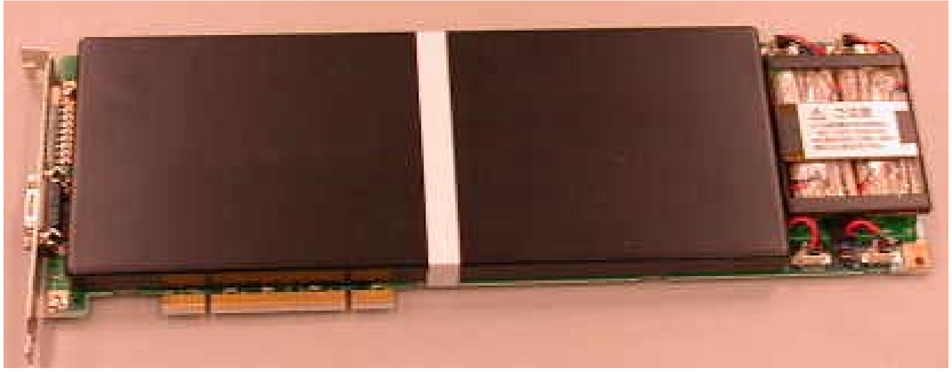
TurboMISTY

(Firmware Version 2.1.3
Hardware Version 1.01)



FIPS 140-2 Non-Proprietary Security Policy

Level 3 Validation
Version 2.6

November 5, 2003

TABLE OF CONTENTS

INTRODUCTION

Purpose

This is a non-proprietary Cryptographic Module Security Policy for the TurboMISTY cryptographic accelerator card from Mitsubishi Electric. This security policy describes how the TurboMISTY meets the security requirements of FIPS 140-2 and how to run the TurboMISTY in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 3 FIPS 140-2 validation of the TurboMISTY.

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 CMVP website at http://csrc.nist.gov/cryptval/.

References

This document deals only with operations and capabilities of the TurboMISTY in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the TurboMISTY from the following sources:

The Mitsubishi Electric Corporation website (http://www.mitsubishielectric.com): contains information on the full line of products from Mitsubishi Electric Corporation

The CMVP Validated Modules website (http://csrc.ncsl.nist.gov/cryptval/): contains contact information for answers to technical or sales-related questions for the TurboMISTY

Document Organization

The Security Policy document is one document in a complete FIPS 140-2 Submission Package. In addition to this document, the complete Submission Package contains:

Vendor Evidence document

Finite State Machine

Module Source Code Listing

Crypto Officer/User Guidance

Other supporting documentation as additional references

This Security Policy and the other validation submission documentation was produced by Corsec Security, Inc. under contract to Mitsubishi Electric Corporation. With the exception of this Non-Proprietary Security

Policy, the FIPS 140-2 validation submission documentation is proprietary to Mitsubishi Electric Corporation and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Mitsubishi Electric Corporation.

MITSUBISHI TURBOMISTY

Overview

The Mitsubishi TurboMISTY is a high-end PCI card that provides cryptographic services and secure storage of cryptographic keys. The module is built to perform cryptographic processing and features a tamper-responsive case to physically protect sensitive information contained within the card.

The TurboMISTY is designed to support eight logical operator slots. Each of these slots supports two operators of the module, a User and a Security Officer. Permissions can be set for each slot separately.

The TurboMISTY supports a number of cryptographic algorithms, including the following algorithms approved for use in a FIPS mode of operation:

- RSA signature generation and verification
- DES (for legacy use only) and Triple-DES encryption and decryption
- SHA-1 hashing

Cryptographic Modules

The Mitsubishi TurbMISTY is classified as a multi-chip embedded module for FIPS 140-2 purposes. The FIPS 140-2 cryptographic boundary is the entire TurboMISTY module, excluding the batteries and power regulation chips on the back of the board.

