ETERNUS DX400/DX8000 Controller Module

Security Policy

December 2013

Version 1.3

FUJITSU LIMITED

Update History

Versions	Dates	Update contents
1.0	1/13/2012	The first version
1.1	10/25/2012	1.1 released
1.2	7/22/2013	1.2 released
1.3	12/24/2013	1.3 released

1. Overview

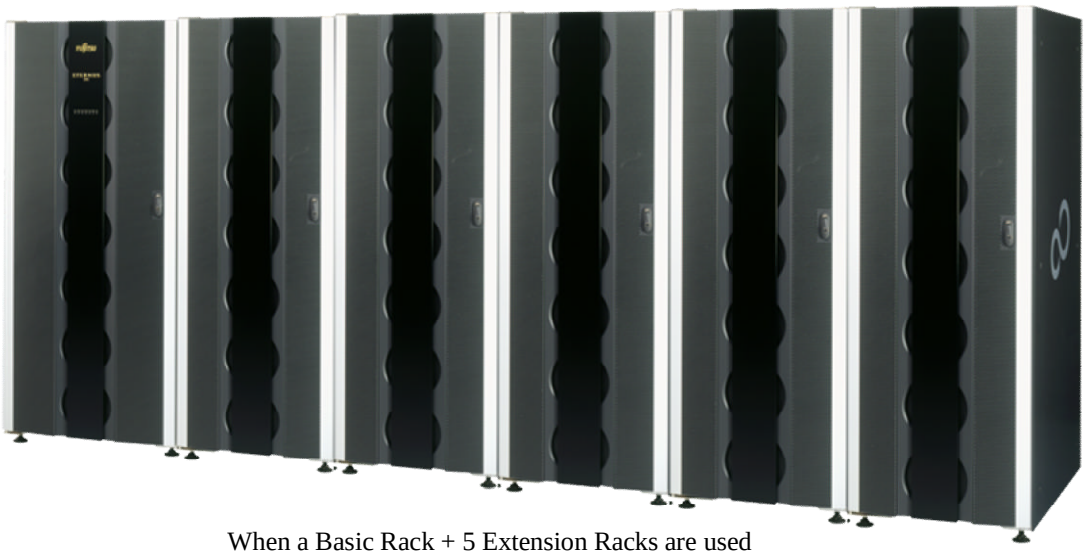
This non-proprietary document defines the security policy of the CM (Controller Module), which offers cryptographic functions, of the FUJITSU's ETERNUS DX400/DX8000 Disk storage system.

Cryptographic module name : ETERNUS DX400/DX8000 Controller Module
Cryptographic module version : V20L80-1000

ETERNUS DX410/DX440 are collectively referred to as "DX400" and ETERNUS DX8100/DX8400/DX8700 as "DX8000" in this document.

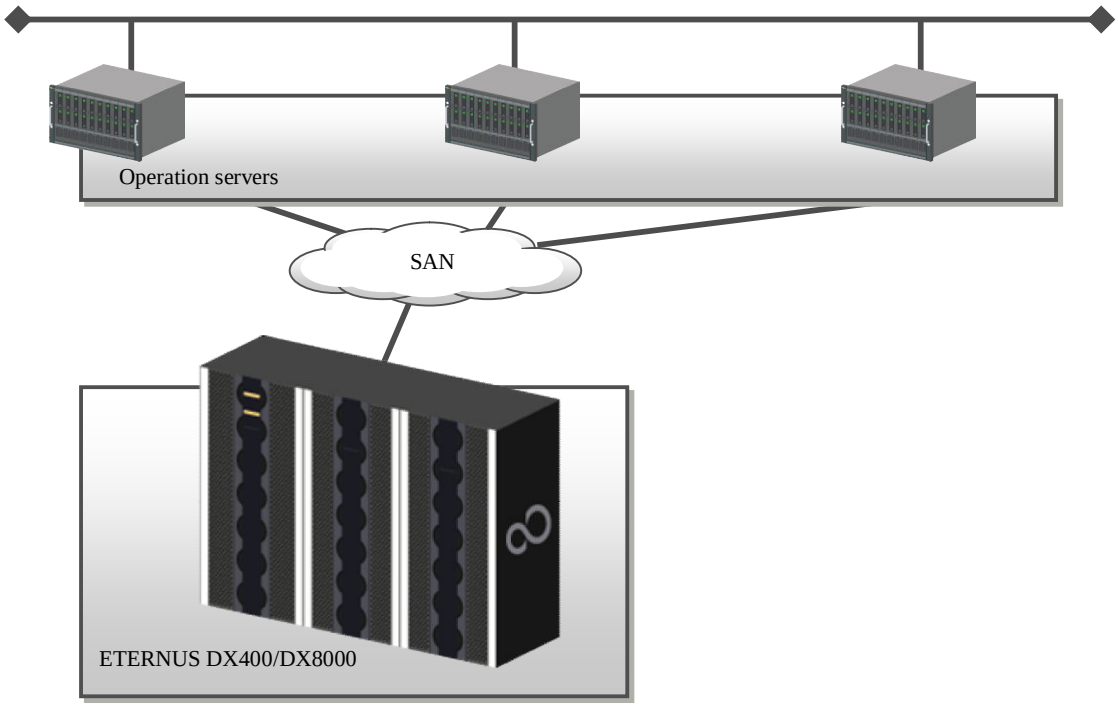
- ETERNUS DX400

- ETERNUS DX8000



When a Basic Rack + 5 Extension Racks are used

ETERNUS DX400/DX8000 Disk storage system is a storage system that offers the most appropriate storage platform to support our customers' IT infrastructures.



A storage platform has the following three requirements of IT infrastructures.

The first requirement is the scalability to store a large amount of information and the readiness for business continuance

to offer information without delay.

The second requirement is data maintainability and security to store information correctly.

The third requirement is the flexible operation and management of a large amount of information at a corporate level, and TCO reduction.

ETERNUS DX400/DX8000 Disk storage system was developed as a storage platform to meet these three requirements.

Scalability and Business Continuance

- World's largest capacity (5.45PB)
- Excellent IOPS performance with high-end CPU configuration

Data Maintainability and Enhanced Security

- Enhanced back-up functions
- Remote disaster control (enhanced midrange products, iSCSI Remote Adaptors)

Flexible Operation Management and TCO Reduction

- LUN dynamic expansion and virtual storage support
- Integrated storage

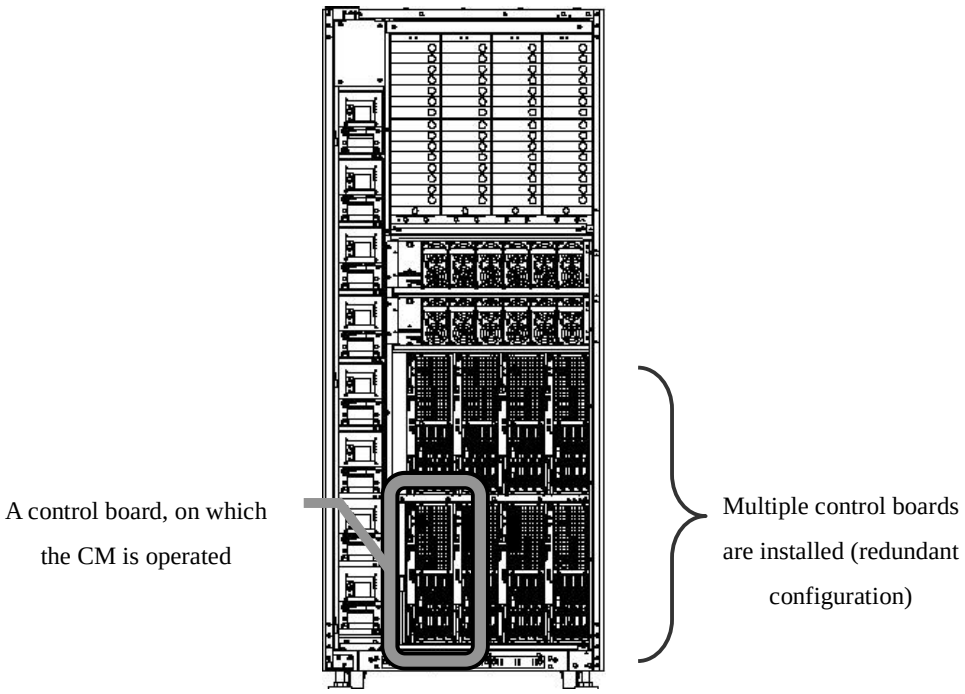
2. Cryptographic Module Specifications

2.1. Overview

The cryptographic function of the ETERNUS DX400/DX8000 Disk storage system is operated by the CM (Controller Module). The CM is a firmware that is operated on the control board, and classified as a multiple-chip-embedded cryptographic module.

2.2. Hardware Configuration

The control board, on which the CM is operated, is installed in the ETERNUS DX400/DX8000 Disk storage system as indicated in the following diagram (this example is a floor stand model).

