

# Cryptographic Module Validation Certificate

Certificate No. J0006



Cryptographic Module Name : **MHZ2 CJ Series of 2.5inch hard disk drive with automatic hardware-based encryption**

Version :

Hardware Version : CA07062-B901 A1, CA07062-B218 A1, CA07062-B903 A1, CA07062-B222 A1, CA07062-B904 A1, CA07062-B226 A1, CA07062-B906 A1, CA07062-B230 A1, CA07062-B908 A1, CA07062-B245 A1, CA07062-B909 A1, CA07062-B242 A1, CA07062-B911 A1, CA07062-B248 A1, CA07062-B913 A1, CA07062-B252 A1, CA07062-B914 A1, CA07062-B256 A1, CA07062-B916 A1, CA07062-B260 A1, CA07062-B918 A1, CA07062-B275 A1, CA07062-B919 A1, CA07062-B272 A1, CA07062-B901 A2, CA07062-B218 A2, CA07062-B903 A2, CA07062-B222 A2, CA07062-B904 A2, CA07062-B226 A2, CA07062-B906 A2, CA07062-B230 A2, CA07062-B908 A2, CA07062-B245 A2, CA07062-B909 A2, CA07062-B242 A2, CA07062-B911 A2, CA07062-B248 A2, CA07062-B913 A2, CA07062-B252 A2, CA07062-B914 A2, CA07062-B256 A2, CA07062-B916 A2, CA07062-B260 A2, CA07062-B918 A2, CA07062-B275 A2, CA07062-B919 A2, CA07062-B272 A2

Firmware Version : 0000801F

Software Version : N/A

Physical Embodiment : Multiple-Chip Embedded

Security Requirements : JIS X 19790:2007

Testing Requirements : JIS X 5091:2007, JCMVP Cryptographic Algorithm implementation Testing Requirements October 29<sup>th</sup> , 2007

Vendor : Toshiba Corporation

Address of Vendor : 1-1, Shibaura 1-chome, Minato-ku, Tokyo 105-8001, Japan

Special Affairs : Date of Validation : October 27, 2008; Date of the first issue : February 19, 2009

Notes : The cryptographic module identified in this certificate has been tested at an accredited Cryptographic Module Testing Laboratory in the Japan Cryptographic Module Validation Program, and the testing results have been validated in accordance with the Cryptographic Module Testing Requirements. This certificate applies only to the specific version of the Cryptographic Module in its tested configurations and operational environments. The Cryptographic Module Tests have been conducted in accordance with the provisions of the Japan Cryptographic Module Validation Program and the conclusions of the testing laboratory in the testing report are consistent with evidence adduced. This certificate is not an endorsement of the cryptographic module by the Information-technology Promotion Agency or by any other organization that recognizes or gives effect to this certificate, and no warranty of the cryptographic module by the Information-technology Promotion Agency or by any other organization that recognizes or gives effect to this certificate, is either expressed or implied.

The misuse of this certificate, including the use of certificate for publications, such as advertisements and catalogs, in an incorrect or misleading manner may result in withdrawal of this certificate.

Signature : **Original Signed** Date : January 29, 2010

Name : Koji Nishigaki

Title : Chairman

**INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN**



# Cryptographic Module Validation Report

The cryptographic module identified in this report has been validated in the following.

Cryptographic Module Name: [MHZ2 CJ Series of 2.5inch hard disk drive with automatic hardware-based encryption](#)

**Version: Hardware:** [CA07062-B901 A1](#), [CA07062-B218 A1](#), [CA07062-B903 A1](#), [CA07062-B222 A1](#), [CA07062-B904 A1](#), [CA07062-B226 A1](#), [CA07062-B906 A1](#),  
[CA07062-B230 A1](#), [CA07062-B908 A1](#), [CA07062-B245 A1](#), [CA07062-B909 A1](#), [CA07062-B242 A1](#), [CA07062-B911 A1](#), [CA07062-B248 A1](#), [CA07062-B913 A1](#), [CA07062-B252 A1](#),  
[CA07062-B914 A1](#), [CA07062-B256 A1](#), [CA07062-B916 A1](#), [CA07062-B260 A1](#), [CA07062-B918 A1](#), [CA07062-B275 A1](#), [CA07062-B919 A1](#), [CA07062-B272 A1](#), [CA07062-B901 A2](#),  
[CA07062-B218 A2](#), [CA07062-B903 A2](#), [CA07062-B222 A2](#), [CA07062-B904 A2](#), [CA07062-B226 A2](#), [CA07062-B906 A2](#), [CA07062-B230 A2](#), [CA07062-B908 A2](#), [CA07062-B245 A2](#),  
[CA07062-B909 A2](#), [CA07062-B242 A2](#), [CA07062-B911 A2](#), [CA07062-B248 A2](#), [CA07062-B913 A2](#), [CA07062-B252 A2](#), [CA07062-B914 A2](#), [CA07062-B256 A2](#), [CA07062-B916 A2](#),  
[CA07062-B260 A2](#), [CA07062-B918 A2](#), [CA07062-B275 A2](#), [CA07062-B919 A2](#), [CA07062-B272 A2](#) **Firmware:** 0000801F

Accredited Cryptographic Module Testing Laboratory: [Information-Technology Promotion Agency, Japan](#)

CRYPTIPA Version: [1.1.0](#)

<i>Cryptographic Module Specification :</i>	Level 1	<i>Cryptographic Module Ports and Interfaces :</i>	Level 1
<i>Roles, Services, and Authentication :</i>	Level 1	<i>Finite State Model :</i>	Level 1
<i>Physical Security : (Multiple-Chip Embedded)</i>	Level 1	<i>Operational Environment :</i>	Level <a href="#">N/A</a>
<i>Cryptographic Key Management :</i>	Level 1	<i>EMI/EMC :</i>	Level <a href="#">N/A</a>
<i>Self-Tests :</i>	Level 1	<i>Design Assurance :</i>	Level 1
<i>Mitigation of Other Attacks :</i>	Level <a href="#">N/A</a>		

tested in the following configuration(s):

OS: Microsoft Windows 98[Version 4.10.2222], Mother Board: Intel DG33FB, CPU: Intel Core2 Duo E6550@2.33GHz, FDD: 1.4MB, Memory: 2GB  
Cryptographic Module: FUJITSU MHZ2080CJ G1 (CA07062-B901-A1), FUJITSU MHZ2320CJ G2 (CA07062-B272-A1)

**Overall Level Achieved : 1**

The following Approved Cryptographic Algorithms are used: [AES\(Cert.#6\)](#), [SHS\(Cert.#6\)](#), [Hash\\_DRBG](#) in [NIST SP800-90\(Vendor Affirmed\)](#)

The cryptographic module also contains the following non approved algorithms: [N/A](#)

Test Results: [Pass](#)

The cryptographic module identified in this report has been tested on the basis of the testing requirements specified by the Japan Cryptographic Module Validation Program, and has achieved the scope of conformance to the specified security requirements from the test results.

Signature: Original Signed Date: February 19,2009

Name: Koji Nishigaki

Title : Chairman



**INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN**