BlockMaster

BM-C1000

FIPS 140-2 Security Policy, Level 2

Revision Date: 19th of April 2011.

Firmware Version 4.0

Hardware versions:
BM-C1000-01, BM-C1000-02, BM-C1000-04, BM-C1000-08,

BM-C1000-16, BM-C1000-32, BM-C1000-64

BM-C1000 Device

Table of Contents

1 Introduction

1.1 Purpose

This is a FIPS 140-2 Security Policy for the BM-C1000 cryptographic module. It describes how this module meets all the requirements as specified in the FIPS 140-2 Level 2 requirements. This Policy forms a part of the submission package to the testing lab.

The BlockMaster controller BM9931 powers the BM-C1000 flash drive. All data stored is encrypted within the hardware in accordance with the specification of the Federal Information Processing Standard (FIPS 140-2).

1.2 Document History

Authors	Date	Version	Comment
Anders Pettersson	November 17th, 2009	0.1	
Johan Söderström	April 9th, 2010	0.5	
Johan Söderström	May 17th, 2010	0.6	
Johan Söderström	June 3rd, 2010	0.9	
Johan Söderström	July 23rd, 2010	0.91	
Johan Söderström	Aug 9th, 2010	1.0	
Johan Söderström	Nov 19th 2010	1.1	
Johan Söderström	March 21th, 2011	1.2	
Johan Söderström	April 19th, 2011	1.3	

2 Product Description

BlockMaster's BM-C1000 (firmware version 4.0) provides FIPS 140-2 validated security.

The module implements AES, SHA-1, SHA-256, RSA and ANSI X9.31 RNG.

The product meets the overall requirements applicable to Level 2 security for FIPS 140-2, with EMI/EMC meeting the Level 3 requirements.

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

Table 1 - Module Compliance Table

2.1 Cryptographic Module Specification

The multi-chip embedded module uses flash memory as means of storage of encrypted data. The module support operation of both MLC and SLC NAND flash memory options. The following versions are being submitted for FIPS 140-2 Level 2 Validation.

Part Number	Memory Option	Firmware Version
BM-C1000-01	NAND flash 1GB	4.0
BM-C1000-02	NAND flash 2GB	4.0
BM-C1000-04	NAND flash 4GB	4.0
BM-C1000-08	NAND flash 8GB	4.0
BM-C1000-16	NAND flash 16GB	4.0
BM-C1000-32	NAND flash 32GB	4.0
BM-C1000-64	NAND flash 64GB	4.0

Table 2 - Part Numbers

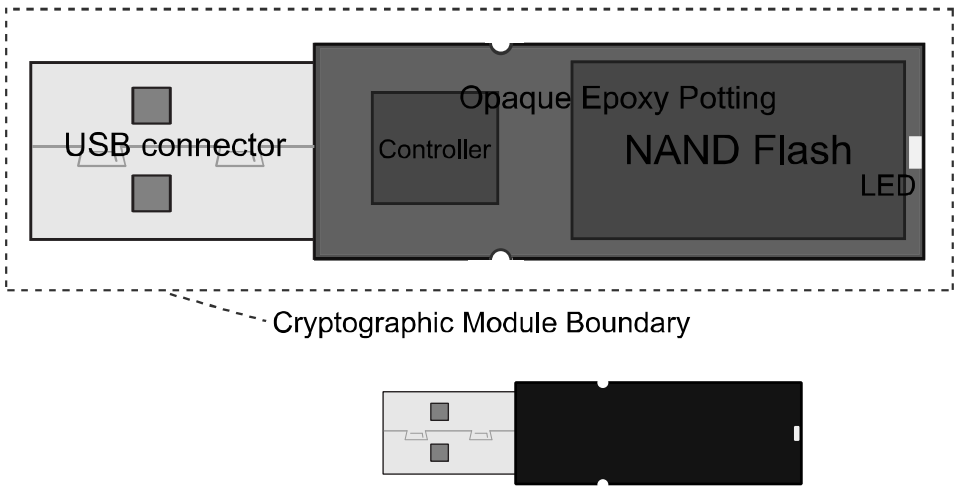

Illustration 1 - Cryptographic Module

Boards with BM9931 controller and flash circuits of variable sizes covered with opaque epoxy rendered semi-transparent in the detail for illustration purposes.