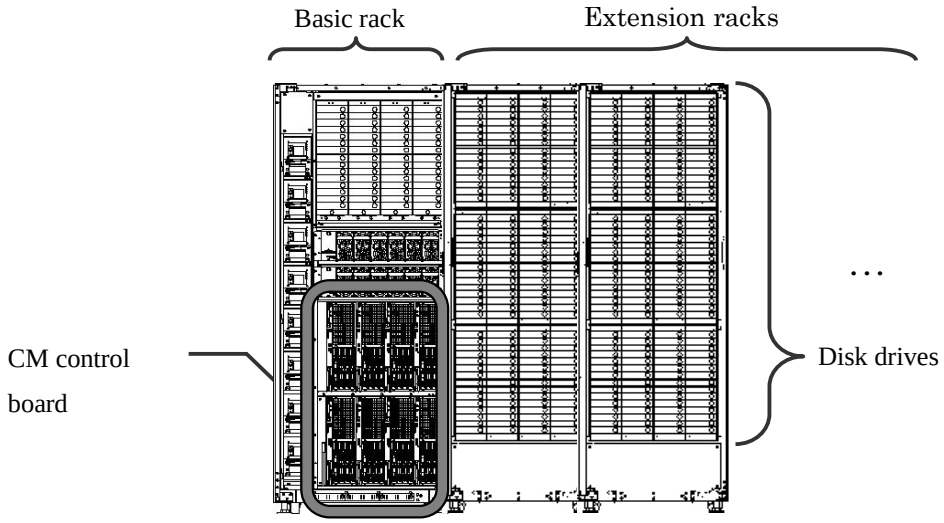


There is a concept of "master CM" and "slave CM" about this cryptographic module.

When multiple CMs are installed, a CM, to which authority to manage the ETERNUS DX Disk storage system has been given, is called a "master CM". The other CMs are called "slave CM".

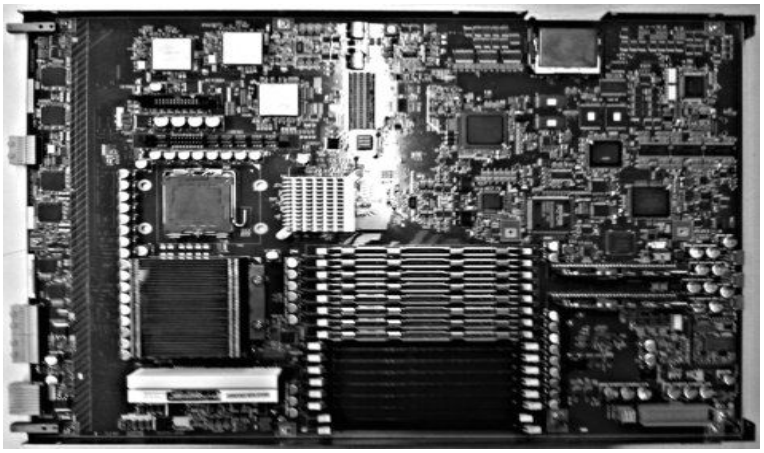
The cryptographic key is generated in a master CM, and transferred to salve CMs.

In this configuration, extra Disk Drives can be added by installing Extension Racks to the Basic Rack on which the CM Control Board is installed.

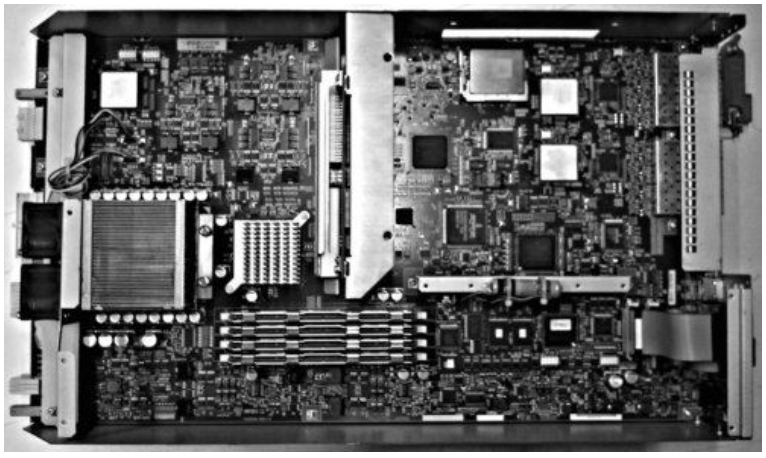


- The external appearance of the CM control board is indicated as follows:

