secret Generation	Diffie-Hellman Shared Secret	R, W, E
User	Key Zeroization	AES, Triple-DES, HMAC-SHA, RSA, Seed Key	E

Table 6: User – Roles and Services

5 PHYSICAL SECURITY

The BigFix Cryptographic Module is a software library and therefore the FIPS 140-2 physical security requirements are not applicable.

6 CRYPTOGRAPHIC KEY MANAGEMENT

The following table summarizes the module's keys. The module does not persistently store keys nor is the module capable of importing or exporting keys on its own. The module relies on the host application to manage key import or export functions. The appropriate API calls are used by the application to transfer keys across the defined cryptographic boundary.

Key	Generation	Use
Triple-DES	Generated internally using a PRNG compliant to ANSI X9.31	Triple-DES is used for data encryption and decryption
AES	Generated internally using a PRNG compliant to ANSI X9.31	AES is used for data encryption and decryption
RSA	Generated internally using a PRNG compliant to ANSI X9.31	Used to digitally sign and verify data
DSA	Generated internally using a PRNG compliant to ANSI X9.31	Used to digitally sign and verify data
HMAC-SHA-1	Generated outside the module	Used to verify module integrity during power-up self-tests
RNG	Seed, RNG Key	Used for generation of module keys

Table 7: Cryptographic Keys and CSPs

The module keys map to the following algorithms certificates:

Approved Security Function	*Certificate*
AES *(ECB; CBC; OFB; CFB-8; and CFB-128)*	806
Triple-DES *(ECB; CBC; CFB; and OFB)*	688
RSA *(SigGen; SigVer; and SigVer 9.31)*	388
SHS *(SHA-1; SHA-224; SHA-256; SHA-384; and SHA-512)*	804
HMAC *(HMAC-SHA-1; HMAC-SHA-224; HMAC-SHA-256; HMAC-SHA-384; and HMAC-SHA-512)*	446
DSA *(SigGen; SigVer; PQGGen; and Keypair Gen)*	298
RNG *(ANSI X9.31)*	464
Allowed Security Functions	
RSA (key wrapping; key establishment; methodology provides between 80 and 256 bits of encryption strength)	
Non-approved Security Functions	
Diffie-Hellman (Shared Secret Generation)	

Table 8: FIPS Approved Algorithms Table

The BigFix Cryptographic Module 1.0 does not implement any non-approved algorithms other than those specified in Table 7.

6.1 Key Zeroization

Key zeroization is performed in the module using a specific API call in order to clear the key in memory. This API call is called from an application. Applications that are shipped with the module by BigFix, are designed to call the module's zeroization function.

7 SELF-TEST

The BigFix Cryptographic Module performs the following self tests at power-up:

Cryptographic Algorithm KATs: Known Answer Tests (KATs) are run at power-up for:

- Triple-DES (CBC Mode encrypt/decrypt)
- AES (CBC Mode encrypt/decrypt)
- RSA (signing/verifying)
- DSA (pair wise consistency test)
- HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512
- RNG KAT

Note: The SHA self-tests are performed as part of the HMAC-SHA self-tests.

Software Integrity Test: The BigFix Cryptographic Module checks the integrity of its various components using HMAC-SHA-1.

The module performs the following conditional self tests:

Pairwise Consistency Test: Pairwise consistency tests are run conditionally when the module generates key pairs. The module performs a signing operation with the private key and verifies it with the public key.

Continuous Random Number Generator Test: The module implements a continuous random number generator test per FIPS 140-2 section 4.9.2.

If any of the self-tests enumerated in this section fail, the module will enter the error state. Cryptographic functions and data output are inhibited while the module is in an error state. In order to attempt to clear the error, the operator should re-instantiate the module. Failing this, the module must be re-installed.

When the module is performing self-tests (is in a self-test condition) it inhibits all data output via the output interface. The module is controlled via API function calls operating in a single threaded capacity; the module cannot execute cryptographic functions by the calling application until the self-tests are completed successfully

The User or Crypto Officer can initiate the On Demand self-tests by re-instantiating the module. The power-up self-tests execute without any intervention by the operator.

8 Crypto-Officer and User Guidance

This section describes the configuration, maintenance, and administration of the cryptographic module.

8.0.1 Verification of Module Distribution

This section describes the procedure necessary to verify the BigFix Cryptographic Module as distributed in the BigFix products available from the BigFix website. This procedure does not serve as a replacement for the module's Software Integrity Check. This procedure provides the operator with assurance that the BigFix product they download — product that contains the module and accompanying BigFix applications — has not been modified in transit.

Steps to verify the SHA1 hash of the software package:

A. Download the BigFix installer from http://support.bigfix.com/bes/install/downloadbes.html. This can be the Server installer or one of the multi-platform Client installers.
B. When the download is complete create a SHA1 hash on the file.
C. Compare the hash value to the values listed on the BigFix website: http://support.bigfix.com/bes/install/sha1_checksums.txt

8.1 Secure Setup and Initialization

This section describes the procedures necessary for the setup and initialization of the BigFix Cryptographic Module 1.0 to place the module in a FIPS Approved Mode of operation. The BigFix Cryptographic Module is included with a calling application — any of the BigFix product components: Server, Console, Relay, or Client — the module itself has no user interface and no logging capability. To verify proper setup and initialization of the module the Cryptographic Officer uses the log output from one of the calling applications in conjunction with the graphical interface provided by the calling application as described in the following steps.

Steps to verify Secure Setup and Initialization

A. Install the BigFix product. This contains the BigFix Cryptographic Module 1.0. The instructions can be found in the BigFix Administrator's Guide, the "Managing and Maintaining BES" section, page 72. The document can be downloaded here: http://support.bigfix.com/resources.html.

B. The Crypo Officer (administrator) must enable FIPS Mode by following these steps:

a. Launch the BigFix Administration Tool from Start > Programs > BigFix Enterprise > BES Administration Tool
b. Browse to the location of your site license and click OK
c. Select the Masthead Management tab
d. Click the Edit Masthead button
e. Check “Require use of FIPS 140-2 compliant cryptography” and click OK
f. Launch the BigFix Console from Start > Programs > BigFix Enterprise > BigFix Console
g. From the Computers tab, right-click any computer, and choose “Edit Computer Settings”
h. In the Settings tab of the Edit Computer Settings dialog enter the setting “_BESClient_Cryptography_FipsMode” with a value of "required"
i. In the Target tab of the dialog choose “All computers”
j. In the Execution tab of the dialog choose “Reapply this action whenever it becomes relevant again” and click OK
k. Quit the Administration Tool and the Console

C. Navigate to the BESRelay.log file (located in the BES Server directory) and verify that "OpenSSL Initialized (FIPS Mode)" appears in the log.

The presence of that log entry indicates that The BigFix Cryptographic module has been successfully setup and initialized. In the case of a failure during setup and initialization the error “Failed FIPS setup! Exiting” will be written to the log and the module will exit.

8.2 Module Security Policy Rules

This section describes the rules for which the module must operate in for it to be operating in FIPS Approved Mode of operation.

1. The Operating System must enforce authentication methods to prevent unauthorized access to the module.
2. All of the Critical Security Parameters for the module are securely generated, temporarily stored in the computer’s RAM, and destroyed.

9 Mitigation of Other Attacks

The BigFix Cryptographic Module 1.0 does not provide mitigation against any commonly known attacks. FIPS 140-2 Level 2 does not require a specific security policy for mitigation of other attacks, except those for which testable requirements are defined in the standard.