2.1.1 Cryptographic module boundary

Cryptographic module boundary is the outer boundary of the epoxy potting that covers the BM9931 controller and the accompanying flash storage. All cryptographic processes take place in the controller and the flash is a mean of storage with variable capacity. The cryptographic module boundary is protected against tampering by opaque epoxy.

No components are excluded from the requirements of FIPS PUB 140-2.

If the device is connected to a computer via USB a CD-ROM may be displayed. The CD drive contents are outside the cryptographic boundary and is read-only which prevents unauthorized modification and substitution.

OpenSSL is used outside the module boundary to establish a secure TLS connection to the management server. The CryptoOfficer uses the encrypted channel to authenticate and to send commands to the module.

2.1.2 Approved mode of operation

The module only supports an Approved mode of operation. The firmware version can be verified by clicking the 'About' menu option of the host software interface.

3 Module Ports and Interfaces

3.1 Physical Interface Description

The cryptographic module supports the following physical ports and logical interfaces:

Illustration 2 - Pin Assignments for USB Interface

PIN	*Function*	*Logical Interface*
USB 1	V^{BUS} supply voltage 4.5V – 5.5V	Power Interface
USB 2	Data +	Data Input, Data Output, Control Input, Status Output
USB 3	Data -	Data Input, Data Output, Control Input, Status Output
USB 4	Ground	N/A

Table 3 - Functional Specifications of Pin

4 Roles, Services and Authentication

The module supports a Crypto-Officer and a User role that are explicitly assumed by the Crypto-Officer. The module implements identity based authentication using passwords. The module doesn't support a maintenance role.

4.1 Identification and Authentication

The Crypto-Officer is uniquely identified by the explicit authentication against the configuration area of the device using the 7 byte password for write access.

The User is uniquely identified by the explicit authentication against the module using the 16 byte user password.

There can be only one Crypto-Officer for the module.

Role	Type of Authentication	Authentication Data
User	Identity Based	16 byte Password Verification
Crypto Officer	Identity Based	7 byte Password Verification

Table 4 – Authentication Type Table

4.2 Roles and Services

The Product Name 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 below tables shows the services available to each role

Authorized Services	Key/CSP	Access Type	Provided by
Authenticate	Password	Execute	Firmware library
Load configuration data	Password	Write	Firmware library
Set password	Password	Write	Firmware library
Reset	Password	Write	Firmware library
Show status	N/A	Read	Firmware library

Table 5 - Cryptographic Officer – Roles and Services

Service	Key/CSP	Access Type	Provided by
Self-Test	N/A	Execute	Firmware library
Authenticate	password	Execute	Firmware library
Set password	password	Write	Firmware library
Generate Key	DEK	Write	Firmware library
Change Password	password	Write, Execute	Firmware library
Reset	DEK, password	Write	Firmware library
Lock	N/A	Execute	Firmware library
Encryption / decryption	DEK	Execute	Hardware AES engine
Show status	N/A	Read	Firmware library
Set language	N/A	Write	Firmware library
Set password	password	Write	Firmware library

Table 6 - User – Roles and Services

5 Operational Environment

The FIPS 140-2 Operational Environment requirement does not apply. The device contains a limited operational environment.

6 Physical Security

The module is defined as a multi-chip embedded module. The module consists of multiple chips and production grade components on a standard PCB which include standard passivation techniques. The module with all its components is covered in epoxy that provides opacity and tamper evidence against physical attacks.

The epoxy is tamper evident, in that attempts to remove it will show visible damage to the coating itself, and possibly expose the underlying circuitry

6.1 EMI/EMC

The base cryptographic module has been tested and found in compliance with the requirement of the following standards.

FCC Part 15: 2005 Subpart B, Class B. (Section 15.31, 15.107 and 15.109)

CISPR 22: 1997, Class B. (Section 5, 6, 9 and 10)

7 Cryptographic Key Management

The following table summarizes the module's keys and CSP's

Key	type	Generation	Storage	Zeroization	Use
Data encryption key	AES	On board RNG	Plain text	Zeroization command	Used to encrypt/ decrypt data
ANSI X9.31 RNG seed key	Random key	On board RNG	Not stored	either power cycle or Zeroize command	Used to generate the Data encryption key
ANSI X9.31 RNG seed	Random seed	On board RNG	Not stored	either power cycle or Zeroize command	Used to generate the Data encryption key
User Password	Password	Set by user	Hashed SHA-256	Zeroize command	Used to authenticate user to module
Crypto Officer password	Password	Generated outside module boundary	Hashed SHA-256	Zeroize command	Used to authenticate user to module

Table 7 - Cryptographic Keys and CSPs

7.1 Key/CSP entry/output

The module supports password entry and not key output.

The module does not support key archiving.

7.2 Key Generation

The module supports an Approved key generation method conforming to ANSI X9.31. Since the approved RSA function (SigVer with modules size of 1024) only performs a Signature Verification function, it neither generates Public/Private key pairs, or has knowledge of the Private Key and as such it can neither perform or is required to perform the pair-wise consistency test as described in Section 4.9.2 of the FIP 140-2 document.

The module algorithms map to the following algorithms certificates:

Approved or allowed Security Function	Certificate Number
AES (CBC and ECB (enc/dec; 128 and 256))	#1236
SHA-1 and SHA-256, byte-oriented	#1134
ANSI X9.31 RNG (256 AES)	#683
RSA-1024 (PKCS1.5 – Sig Ver.)	#617

Table 8 - FIPS Approved Algorithms

Non-Approved Security Function	Description
Non Deterministic H/W RNG	For seeding the approved DRNG.
RSA (512 bit Modulus)	Used to encrypt the communication channel between the module (hardware device) and the host PC application during the authentication process only and should be considered as a plaintext-function from a FIPS 140-2 perspective.

Table 9 - Non Approved Algorithms

7.3 Zeroization

Zeroization can only be performed if the module is powered on.

Zeroization will erase all encryption keys, and CSPs

8 Self-test

The module automatically performs the following self tests at power on without operator intervention:

Cryptographic Algorithm KATs:

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

- AES (CBC mode Encrypt/Decrypt)
- SHA-1
- SHA-256
- RNG KAT
- RSA-1024

Firmware Integrity Tests:

The module checks the integrity of its various components using 16 bit CRC at power up.

Conditional Tests:

The module performs the following conditional self-tests:

- Continuous RNG Test for the ANSI X9.31 RNG
- Continuous RNG test for the H/W RNG

Self test errors:

If any of the self tests fails the module will enter a 'Self test error' state and all data input / output will be disabled and no cryptographic operations can be performed.

The user interface will present the operator with an error message and the status output LED will blink in 16 hertz

Self tests on demand:

To perform the self tests on demand the operator should power cycle the module

9 Crypto-Officer and User Guidance

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

9.1 Secure Setup and Initialization

1. The user must first set a password; and
2. Register the module with the server

At this point, the server will Set a Crypto-Officer Password
Load configuration data / Security Policy on the module

9.2 Zeroization of Keys and CSPs

The user must choose the factory reset command to initialize zeroization of keys
The module will erase all encryption keys, authentication data and configuration data
The module will generate a new seed, seed key and data encryption key using the on board RNG
The user is prompted to choose a new password

9.3 Zeroization

When the device is reset using the reset command, the following keys and CSP's will be cleared and erased from flash and replaced with new information.

- Data encryption key
- User password
- Crypto Office Password

9.4 Maintain physical security

The Crypto Officer should check the module for tamper evidence periodically by examining that the epoxy is intact and that the circuitry is not exposed to ensure that the device have not been tampered with.

10 Mitigation of Other Attacks

The module does not mitigate against any specific attacks.