ETERNUS DX8000



ETERNUS DX400

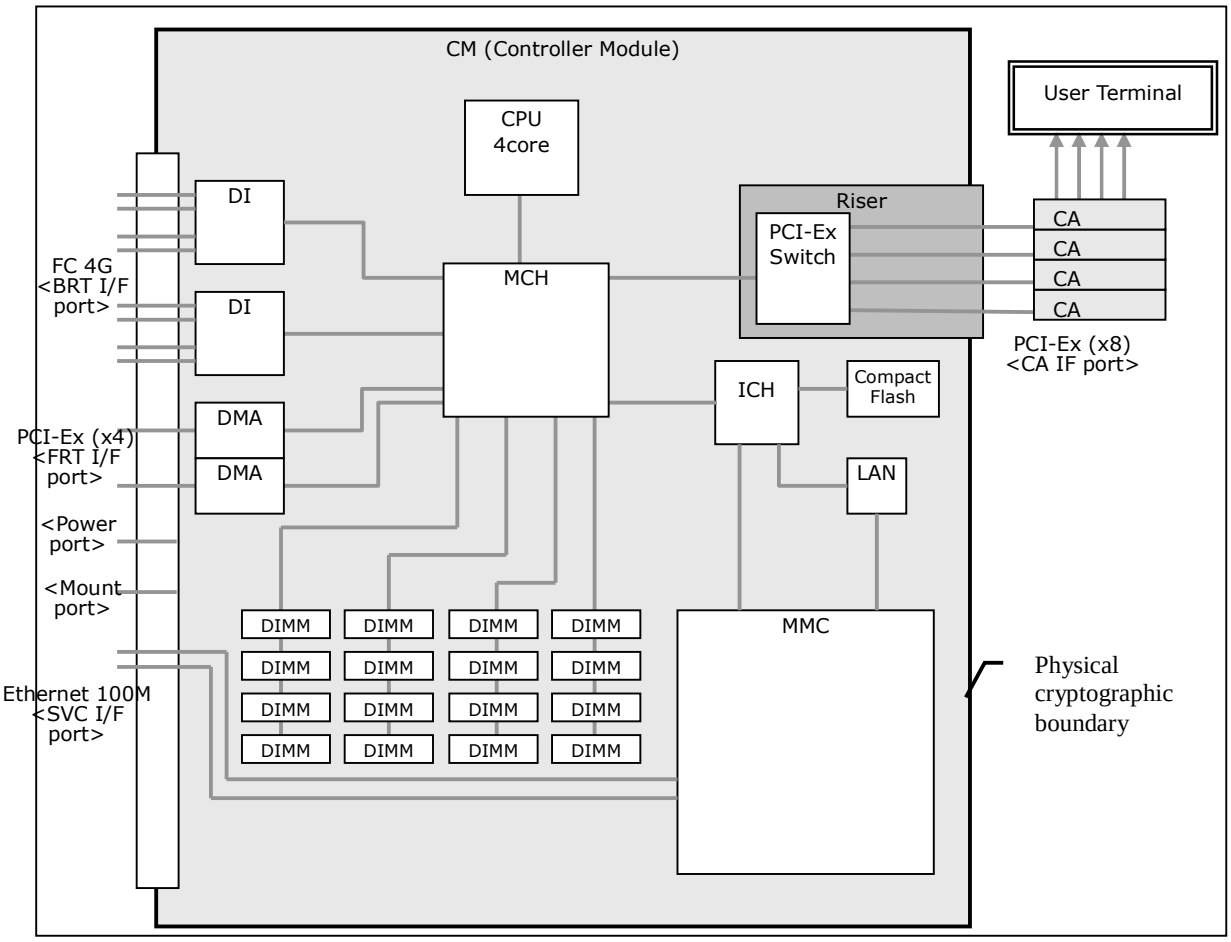


The CM control board is indicated in the following block diagram.

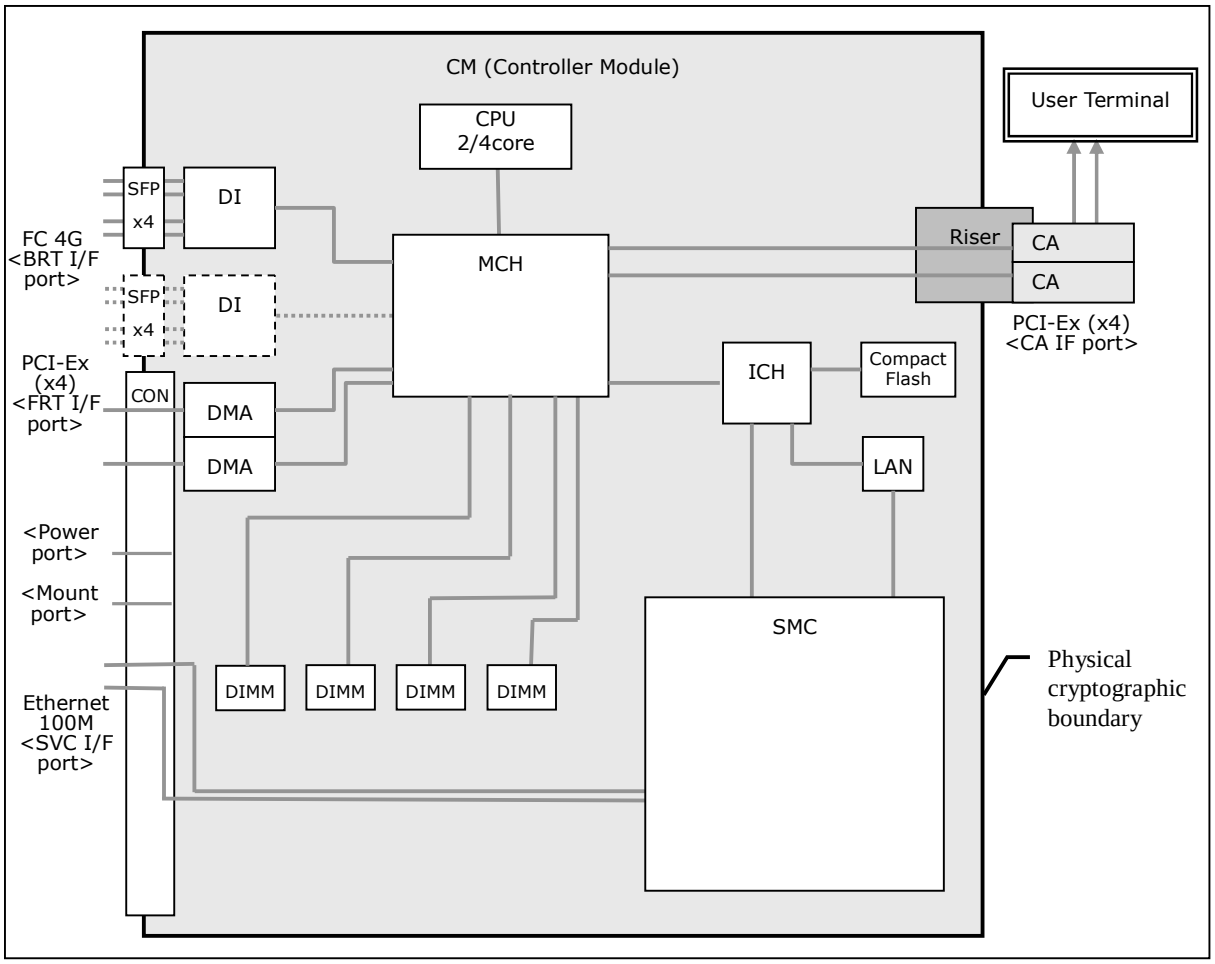
(For explanation on the module included in the diagram, refer to “Acronyms and Terms”.)

The firmware is stored in Compact Flash to show in this block diagram.

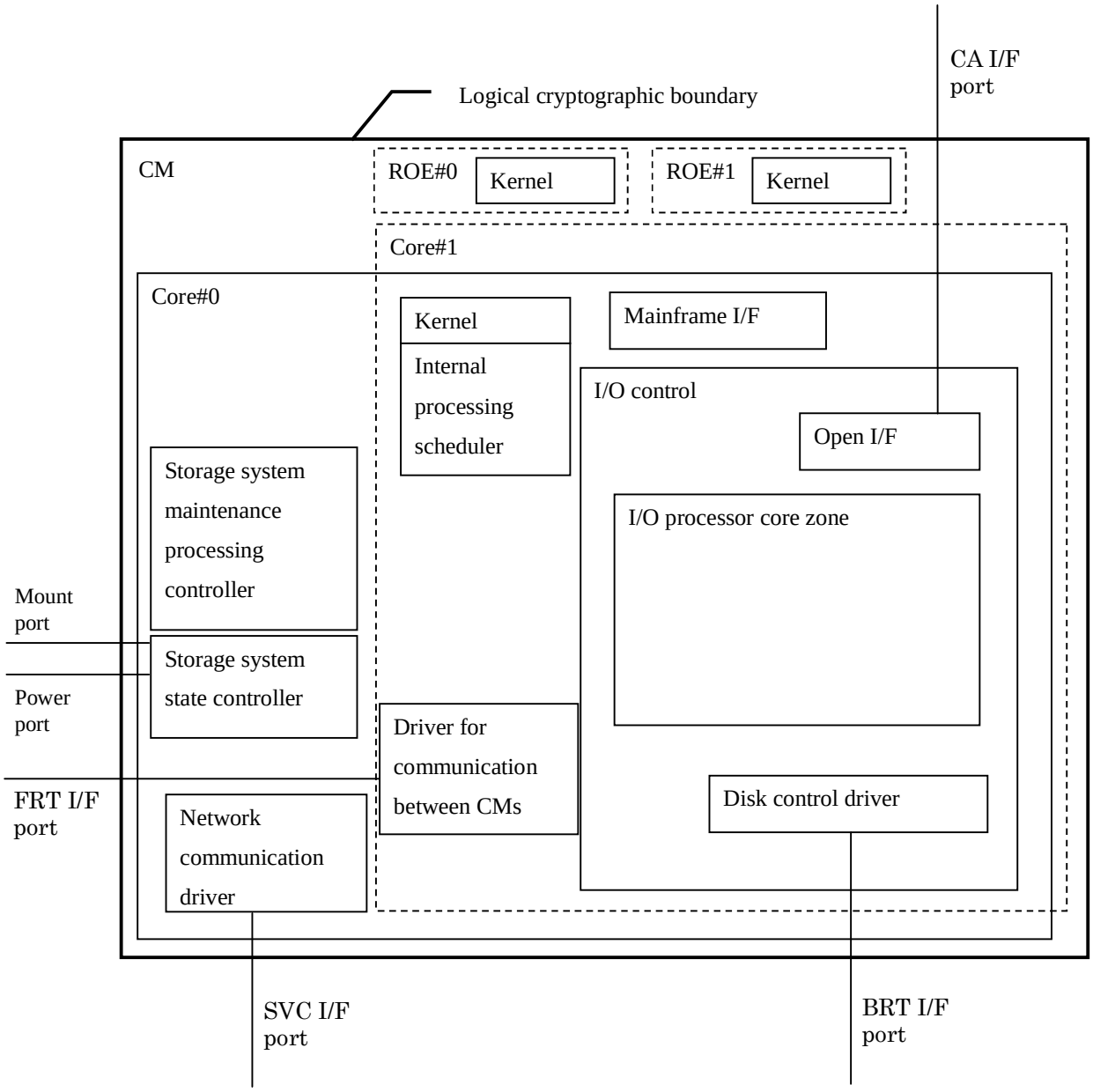
- ETERNUS DX8000



- ETERNUS DX400



2.3. Firmware Configuration



2.4. Security Functions and Operation Modes

The cryptographic module has three modes:

- AES mode (FIPS mode)

  This mode uses the AES(Advanced Encryption Standard) algorithm.
- Fujitsu original encryption mode (non-FIPS mode)

  This mode uses a Fujitsu proprietary algorithm.
- No encryption mode (non-FIPS mode)

  This mode uses no security functions.

The AES mode and Fujitsu Original Encryption mode have the following security functions.

AES Mode (Approved operation mode)

Function	Algorithm	Standard	Algorithm Certificate
Encryption and decryption	AES-128	FIPS PUB 197	#2542
Key encryption	AES-256	FIPS PUB 197	#2542
Key wrapping	AES-256 (AES Key Wrap)	FIPS PUB 197	#2542
Random number generation	X9.31 A.2.4 AES	ANSI	#1207
Hash function	SHA-256	FIPS PUB 180-4	#2142

Fujitsu Original Encryption mode (Non-approved operation mode)

Function	Algorithm	Standard	Algorithm Certificate
Encryption & Decryption	Fujitsu Original Encryption	Fujitsu proprietary	non-compliant
Key encryption	AES-256	FIPS PUB 197	
Random number generation	X9.31 A.2.4 AES	ANSI	

- The Crypto Officer uses the management console to switch between the AES mode and Fujitsu Original Encryption mode.
- The Crypto Officer can invoke approved mode of operation by setting encryption mode to AES on the management console.
- The AES mode and Fujitsu Original Encryption mode are mutually exclusive and do not coexist.

[Fujitsu Original Encryption mode]

In Fujitsu Original Encryption mode, such as roles and services are the same as that of AES mode. Data cryptographic key and Encryption mode management flag are zeroed when the Encryption mode is modified. So, Fujitsu Original Encryption mode does not affect AES mode.

[Summary of Encryption mode and Encryption Algorithm]

Approved Encryption Algorithm

AES-128 / AES-256 / X9.31 A.2.4 AES / SHA-256

Non-approved Encryption Algorithm

Key wrapping Algorithm / Fujitsu Original Encryption Algorithm

FIPS mode

AES Mode (AES-128 / AES-256 / X9.31 A.2.4 AES / SHA-256 / Key wrapping Algorithm)

Non-FIPS mode

Fujitsu Original Encryption Mode (Fujitsu Original Encryption Algorithm), or disable encryption mechanism

2.5. Security Level

This cryptographic module satisfies the following level for each of the following security requirements. This module satisfies Security Level 1.

Security requirement	Level
Cryptographic module specification	1
Cryptographic module ports and interfaces	1
Roles, services, and authentication	1
Finite state models	1
Physical security	1
Operational environment	N/A
Cryptographic key management	1
Electromagnetic interference/Electromagnetic compatibility (EMI/EMC)	1
Self-tests	1
Design assurance	1
Mitigation of other attacks	N/A

3. Cryptographic Module Ports and Interfaces

The following table indicates the specifications of the physical ports and logical interfaces of the cryptographic module. It also shows the presence of cryptographic services and functions each physical port is equipped with.

Physical ports	Logical interfaces	Cryptographic services	Functions
CA I/F port	Data input interface Data output interface	No	• User data read • User data write • Data transfer between the cryptographic module and the user terminal
FRT I/F port	Data input interface Data output interface Control input interface	Yes	• User data read • User data write • Data transfer between cryptographic modules
BRT I/F port	Data input interface Data output interface	Yes	• User data read • User data write • Data transfer between the cryptographic module and the disk
SVC I/F port	Control input interface State output interface	Yes	• Encryption settings • Cryptographic state display
Mount port	State output interface	No	• Notification of the mount state for the cryptographic module The cryptographic module output the signal indicating own being inserted in the ETERNUS DX400/DX8000. This is used for the state management of the ETERNUS DX Disk storage system.
Power port	Power source	No	• Power supply to the cryptographic module

4. Roles, Services and Authentication

4.1. Roles

This cryptographic module supports the user role and the Crypto Officer role. The following table indicates the roles, which this cryptographic module supports, and the roles' authorized services.

Role	Authorized service
User Role	A user role is used to access the user data of this cryptographic module.
Crypto Officer Role	A Crypto Officer role is used to perform cryptographic settings of this cryptographic module (including cryptographic key initialization) and display cryptographic states.

4.2. Services

This cryptographic module supports settings and display operations to use the essential functions, specified in SCSI, and cryptographic functions. The following table indicates the relationship between the cryptographic module's CSPs and supported services, I/F and CSPs that the services use, and access types (read, write, execute, etc.).

- CSP List

CSP name	Description
Data cryptographic key	A secret key that is used for user data encryption and decryption
Master cryptographic key	A secret key that is used to encapsulate the data cryptographic key
Random seed value	A random seed value that is used to generate a data cryptographic key
Encryption mode management flag	Management information of the security function's operation modes (the AES mode and Fujitsu Original Encryption mode) that is offered by the cryptographic module

- Relationship between services and CSPs

Service	CSP	Access type (Read/Write/Execute, etc.)
User Data Read (in encrypted volume)	Data cryptographic key (reference)	Read (Decrypt) • Read user data from the disk via the BRT I/F port, and decrypt the data with the cryptographic module ↓ • After decrypting the user data with the cryptographic module, send the data to the user terminal via the CA I/F port
User Data Read (in non-encrypted volume)	None	Read (Alternating bypass mode) • Read user data from the disk via the BRT I/F port, and send the data to the user terminal via the CA I/F port
User Data Write (in encrypted volume)	Data cryptographic key (reference)	Write (Encrypt) • Encrypt the user data that was sent from the user terminal via the CA I/F port, with the cryptographic module ↓ • After encrypting the user data with the cryptographic module, write the data onto a disk via the BRT I/F port
User Data Write (in non-encrypted volume)	None	Write (Alternating bypass mode) • After receiving the user data that was sent from the user terminal via the CA I/F port, write the data onto a disk via the BRT I/F port
Encryption Settings (Master CM Only)	Data cryptographic key (generation and initialization) Master cryptographic key (generation) Random seed value (generation) Encryption mode management flag (update)	Execute (Change the cryptographic state) • After receiving a request for an encryption setting via the SVC I/F port, generate a data cryptographic key and a master cryptographic key with the cryptographic module, and update the encryption mode management flag ↓ • Communicate with all the other cryptographic modules via the FRT I/F port, and update the management information
Cryptographic State Display (Master CM Only)	Encryption mode management flag (reference)	Execute (Check the cryptographic state) • After receiving a request for cryptographic state display via the SVC I/F port, acquire the management information with the cryptographic module, and display the state

Data cryptographic key is made in master CM, and transferred to slave CM. Key wrapping of Data cryptographic key is performed, when this transfer is occurred by way of FRT I/F port.

Bypass Mode:

The cryptographic module supports alternating bypass mode, which enables the module to transfer plaintext data. To enable the bypass mode, the Crypto Officer must configure the volume for "non-encrypted volume" before using it. The cryptographic module has an internal table of volumes, and judge it for I/O requests of the user data whether the target volume is the encrypted volume or not, and bypass the cryptographic processing if it is the non-encrypted volume.

4.3. Operator Authentication

There are two roles in the module that operators may assume: Crypto Officer role, and User role.

Please note that, as the cryptographic modules were validated against Level 1 requirements, they do not support role-based or identity-based authentication.

The User and Crypto Officer roles are implicitly assumed by the entity accessing services implemented by the Module.

Service	Role
Read user data	User role
Write user data	
Perform encryption settings	Crypto Officer role
Display cryptographic state	

4.3.1. Crypto Officer role

The Crypto Officer role is implicitly assumed when performing encryption settings, or displaying cryptographic state.

The Crypto Officer accesses the modules via SVC I/F port by the management console operations.

(for example : switch between the AES mode and Fujitsu Original Encryption mode,

create new encrypted volumes, encrypt non-encrypted volumes, or display encrypted volumes)

4.3.2. User role

The User role is implicitly assumed when reading user data, or writing user data.

The User accesses the modules via CA I/F port by the user terminal as Read I/O or Write I/O.

(for example : VMware ESX I/O, HyperV I/O, Oracle DB I/O, Symantec NetBackup I/O, or CA ARCserve I/O)

5. Physical Security

CM is multiple-chip embedded cryptographic module that is installed in the product grade ETERNUS, thus, this cryptographic module satisfies Level 1 of FIPS PUB 140-2 physical security requirements.

6. Operational Environment

Since this cryptographic module is non-modifiable firmware, the application of security requirements to the operational environment is not applicable.

7. Cryptographic Key Management

7.1. Random Bit Generator (RBG)

This cryptographic module employs a standalone RBG that is used to generate a data cryptographic key. RBG and its operation mode comply with ANSI X9.31 A.2.4 AES.

7.2. Key Establishment and Key Entry and Output

This cryptographic module encapsulates and delivers a key with several cryptographic modules.