Module Interfaces

The physical ports for the TurboMISTY are listed as follows:

PCI Port

LEDs

Power interfaces from batteries

RS-232 port (unused)

All of these physical ports are separated into the logical interfaces from FIPS as described in the following table:

FIPS 140-2 Logical Interface	Module Mapping
Data Input Interface	PCI port
Data Output Interface	PCI port
Control Input Interface	PCI port

FIPS 140-2 Logical Interface	Module Mapping
Status Output Interface	LEDs, PCI port
Power Interface	Battery interface, PCI port

Table 1 – FIPS 140-2 Logical Interface

Roles and Services

The TurboMISTY performs identity-based authentication. Operators are identified by a username and authenticate with a password. During authentication, an operator selects their role by specifying their user type.

The strength of the authentication mechanism with 82 possible characters with repetition and a minimum of a 6-character password is 1 in 304006671424 (82^6). The board delays a reply for five seconds when an incorrect password is entered.

Status

Status of the TurboMISTY can be viewed from function calls/returns from the firmware, the TurboMISTY client application, and through the LEDs located on the back of the module. Status allows the Crypto Officer to recognize if the module is operating properly or needs maintenance.

Each main TurboMISTY function provides a returnCode through the PCI interface. The returnCode provides status both to the Manager and to the library of PKCS #11 conversion functions.

The module has 8 LEDS, which provide the following status indications.

LED Number	Item
0	Battery voltage drop
1	Mechanical switch detection (cover removed)
2	Slot removed
3	Optical sensor detection
4	Error state
5	Permission to pull out board
6	Mechanical switch error
7	Power-up self-tests passed

Table 2 – LEDs

A simple way to view the status of the module is through the TurboMISTY Manager software, which communicates with the module using function calls. In this tool, an operator can view the status of the module under the “State.” The content of the display is as follows.

1. State of operation

a. When normally operating "Normal"

b. When user password is locked "User PIN (password) lock"

c. Stored secret key has been zeroized by unauthorized means: "Secret key check error"

d. When an internal error occurs "*** the test error" (*** RSA etc.)

2. Number of use sessions

   The number of sessions which have been opened to TURBOMISTY is displayed from the application. The number of applications in the PKCS#11 library in the state of log in is displayed. Minimum value becomes one because the Crypto Officer uses one of the sessions to access the TurboMISTY through the TurboMISTY Manager. The maximum value is 256.

3. State of battery

   Either "100%-10% remainder", "10%-5% remainder" or "Less than remainder amount 5%" is displayed. Please exchange the battery promptly when "10%-5% remainder" is displayed.

4. Initial setup date

   The date when TURBOMISTY was initialized is displayed.

5. Version

   The version of hardware and the firmware is displayed.

Crypto Officer and User Roles

The Security Officer role specified in the TurboMISTY documentation directly maps to the Crypto Officer role required by FIPS 140-2. The services available to the Crypto Officer role and the User role are as follows:

Service	**Description**	**Role(s)**	**CSP**	**Type of Access to CSP**
Initialize	Initializes a slot	Crypto Officer	3DES authentication key	Read
			3DES session key	Write, Read
Initialize password	Initializes an operator’s password	Crypto Officer	Password	Write
			3DES session key	Read
			3DES authentication key	Write

