# MHZ2 CJ series of

# 2.5" inch hard disk drive with automatic hardware based encryption

# Security Policy

Rev. 1.0
2009/02/02

FUJITSU LIMITED

# List of contents

# Revision record

| Rev. | Date | Descriptions |
|---|---|---|
| 01 | 2009/02/2 | Newly established |
| | | |
| | | |
| | | |

## 1. Overview

This document describes the Security policy for the Fujitsu Limited, 2.5" HDD with hardware-based encryption, models as shown in Table-1.

Table-1 2.5" HDD with hardware-based encryption

| Unit | | Firmware | | Product Spec. | |
|---|---|---|---|---|---|
| Part Number | Revision | Model | Revision | Capacity | SATA transfer rate |
| CA07062-B901 | A1、A2 | MHZ2080CJ G1 | 0000801F | 80GB | 1.5Gbps |
| CA07062-B218 | A1、A2 | | | | |
| CA07062-B903 | A1、A2 | MHZ2120CJ G1 | 0000801F | 120GB | 1.5Gbps |
| CA07062-B222 | A1、A2 | | | | |
| CA07062-B904 | A1、A2 | MHZ2160CJ G1 | 0000801F | 160GB | 1.5Gbps |
| CA07062-B226 | A1、A2 | | | | |
| CA07062-B906 | A1、A2 | MHZ2200CJ G1 | 0000801F | 200GB | 1.5Gbps |
| CA07062-B230 | A1、A2 | | | | |
| CA07062-B908 | A1、A2 | MHZ2250CJ G1 | 0000801F | 250GB | 1.5Gbps |
| CA07062-B245 | A1、A2 | | | | |
| CA07062-B909 | A1、A2 | MHZ2320CJ G1 | 0000801F | 320GB | 1.5Gbps |
| CA07062-B242 | A1、A2 | | | | |
| CA07062-B911 | A1、A2 | MHZ2080CJ G2 | 0000801F | 80GB | 3.0Gbps. |
| CA07062-B248 | A1、A2 | | | | |
| CA07062-B913 | A1、A2 | MHZ2120CJ G2 | 0000801F | 120GB | 3.0Gbps. |
| CA07062-B252 | A1、A2 | | | | |
| CA07062-B914 | A1、A2 | MHZ2160CJ G2 | 0000801F | 160GB | 3.0Gbps. |
| CA07062-B256 | A1、A2 | | | | |
| CA07062-B916 | A1、A2 | MHZ2200CJ G2 | 0000801F | 200GB | 3.0Gbps. |
| CA07062-B260 | A1、A2 | | | | |
| CA07062-B918 | A1、A2 | MHZ2250CJ G2 | 0000801F | 250GB | 3.0Gbps. |
| CA07062-B275 | A1、A2 | | | | |
| CA07062-B919 | A1、A2 | MHZ2320CJ G2 | 0000801F | 320GB | 3.0Gbps. |
| CA07062-B272 | A1、A2 | | | | |

The Unit Hardware Versions were specified by the configuration of both Part Numbers and Unit Revisions.

This Security policy states that the cryptographic module meets the overall requirements applicable to Level 1 security of JIS X 19790.

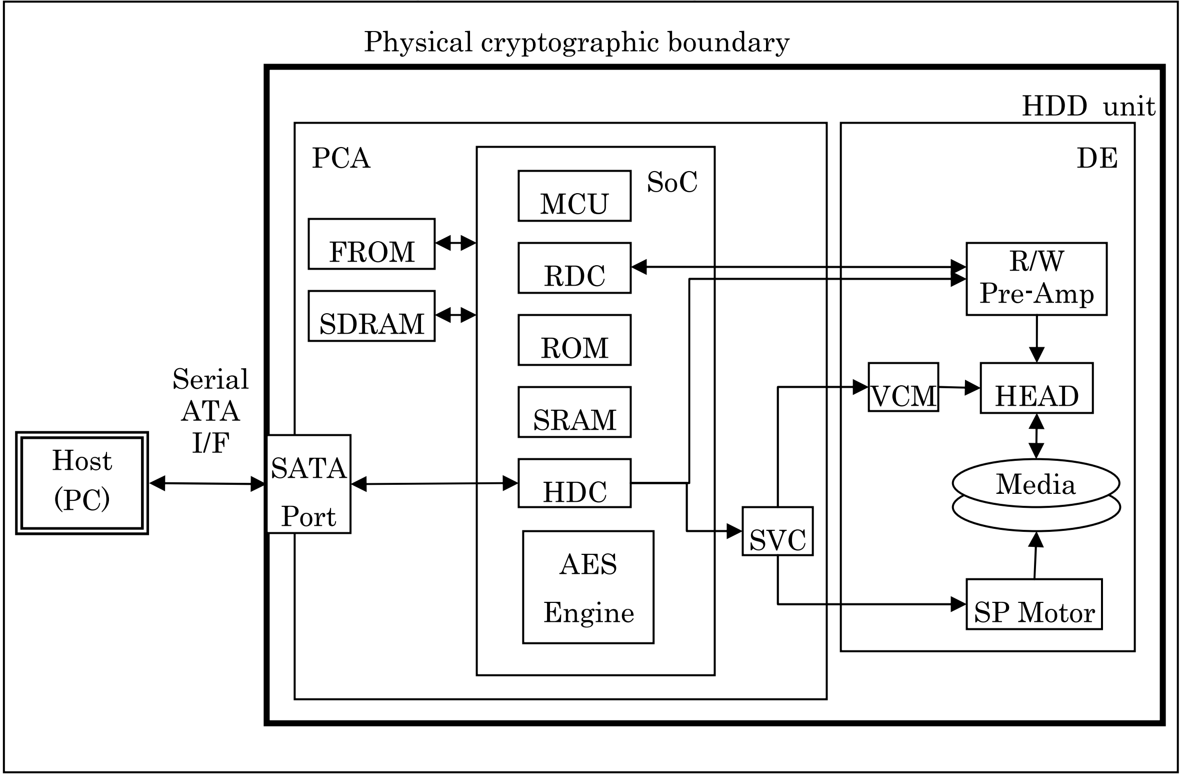
## 2. Cryptographic Module Specification

### (1) Product Overview

The MHZ2 CJ series 2.5” HDD with hardware-based encryption has a Serial ATA interface which is in accordance with AT Attachment 8, Serial ATA spec. R2.6. The HDD is structured with hardware and firmware and is categorized as a Multiple-Chip Embedded Cryptographic Module.

### (2) Hardware configuration

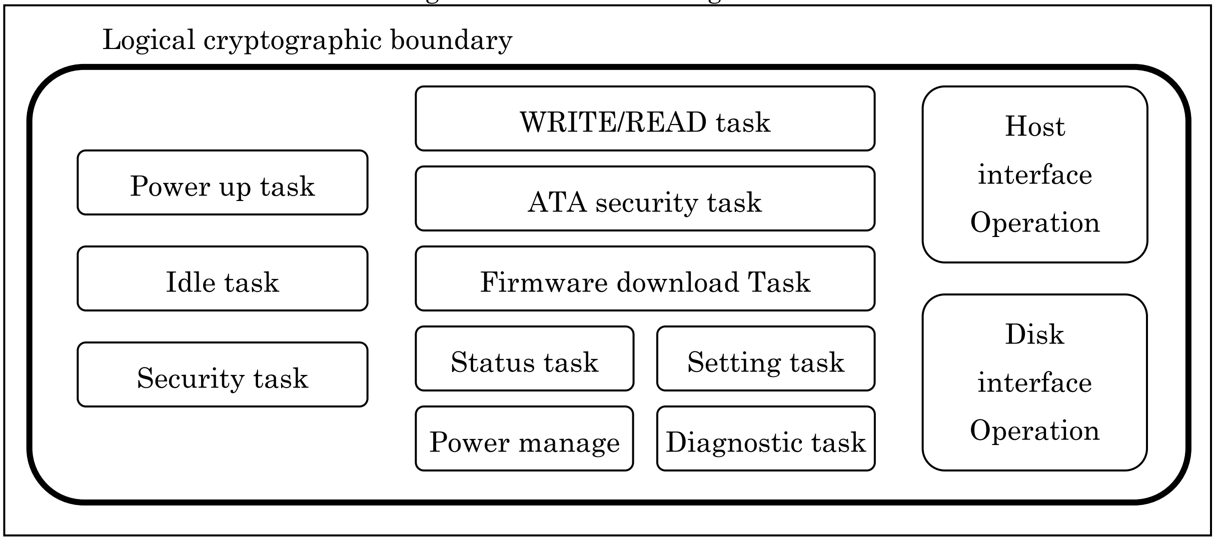
Fig.-1 Hardware configuration



- ■ PCA : Printed circuit assembly
- ■ DE : Disk Enclosure
- ■ SVC : Servo Combo
- ■ HDC : Hard Disk Controller
- ■ RDC : Read Channel
- ■ SP Motor : Spindle Motor
- ■ VCM : Voice Coil Motor

### (3) Firmware configuration

Fig. -2 Firmware configuration



### (4) Secure function and operational modes

The cryptographic module has the following secure functions.