7.3. Key Generation, Key Storage, and Key Zeroization

CSP	Usage, generation, storage, and zeroization
Data cryptographic key	Data cryptographic key is used for user data encryption and decryption. Generated by a Random Bit Generator. The key is encrypted in accordance with AES-256, using the after-mentioned master cryptographic key in the cryptographic module, and stored on a CompactFlash card. The key is zeroed just before the encryption mode is modified.
Random seed value	Random seed value is a seed value that is used to generate random numbers. This value is generated and temporarily stored on DIMM when the encryption mode that generates random numbers is changed or when the cryptographic module's power is turned on. When the encryption mode is changed, the value is zeroed.
Master cryptographic key	The master cryptographic key is used to encapsulate a data cryptographic key, and generate random numbers in accordance with AES. The key is generated, when it is needed to use, and temporarily stored on DIMM. The key is zeroed, when it is finished to use.
Encryption mode management flag	Encryption mode management flag is the management information of the operation modes for the security function (AES or Fujitsu Original Encryption) that are provided by the cryptographic module. The information is stored on a CompactFlash card. The information is zeroed when the Encryption mode is modified.

8. Self-Tests

8.1. Power-up Self-Tests

This cryptographic module performs a power-up self-test when the module's power is turned on. An operator can start the power-up self-test on demand when the power of the cryptographic module is turned off and then on again.
The cryptographic module performs the following power-up self-tests.

(a) Cryptographic algorithm test

Function	Algorithm	Test
Encryption & decryption	AES-128	Known-answer test
Encryption & decryption of a cryptographic key	AES-256	Known-answer test
Random number generation	X9.31 A.2.4 AES	Known-answer test
Hash function	SHA-256	Known-answer test

(b) Firmware integrity test

Firmware has a feature to validate integrity, and confirm the integrity before loading data from a storage location to DIMM.

8.2. Conditional Self-Tests

This cryptographic module performs the following conditional self-tests when the relevant security function is being invoked.

(a) Continuous random bit generator test (RBG test)

The module generates a new block, and confirms that the block is not equivalent to the one that has just been created.

(b) Bypass test

If the mechanism to manage the switching procedure of a cryptographic service is going to be modified, the module validates that the last modification of the mechanism has been unchanged. The cryptographic module also performs a test for the correct operation of the services providing cryptographic processing.

9. Design Assurance

9.1. Configuration Management and Development

Configuration management and development of this cryptographic module is implemented in accordance with the quality management system that has been certified by ISO9001:2008.

9.2. Delivery and Operation

This cryptographic module operates to control the ETERNUS DX Disk storage system, and is securely distributed and operated in accordance with the manual for the ETERNUS DX Disk storage system installation and operation.

9.3. Guidance Documents

Guidance documents are offered as a manual to support the ETERNUS DX Disk storage system operation. Crypto Officer guidance and user guidance are included in these documents.

10. Mitigation of Other Attacks

This cryptographic module does not address other attacks.

11. References

(1) FIPS PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

(2) Derived Test Requirements for FIPS PUB 140-2, Security Requirement for Cryptographic Modules

(3) FIPS PUB 197, ADVANCED ENCRYPTION STANDARD (AES)

(4) FIPS PUB 180-4, SECURE HASH STANDARD

(5) Annex C: Approved Random Number Generators for FIPS PUB 140-2, Security Requirements for Cryptographic Modules

(6) NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms

12. Acronyms and Terms

BRT (Back-end Router)

A module that controls communication routing between a CM and a disk

CA (Channel Adaptor)

A module that controls interfaces and data transfers between a CM and a user terminal

CM (Controller Module)

A module that manages entire operations of the ETERNUS DX Disk storage system

DI (Drive Interface)

A module that controls interfaces and data transfers between a CM and a disk

FRT (Front-end Router)

A module that controls communication routing between CMs

ICH (I/O Controller Hub)

A chip that connects a PCI bus or an IDE bus with another component

MCH (Memory Controller Hub)

A chip that connects a CPU and a memory device

MMC (Module Management Controller)

A module that performs various maintenance functions by monitoring a CM board or communicating with the SVC

SVC (Service Controller)

A module that operates with a resident power source, and monitors the entire ETERNUS DX Disk storage system

SMC (Server Management Controller)

A module that is installed only on DX400, and has the MMC and SVC functions of DX8000

Encryption Setting

Encryption setting of the cryptographic module that is conducted by an operator

The operator assumes the Crypto Officer role to carry out this operation

The encryption setting of the cryptographic module includes the following operations:

- Encryption mode setting

  (Select the AES mode or Fujitsu Original Encryption mode, or disable encryption mechanism)
- Create a new encrypted volume

  (Each volume can be set as encrypted or non-encrypted)
- Encrypt a non-encrypted volume

Cryptographic state display

An operation conducted by an operator to display the cryptographic state of the cryptographic module

The operator assumes the Crypto Officer role to carry out this operation

The cryptographic states of the cryptographic module are displayed as follows:

- Displays the currently selected encryption mode
- Displays encrypted volumes

User Data

Data that is read or written from a user terminal that is connected with the ETERNUS DX Disk storage system

User Terminal

Host computer which connects to this cryptographic module