Service	Description	Role(s)	CSP	Type of Access to CSP
Change passwords	Changes an operator's password	Crypto Officer, User	Password	Write
			3DES session key	Read
			3DES authentication key	Write
Login	Logs an operator into the module and establishes a session key	N/A	3DES authentication key	Read
			3DES session key	Write
Create object	Creates an object	User	RSA private key, 3DES key, DES key	Write
			3DES session key	Read
Copy object	Creates a copy of an object	User	RSA private key, 3DES key, DES key	Write
			3DES session key	Read
Find objects	Performs an object search	User	3DES session key	Read
Destroy object	Destroys an object	User	3DES session key	Read
Encrypt	Performs encryption using a symmetric key (DES, TDES)	User	3DES key, DES key	Read
			3DES session key	Read
Decrypt	Performs decryption using a symmetric key (DES, TDES)	User	3DES key, DES key	Read
			3DES session key	Read
Hash	Generates a SHA-1 hash	User	3DES session key	Read
Sign	Generates a digital signature using RSA	User	RSA private key	Read
			3DES session key	Read
Verify	Verifies a digital signature using RSA	User	3DES session key	Read
Generate new key(s)	Generates a key (DES, TDES) or key pair (RSA). The FIPS-approved PRNG from FIPS 186-2 Appendix 3.1 (G function suing SHA-1) is used to generate the key or seed the generation mechanism.	User	3DES key, DES key, RSA public/private key pair	Write
			3DES session key	Read
Random number generation	Generates a random number using the FIPS-approved PRNG from FIPS 186-2 Appendix 3.1 (G function using SHA-1).	User	3DES session key	Read
Get attribute value	Obtains an attribute value of an object	User	3DES key, DES key	Write
			3DES session key	Read
Set attribute value	Modifies an attribute value of an object	User	3DES session key	Read
Wrap key	Wraps (encrypts) a key	User	RSA private key	Write
			3DES key	Read
			3DES key, DES key	Write
			3DES session key	Read
Unwrap key	Unwraps (decrypts) a key	User	RSA private key	Write
			3DES key	Read
			3DES key, DES key	Write
			RSA private key	Read
			3DES session key	Read

Service	Description	Role(s)	CSP	Type of Access to CSP
Logout	Logs an operator off of the module.	Crypto Officer, User	3DES session key	Read
Close session	Closes a session	Crypto Officer, User	3DES session key	Read
Close all sessions	Closes all sessions with a token	Crypto Officer, User	3DES session key	Read

Table 3 – Roles and Services

Unauthenticated Services

The TurboMISTY also supports the following unauthenticated services from PKCS#11:

- C_GetSlotInfo() – Obtains information about a particular slot
- C_GetTokenInfo() – Obtains information about a particular token

Finite State Machine Model

The TurboMISTY is designed around a Finite State Machine (FSM) which is detailed in a proprietary document (*Mitsubishi TurboMISTY FIPS 140-2 Finite State Machine – Level 3 Validation*). Parties interested in reviewing this document should contact Mitsubishi via the sources listed in the Introduction section of this document.

Physical Security

This board has tamper detect and response functionality to prevent illegal access to stored secret information.

The TurboMISTY is enclosed in a metal case and sealed with a tamper evidence label from the factory. The tamper evidence label has a special adhesive backing to adhere to the module's painted surface. Removing the cover of the board will damage the tamper evidence label.

External physical access is detected by several sensors, and stored secret information is erased.

- Detection of removal of circuit cover: A mechanical detection switch detects the circuit cover being opened.

- Detection of removal of PCI slot: Removal of the card from its PCI slot is detected

- Detection of hole in circuit cover: A photosensor detects a break in the circuit cover.

- Detection of residual amount of batteries: Battery voltage drop to a certain level is detected, and stored secret information is erased.

Note: Detection of the removal of the module from its PCI slot is configurable by the Crypto-Officer. This mechanism only provides physical security if it has been enabled so that the card cannot be removed from its PCI slot without tamper-response.

Operational Environment

This section does not apply. The TurboMISTY does not provide a modifiable operational environment.

Cryptographic Key Management

The module supports the following FIPS approved algorithms: DES (to be used in legacy systems only), 3DES, RSA, and SHA-1. The module also supports MD5 and MISTY1, which are not FIPS-approved algorithms and are not available when the TurboMISTY is operating in FIPS mode.

The CSPs used for the TurboMISTY are:

1. RSA private keys

2. DES/3DES keys

3. MISTY keys

4. Passwords

User RSA keys are RSA keys used by operators to sign/verify data. Public keys may be output, but private keys are never output unless they are wrapped with 3DES using the function MKDS_BackupKey(). Only the User role has access to RSA public/private keys.

DES and 3DES algorithms are supported for the block cipher cryptosystem. The board uses a dedicated LSI to encrypt (decrypt) text at a high speed using an encryption key up to 168 bits long. User 3DES keys are used by operators to encrypt/decrypt data and to authenticate. The module generates DES or 3DES keys using a FIPS-approved RNG for session keys. DES and 3DES keys are only output during the key transport to establish sessions (RSA encrypted) and wrapped with RSA using MKDS_BackupKey(). Only the User role has access to control DES/3DES keys such as key generation. User 3DES keys are used by operators to encrypt/decrypt data and to authenticate and User DES keys may be used in legacy systems to encrypt/decrypt data.

Passwords are used by operators to authenticate. Both the Crypto Officer and User have access to their own passwords created upon initializing the TurboMISTY board and these passwords are never output. The passwords of both the User and Crypto Officer can be created and changed by the Crypto Officer using the TurboMISTY Manager.

Random Number Generator

The module uses the FIPS-approved RNG specified in FIPS 186-2 DSA-RNG Appendix 3.1 with the underlying G function using SHA-1for generation of cryptographic keys.

Key Storage

This board uses a battery-backed up SRAM to store secret information on internally generated secret keys. To access the SRAM, the password must be written in the access permission register in the FPGA in each access cycle.

RSA private keys and passwords are stored in the SRAM. RSA public keys, DES keys, and 3DES keys are stored in SDRAM. The RSA public key used for key transport is stored in ROM. RSA private/public keys, 3DES and DES keys, and passwords are stored in plaintext.

Key Zeroization

If any of the following external physical access is detected by several sensors, the stored secret information is erased.

1. Detection of removal circuit cover

2. Detection of removal of PCI slot

3. Detection of hole in circuit cover

4. Detection of residual amount of batteries

Note: Zeroization upon detection of the removal of the module from its PCI slot is configurable by the Crypto-Officer.

EMI/EMC

The module conforms to FCC Part 15 Class B requirements for home use.

Self-Tests

The TurboMISTY includes all FIPS-required self-tests at Level 3 validation. More detail about the specific self-tests can be found below.

Known Answer Tests

The self-test run at power-up includes a cryptographic known answer test (KAT) on the FIPS-approved cryptographic algorithms (DES, 3DES, RSA, SHA-1) and the FIPS-approved random number generator.

Random Number Generator Tests

The module includes a continuous test on the output from the DSA random number generator and the hardware random number generator. For each RNG, the module compares the newly generated block of output with the previously generated block of output. In the event of an error, the module outputs an error code.

The module also implements statistical random number generator tests run on the hardware random number generator (monobit, runs, long runs, and poker) at startup. If these tests fail, the module enters an error state.

Pairwise Consistency Tests

When the TurboMISTY generates a new key pair, it runs a pairwise consistency check on those keys to make sure that the keys function properly. The module also runs a pair wise consistency check at startup.

Software/Firmware Tests

The encryption board firmware uses the checksum as an integrity check. The program data in the ROM to be transferred to the program RAM area is calculated, and a check is made to confirm that the sum is 0. If any trouble is found as the result of the above hardware diagnosis during booting, the following processes are performed:

- Collection of errors in log
- Termination of program
- Execution of endless loop
- Lighting of LED

Design Assurance

The board uses TMS320VC5402 that is a general-purpose DSP and firmware for DSP to perform RSA public-key cryptographic arithmetic. All firmware components are written in a high level C and C++ language, except for the use of assembly language that is needed for the startup sequence. Please refer to the TurboMISTY functional specification documents, External Specification for TurboMisty F/W, and TURBOMISTY F/W Input/Output Data Specification for details on the firmware and hardware.

Mitsubishi has a configuration management system for the TurboMisty hardware and firmware and for the documentation associated with the TurboMisty.

Additionally, Microsoft Visual Source Safe (VSS) version 6.0 was used to provide configuration management for the module's FIPS documentation. This software provides access control, versioning, and logging.

Mitigation of Other Attacks

The TurboMISTY does not employ any technology that applies here.

SECURE OPERATION OF THE TURBOMISTY

The Mitsubishi TurboMISTY meets Level 3 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-approved mode of operation.

Crypto Officer Guidance

Initialization

After the module is received, the Crypto Officer must check the module's case and the tamper evidence label on the case for evidence of tampering. Such indications include damage to the tamper-evident label (see the next paragraph), and prying, bending, or cutting of the metal casing. The card should look like the following picture in figure 1.

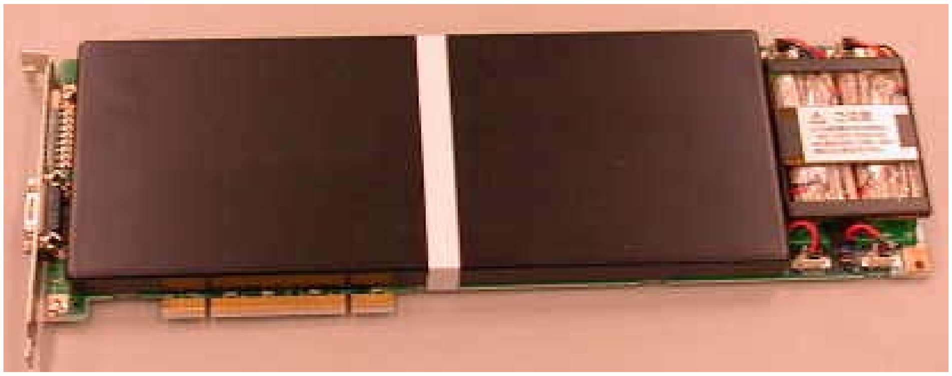


Figure 1 - View of Mitsubishi TurboMisty with Tamper Evidence Label

The tamper evidence label has an adhesive backing to adhere to the module's painted surface. The label is affixed to the cover and the board on both sides of the board, and removing the cover of the board will damage the tamper evidence label. Signs of tampering include the following: curled corners, bubbling, and rips. Attempts to carefully remove the label using a sharp metal blade split the layers of the label and left tamper evidence in the form of Japanese characters on the bottom portion (see Figure 2 for a close-up).

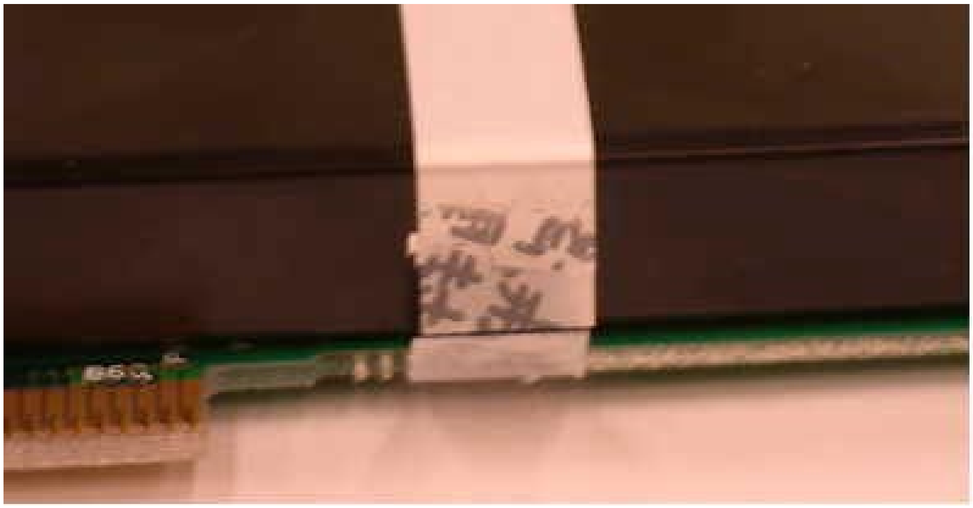


Figure 2 - Closeup of Tamper Evidence Label

After checking the module for evidence of tampering, the Crypto Officer must connect the module to the PCI port on the computer to be used. The installation CD contains all the setup files needed to access the TurboMISTY module.

The Crypto Officer needs to configure the module in order to operate in a FIPS approved mode of operation. This can be accomplished by calling the appropriate functions on the module or by using the TurboMISTY Manager, the management software for the TurboMISTY that is included on the installation CD provided with the TurboMISTY, which provides a graphical wrapper to the underlying functions.

Initialization of the board is done by the Crypto Officer per slot using the MKDS_SetInitialInfo() function. This initialization is most easily performed using the TurboMISTY Manager software. The Crypto Officer first selects the slot ID from the pull down menu and inputs the SO password. If this is the first time logging in, the initial SO PIN (password) is: 111111. If the input password is correct, "TURBOMISTY MANAGER" is started. Under the *Initialize* tab in the options menu, the Crypto Officer can set the *Login retry count* and give a name to the *Token Slot* label. The mode of operation must be set to FIPS in order for the board to be running in a FIPS-approved mode of operation. This means that only FIPS-approved algorithms listed in the Key Management section can be used.

The number of password attempts before lockout occurs must be set and logging to be turned on, and choosing passwords that are less likely to be guessed. The Crypto Officer can perform these steps using the following functions “MKDS_SetLockCount()” , “MKDS_SetLogMode()”.

If the Crypto-Officer wants to use the PCI slot detection as a physical security mechanism, the Crypto-Officer must configure this detection to be enabled. This can be set using the function “MKDS_SetBoardRemovalState()”.

Management

Upon first logging in after a slot has been initialized, the Crypto-Officer must change their password from the default set during initialization. This can be accomplished through the function provided to change passwords.

The Crypto Officer can check the mode of operation by issuing the command C_GetTokenInfo() or C_GetSlotInfo() to the module's PKCS#11 software library, which in turn issues a MKDS_GetNormalInfo() command to the module. The command returns a MKDS_FIPS_MODE boolean variable, which indicates the FIPS mode status.

The Crypto Officer is responsible for keeping track of the module and must routinely check the module for signs of physical tampering. Indications of physical tampering include damage to the tamper-evident label (see figure 2), and prying, bending, or cutting of the metal casing. If strange activity or damage to the label is found, the Crypto-Officer should take the module offline and investigate. If the board has been zeroized, the Crypto Officer must inspect the tamper evidence label or remove the board and perform a thorough inspection for physical damage.

When use of the TurboMISTY board has completed, the Crypto Officer should zeroize any CSPs.

User Guidance

Upon first logging in to their account, the User should change their password from the one provided to them by the Crypto-Officer.

The User role of the TurboMISTY has access to his/her own private objects, key control, data control, and cryptographic processing. Please see the document *TURBOMISTY F/W Input/Output Data Specification* and the *PKCS#11* standard for the listing and descriptions of these functions.

The User also has control of the RSA public/private keys, DES/3DES session keys, and his/her own password. The User should be careful not to disclose session keys or secret RSA keys to other parties. Passwords should be chosen that are less likely to be guessed and should also not be shared with other parties.

Additionally, when inputting or outputting 168 bit 3DES keys wrapped with RSA, only 2048 bit or greater RSA keys may be used.

TERMS AND DEFINITIONS

The following table lists the terms discussed in this security policy and their respective definitions

Term	Definition
3DES	Triple DES
CD	Compact Disk
CO	Crypto Officer
CSP	Critical Security Parameter
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DSP	Digital Signal Processor
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
FPGA	Field-Programmable Gate Array
FSM	Finite State Machine
ID	Identification
KAT	Known Answer Test
LED	Light Emitting Diode
LSI	Large-Scale Integration
MD5	Message Digest 5
NIST	National Institute of Standards and Technology
OS	Operating System
PCI	Peripheral Component Interconnect
PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standard
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read-Only Memory
RS-232	Recommended Standard 232
RSA	Rivest, Shamir and Adleman
SHA-1	Secure Hash Algorithm
SO	Security Officer
SDRAM	Synchronous Dynamic Random Access Memory
SRAM	Static Random Access Memory

Table 4 – Terms and Definitions