Table-2 Security functions

| Function | Algorithm | Specification |
|---|---|---|
| Encryption / Decryption | AES-256 | FIPS PUB 197 |
| Hash | SHA-256 | FIPS PUB 180-2 with Change Notice 1 |
| Message Authentication | CMAC(AES-256) | NIST Special Publication 800-38B |
| Random bit generation | Hash_DRBG(SHA-256) | NIST Special Publication 800-90 |

- The cryptographic module always operates in the approved mode of operation after booting.
- The cryptographic module does not have PSP.
- The Random bit generate algorithm is vendor affirmed.

### (5) Security level

The cryptographic module meets the security level shown in Table-3 in each security requirements area. And its overall level is 1.

Table-3 Security level

| Security Requirements Area | Level |
|---|---|
| Cryptographic Module Specification | 1 |
| Ports and Interface | 1 |
| Roles, Services and Authentication | 1 |
| Finite State Model | 1 |
| Physical Security | 1 |
| Operational Environment | N/A |
| Cryptographic Key Management | 1 |
| Self Test | 1 |
| Design Assurance | 1 |
| Mitigation of Other Attacks | N/A |

## 3. Port and Interface

### (1) Physical Port

The cryptographic module has one Serial ATA port.

### (2) Logical Interfaces

All Logical Interfaces belong to the Serial ATA port.

Table-4 Logical Interface

| Logical Interfaces | Physical Port |
|---|---|
| Data Input | Serial ATA Port |
| Data Output | Serial ATA Port |
| Control Input | Serial ATA Port |
| Status Output | Serial ATA Port |
| Power | Serial ATA Port |

### (3) ATA commands

The data transaction protocol between the cryptographic module and the outside host use the host attachment interface as defined by AT Attachment8, Serial ATA R2.6. The cryptographic module operates as a dependent module as controlled by the host.

## 4. Roles, Services and Authentications

### (1) Roles

The cryptographic module supports both a User Role and a Crypto Officer Role.

a) User Role

The role for access to user data on the cryptographic module. User Role shall be implicitly assumed while performing services other than the initialization of data cryptographic key and Firmware download.

b) Crypto Officer Role

The role for initialization of data cryptographic key and Firmware download. Crypto Officer Role shall be implicitly assumed for initialization of data cryptographic key and Firmware download.

### (2) Services

The cryptographic module supports the mandatory functions specified in AT Attachment 8, Serial ATA spec. R2.6 and its optional functions and vendor unique setting/diagonal functions.

The services which are supported by the cryptographic module are shown in Table-5. There are security functions and CSP access status for each service in the table. The roles that can perform each service are also indicated in the table.

Table-5 Services

| Item | Services | Security Function | CSP Access | User Role | Crypto Officer Role |
|---|---|---|---|---|---|
| User Command | WRITE command | AES encryption | Data cryptographic key reference | o | - |
| | READ command | AES decryption | Data cryptographic key reference | | |
| | ATA security password management command | SHA Hash<br>AES encryption | Data password entry<br>Data password setting or matching<br>Data cryptographic key matching | | |
| | Status command | — | — | | |
| | Setting command | — | — | | |
| | Diagnostic command | — | — | | |
| | Power manage command | — | — | | |
| Crypto Officer Command | Data cryptographic key initialization command | SHA Hash<br>AES encryption<br>Random bit generate | Data password entry<br>Data password patching<br>Random bit generation and reference<br>Data cryptographic key regeneration | - | o |
| | Firmware download command | CMAC message authentication<br>SHA Hash<br>AES decryption | Download password entry<br>CMAC key reference<br>Firmware decrypt graphic key refer | | |

### (3) Authentications

There is no authentication for an operator accessing the module. There is no mechanism to enforce that the operations being performed are confined to a role.

User Role and Crypto Officer Role shall be selected implicitly.

When ATA security function is enabled, user data is protected by ATA password within ATA security function area.

## 5. Physical security

The product is a Multiple-Chip Embedded Cryptographic Module, and meets the security requirement of JIS X 19790 physical security Level 1.

## 6. Operational Environment

The cryptographic module executes within the limited operational environment. Therefore the security requirements for operation environment are not applicable.

## 7. Cryptographic Key Management

### (1) Random Bit Generator (RBG)

The cryptographic module uses RBG for data Key generation/initialization. RBG and its operation mode are adopted based on JCMVP Implementation Guidance (JIG-01 August. 7th 2008) and conform to NIST Special Publication 800-90.

### (2) Key establishment and Key output

The cryptographic module does not use key establishment and does not perform Key output.

### (3) Key Generation, Key entry, Key storage and Key zeroization

Table-6 Key management

| CSP | Key generation, Key entry, Key storage and Key zeroization |
|---|---|
| Data cryptographic key | Used for user data encryption and decryption.<br>Generated by Random bit generator<br>Stored in the area inaccessible from operator after being encrypted by the data password in the module.<br>Set with zeroization by data cryptographic key initialization command. |
| Data password | Used for confirmation of user data access authentication and data cryptographic key encryption.<br>Entered from host system through the ATA security command as plaintext, and stored in RAM.<br>After performing command task with data password, the plaintext data password in the RAM shall be erased. |
| Data password authentication data | Used for confirmation of user data access authentication.<br>The data password entered from the host system as plaintext through the ATA Security Set Password command shall be hashed and stored in the area inaccessible from operator.<br>It cannot be zeroized by operator. |
| Firmware MAC key | Used for authentication of downloaded firmware.<br>This is generated at the develop stage and encrypted by using the download password. It shall be stored in the area inaccessible from operator.<br>It cannot be zeroized by operator. |
| Download password | Used for encrypting the Firmware MAC key and Firmware decrypt cryptographic key, and generated at the development stage.<br>This is entered from host system as plaintext at firmware download, and shall be deployed in the RAM.<br>It shall be erased from the RAM after completion of firmware download command execution. |
| Firmware decrypt graphic key | Used for decryption of downloaded firmware.<br>This is generated at the development stage and encrypted by using the download password. It shall be stored in the area inaccessible from operator.<br>It cannot be zeroized by operator. |
| Random data | Internal data for using Random bit generation.<br>Generated by entropy.<br>Stored in the RAM<br>It shall be Zeroized after completion of the Random Bit Generation. |

## 8. Self-Tests

### (1) Power up Self-Tests

The cryptographic module starts Power up Self-Test when powered on. The operator is able to start the Power up Self-Tests on demand by powering the cryptographic module off then on. The cryptographic module performs the following Power up Self-tests.

a) Cryptographic algorithm test

Table-7 Cryptographic algorithm test

| Function | Algorithm | Test |
|---|---|---|
| Encryption / Decryption | AES-256 | Known-answer test |
| Hash | SHA-256 | Known-answer test |
| Message Authentication | CMAC | Known-answer test |
| Random bit generation | Hash_DRBG | Known-answer test |

b) RBG entropy test

Performs minimum entropy evaluation.

c) Firmware integrity test

The firmware has 32bit CRC, and shall be verified when loaded from store device to RAM.

d) Critical Functional Test

Bus testing on MPU bus, Write/Read test for internal register and work area RAM and Write/Read test on data buffers are performed.

### (2) Conditional Self Tests

The cryptographic module performs the following conditional tests whenever the security function is performed.

Firmware download test

The firmware to be downloaded has CMAC as the message authentication.

Continous Random Bit Generator test (RBG test)

Confirms that the newly generated block shall not be equal to the previous generated block.
Performs the self test required by NIST Special Publication 800-90.

## 9. Design Assurance

The cryptographic module has the following document.

- MHZ2080 CJ, MHZ2120 CJ, MHZ2160 CJ, MHZ2200 CJ, MHZ2250 CJ, MHZ2320 CJ DISK DRIVES PRODUCT/MAINTENANCE MANUAL.

  This document is subsequently referred to as the "product manual."

### (1) Configuration Management and Development

The functional specification of the cryptographic module is described in the product manual.

The configuration management and development are controlled based on a quality management system certified by ISO9001:2000.

### (2) Delivery and Operation

The cryptographic module shall be installed into a host system such as a PC. The product manual describes the following items.

- Installation of HDD (the cryptographic module).
- Host side Power-on method.
- Host command interface including data password entry.

### (3) Guidance Documents

The guidance information is provided within the product manual. Both the Crypto Officer guidance and the User guidance are contained in the manual.

## 10. Mitigation of other attacks

The cryptographic module does not claim to mitigate other attacks.

## 11. References

(1) JIS X 19790 : 2007 Security techniques -- Security requirements for cryptographic modules.

(2) JIS X 5091:2007 Security techniques -- Security test requirements for cryptographic modules.

(3) IPA Approved Security Functions. (ASF-01) April. 7th 2008.

(4) IPA JCMVP Cryptographic Algorithm implementation Testing Requirements (ATR-01) October. 29th 2007.

(5) IPA JCMVP Implementation Guidance (JIG-01) August. 7th 2008

(6) FIPS PUB 197, Advanced Encryption Standard (AES), November 26, 2001

(7) FIPS PUB 180-2 with Change Notice 1, Secure Hash Standard, February 25, 2004.

(8) Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, National Institute of Standards and Technology Special Publication 800-38B, May 2005.

(9) Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised), National Institute of Standards and Technology Special Publication 800-90, March 2007.